TS

NOT MEASUREMENT SENSITIVE

DOE-STD-3024-98
October 1998

DOE STANDARD

CONTENT OF SYSTEM DESIGN DESCRIPTIONS

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

AREA EDCO

FOREWORD

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

A System Design Description (SDD) describes the requirements and features of a system. This standard envisions "systems" and "subsystems" within the context of the way these terms are defined within this standard.

This standard provides guidance on the expected technical content of SDDs. The need for such a standard was recognized during efforts to develop SDDs for safety systems at DOE Hazard Category 2 nonreactor nuclear facilities. Existing guidance related to the corresponding documents in other industries is generally not suitable to meet the needs of DOE nuclear facilities. Across the DOE complex, different contractors have guidance documents, but they vary widely from site to site. While such guidance documents are valuable, no single guidance document has all the attributes that DOE considers important, including a reasonable degree of consistency or standardization. This standard is a consolidation of the best of the existing guidance.

This standard has been developed with a technical content and level of detail intended to be most applicable to safety systems at DOE Hazard Category 2 nonreactor nuclear facilities. Notwithstanding that primary intent, this standard is recommended for other systems at such facilities, especially those that are important to achieving the programmatic mission of the facility. In addition, application of this standard should be considered for systems at other facilities, including non-nuclear facilities, on the basis that SDDs may be beneficial and cost-effective.

This standard should be applied in a logical and systematic manner that fits the local situation in a way that leads to SDDs that are user friendly, promote safety, and increase operating efficiency. This standard is intended to be applied either to new facilities and systems or to existing systems. Attachments to this standard provide guidance on tailoring SDDs that should be considered when preparing SDDs for existing systems.

Like National consensus standards, the DOE Technical Standards program expects its standards to be applied generally voluntarily. The existence of a standard does not mandate its use. Sometimes standards are applied voluntarily by the local design engineering organization or by the sponsoring organization. Sometimes, a standard is mandated by a higher authority or a regulatory agency, and hence the standard becomes mandatory. Whether a standard is applied on a voluntary or mandatory basis, distinguishing the requirements contained in a standard from its recommendations becomes highly desirable. This distinction is accomplished by the careful use of the terms "shall" to designate requirements and "should" to designate recommendations within the standard. Compliance with a standard is then achieved by adherence to its requirements and consideration of its recommendations. This standard does not create a requirement for the development of SDDs for particular systems at particular facilities, nor that such SDDs must adhere to this standard. Consideration of the Introduction or Attachments to this standard is not mandatory for adherence to this standard.

Beneficial comments for improvements of this standard (additions, deletions, or other changes) and any pertinent information should be addressed to either Mr. John Fredlund or Mr. Rick Kendall at DP-45/GTN, U. S. Department of Energy, 19901 Germantown Rd., Germantown, MD 20874-1290. Commenters are encouraged to use the form DOE F 1300.3, "Document Improvement Proposal."

INTENTIONALLY BLANK

Table of Contents

TABLE OF CONTENTS (continued)

PARAGRAPH **PAGE**

Attachments to DOE-STD-3024-98

Introduction to DOE-STD-3024-98

This section provides background information concerning the purpose and functions of System Design Descriptions (SDDs) and the use of this standard in preparing SDDs. This section has been formatted differently from the main body of this standard, which starts on page 1 with the outline for an SDD.

Purpose of a System Design Description

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. As part of a configuration management change control process, the SDD helps ensure consistency among the engineering requirements for systems, the actual installed physical configuration, and the associated documentation.

The SDD is a central coordinating link among the engineering design documents, the facility authorization basis, and implementing procedures. An SDD does not originate requirements or basis information, but rather collects that information into a convenient usable form. The SDD consolidates information about a particular system into one document. This provides the advantage that a reader does not have to wade through many different documents and pull out the pertinent parts or have to decipher the details in vendor technical manuals and engineering documents.

During the design and construction of a new facility or new system, the SDD might serve as the vehicle for collecting and conveying the system requirements and their bases (i.e. the technical baseline). The SDD should contain requirements that are derived from programmatic needs as well as from the associated safety analyses. Accordingly, the development of the SDD must be coordinated with the engineering design process and with the safety analysis development. The SDD may be used for controlling changes as the design evolves from a concept through the preliminary design to the final design. Sometimes this is accomplished 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, and the FDD refers to SDDs for more detailed information. An FDD provides a mechanism for addressing simple, less important systems such as a potable water system, without having to develop separate SDDs. The SDD is updated periodically and hence becomes more complete and detailed as the design and safety analysis processes mature. Toward the end of the design phase, the SDD may be used as a source document for the development of the facility authorization basis. Safety information in the SDDs is extracted and placed into the SAR. In this case, the authorization basis mirrors the safety information in the SDD. Even though the SDD may precede the development of the SAR, and hence may become a source document for the authorization basis, an SDD is not a part of the authorization basis. DOE does not rely upon information found uniquely in the SDD to make decisions regarding the safety of the facility.

For an existing facility or system, when the development and approval of the authorization basis have preceded the development of SDDs, the safety portions of the SDDs must mirror the authorization basis documents. Accordingly, the SDD is not an authorization basis document. Controlling equipment changes depends on recognizing changes, knowing what the existing requirements are, and understanding why those requirements exist. The modification might involve a change in how the requirement will be met, or might involve modifying a requirement or establishing a new requirement. Evaluating the acceptability of a change in requirements is difficult if the reasons behind the requirements are not understood. The SDD can help meet this change control need. When a change to the system is proposed, the SDD can be consulted to identify the pertinent requirements and the referenced engineering source documents. The results of the change would be reflected back into the

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

An SDD supports the authorization basis and helps ensure that operations of the system will be consistent with the authorization basis. While the authorization basis is focused on safety, the SDD is broader because it also addresses other important features provided to accomplish the programmatic mission, to maintain system reliability, and to promote effectiveness, efficiency, and flexibility in operations and maintenance. To treat the SDD as a part of the facility authorization basis would be counter-productive to these broader purposes.

The SDD promotes safe and efficient operation by providing the information necessary for a solid technical understanding of the system. The SDD collects and provides significantly more detail than is appropriate for authorization basis documents but less detail than the engineering design documents. This level of detail is particularly appropriate for the intended audience of facility operations personnel, maintenance personnel, and technical support personnel. The SDD identifies procedures for facility operations, testing, and maintenance related to the system being described, and points the reader to those specific documents in their proper context. This information leads to fewer operational errors and incidents. SDDs also identify which performance characteristics of the system are the most important. This information promotes a better understanding of where to exercise greatest care and attention to detail. In both operations and maintenance, an understanding of why requirements exist promotes better employee performance and adherence to safety management programs, implementing procedures, and administrative controls.

The SDD is a convenient reference for evaluating the performance of the system. System performance evaluations are important for several reasons. These 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.

The SDD should be a controlled document and maintained as an authoritative up-to-date source of technical information on the system. The SDD records technical information that might tend to get lost as personnel changes occur over the years. SDDs can be used also as technical source documents for the development of personnel training programs.

Purpose of DOE-STD-3024-98

This standard defines the expected technical content and organizational structure of SDDs.

Applicability

This standard may be used to develop an SDD for any new or existing system at any DOE facility.

Tailoring Requirements (Graded Approach)

Provisions and flexibilities have been incorporated into this standard so that it can be applied directly in many situations and accommodate systems of varying importance and systems of different physical types (such as ventilation, fluids, and electrical power systems).

Since the requirements in this standard have been selected to be most applicable at DOE Hazard Category 2 nonreactor nuclear facilities, and more specifically to safety systems at those facilities, further tailoring of the requirements for those systems would generally be inappropriate.

When applying this standard to non-safety systems at nuclear facilities and to systems at nonnuclear facilities, the graded approach should be employed. Attachment 1 to this standard provides guidance on these applications. The graded approach considers many factors that must be considered on a case-by-case basis. These include importance of the facility, remaining facility lifetime, the magnitude of the hazards involved, the importance of the system, and the complexity of the system. The types and amount of information contained in an SDD will vary depending on the specific system being described. Engineering judgement must be used to ensure that appropriate, useful, and necessary information is provided in the SDD, while avoiding the expenditure of resources to include information that does not add value to the SDD. The level of effort involved in the development of an SDD will be determined in part by the availability of current and dependable design information. Attachment 2 to this standard provides guidance on compiling technical information for preparation of SDDs and may be useful for existing systems where a well documented design information is not readily available.

Format and Content of DOE-STD-3024-98

Following this introduction, this standard presents the outline for an SDD, followed by guidance on the technical content of an SDD. Because this standard provides guidance on developing a document, the technical content guidance sections have been numbered to correspond with the outline of that document. This formatting is intended to make this standard easier to understand and easier to refer to later.

This standard and the outline of the SDD have been developed in a style intended to be as user friendly as possible. The standard and the corresponding SDDs may be read the first time on a straight-through, cover-to-cover basis, or various sections may be referred to as the need arises. To facilitate this first reading, certain information is presented early to promote a solid understanding of the information that follows. Section 1 and Section 2 of the SDD provide preliminary information that is will be advantageous to understanding the requirements that follow in Section 3. The requirements are presented first in order to lay the ground work for why the system is designed with certain capabilities and characteristics. Section 4 then describes how the system meets its requirements.

As used in this standard, the term “requirement” refers to those characteristics that have been developed, specified, and approved as an output of the design engineering process, and have been issued by the design engineering authority for the system. These requirements may be contained in documents such as drawings, procurement specifications, components lists, bills of materials, installation specifications, and testing specifications. All the engineering considerations behind these issued requirements are considered the bases of the requirements. Basis information includes specific design inputs and constraints (for example, functional and performance needs, mandated regulations, codes, and standards and design procedures), and intermediate products of the design process (such as studies, analyses, and calculations). The basis for a requirement might address several different considerations. For example, the bases might include information that indicates that a portion of certain capability was specified in order to meet the functional requirements that were design inputs, another portion because of particular regulatory requirements, an additional part of the total capability was to meet certain general engineering design constraints that might include site-specific engineering policies, standards, and procedures, and that another part of the total capability was specified as safety margin.

It is important that an SDD clearly distinguish between the items that are true requirements that the system must meet and those additional characteristics that are optional. In an SDD, it is intended that Section 3 would contain only the requirements on the system (and their bases), but not the extra, non-mandatory performance capabilities that might exist in the actual system design configuration. Section 4 of the SDD, on the other hand, presents a description of the actual system that, not only describes how the system meets its requirements, but also describes the full capacity and capabilities of the system. The principle of stating requirements only in Section 3 and describing the full capability in Section 4 is illustrated in the example below:

> Requirement
> The output power from the UPS system shall be provided (1) when incoming normal building electrical power is available, (2) through incoming electrical transients and momentary disturbances, and (3) for 2 hours following the loss of incoming building power.
>
> Description
> The UPS battery is rated at a nominal 125 Vdc and has been sized at 1800 Ampere-hours (Ah). This sizing has been shown to be capable of driving the full-rated inverter output for 3 hours. This ensures that the UPS will be able to provide clean electrical power not only when normal building power is available and through incoming switching transients, but also for a period significantly greater than the 2 hours required after the loss of building power. The capacity beyond the 2-hour requirement is an additional and optional design feature, not margin.

Performance capabilities that might exist in the actual installed system that exceed the "requirements" are not considered to be "requirements" but rather would be extra capabilities. Changes to characteristics presented in the Description (Section 4) that do not have a corresponding requirement (Section 3) or exceed the requirements can normally be approved by the contractor facility operating organization. Changes to a requirement stated in Section 3 would necessitate the review and approval by the design engineering authority. In considering a particular change request, the design engineering authority would be expected to review the design basis and in some cases might need to request approval from the authority that issued the design inputs (for example, a regulatory agency), before such a change could be approved. For codes and standards identified in an SDD that have been applied voluntarily at the option of the DOE contractor, the authority to modify that application remains at the discretion of the contractor. It should be noted that the DOE program for Unreviewed Safety Questions is aimed at determining if contractor final approval of a change is sufficient or DOE approval is required.

A major purpose of the SDD is to collect information so that the reader does not have to wade through numerous complex documents in an effort to locate the pertinent information. The information to be provided in the SDD is to be a combination of comprehensive (or narrative) and index (or road map) approaches. This middle-ground approach is based on including that information that the system engineer, facility operator, or other user may need but not including excessive details such as specifications of reinforcement bars for the structural members of the building or specific steps in an alarm response procedure. Engineering judgement must be applied to determine when information might be more detailed than is worthwhile for the intended audience of the SDDs and hence that information should only be referenced. 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 approach may often be to provide a brief 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. If the information is important to the overall purposes of an SDD and to the intended audience, it should be included in the SDD.

In some cases, there are sections that may appear to be repetitious. Repetition of the same information is not intended. It is appropriate to address the same topic in different ways and for different purposes in different parts of the standard or SDD. For example, “boundaries and interfaces” is the topic in four different places. In Section 1, the Introduction, it is necessary to address boundaries only so that the reader can easily determine if this SDD covers a specific component of interest or if a different SDD should be consulted. In Section 2, the Overview, it is necessary to depict the system boundaries and interfacing systems on the system diagram. In Section 3, the Requirements, it is necessary to address boundaries and interfacing systems only to the extent that there are system requirements in these areas. In Section 4, the Description, it is necessary to describe the precise physical boundaries of the system in order that components at or near the boundaries are properly classified and hence receive the appropriate care and attention in activities such as procurement and maintenance. Thus, while the same topic is addressed in multiple locations, the information presented in these sections is not repetitious. Different types of requirements in Section 3, especially the various engineering disciplinary requirements, are potentially repetitious. As stated in the standard, the information should be presented once and referred to if the same information is needed elsewhere. As this standard is applied to develop SDDs, care should be exercised to avoid presenting the same information repeatedly.

Glossary

This glossary explains important terms in this standard. To the extent practical, standard definitions have been used, and the source of that definition is referenced within square brackets at the end of the entry. The full bibliographical information on these references is given in Attachment 3 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.

Authorization Basis. Those aspects of the facility design basis and operational requirements relied upon by DOE to authorize operation. These aspects are considered to be important to the safety of the facility operations. The authorization basis includes the safety basis for the facility, which focuses on the protection of personnel, both offsite and onsite. DOE-STD-3009-94 defines "safety basis" as information relating to the control of hazards at a facility (including design, engineering analyses, and administrative controls) upon which DOE depends for its conclusion that activities at the facility can be conducted safely. The terms "authorization basis" and "safety basis" are sometimes used interchangeably. The authorization basis may also include information related to environmental protection. [See References 4 and 10.]

Authorization Basis Documents. Documents providing authorization basis information. These typically include, but are not necessarily limited to, the SAR, TSRs, EISs, DOE-issued Safety Evaluation Reports, and documents containing facility-specific commitments to comply with DOE Orders or policies. [See Reference 10.]

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. [See Reference 7.]

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 SAR, TSRs, and hazard and accident analyses. [See Reference 5.]

Design Information. Design information is the combination of the requirements and the corresponding basis information associated with the engineering design process. [See Reference 7.]

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. This process defines and documents the inputs; adheres to the constraints; performs and documents the necessary analyses, calculations, technical studies and evaluations; and ensures the outputs of the process (i.e., the requirements that dictate a design that satisfies the inputs and constraints) are documented and complete. [See Reference 7.]

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. [See Reference 7.]

Safety Structures, Systems, and Components (Safety SSCs). The set of safety-class SSCs and safety-significant SSCs for a given facility. The definitions for safety-class SSCs and safety-significant SSCs and associated relevant information are provided in DOE-STD-3009-94. [See Reference 8.]

Subsystem. A combination of components, modules, devices, or software within a system which 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 a supporting service to another system that is necessary for the supported system to be capable of meeting its system requirements. For example, an instrument air system may be necessary 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 necessary to maintain the temperature of the environment to within the limits for which some components are rated. In some designs, components or 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 support system being necessary.

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 Engineer. An engineer assigned technical responsibility for a particular system(s) and who coordinates technical activities related to the assigned system(s). The system engineer has technical understanding of the system requirements, design, operation, testing, and maintenance. The system engineer ensures that relevant documents such as system design descriptions, technical drawings, diagrams, lists, and procedures for surveillance, testing, and maintenance are complete, accurate, and up to date. The system engineer may also keep vendor technical information and appropriate files concerning system history of repairs, modifications, operational problems and other unique conditions or circumstances. Equivalent terms include: cognizant engineer, system specialist, and subject matter expert.

Abbreviations and Acronyms

CM	Configuration Management
CRT	Cathode Ray Tube type of display unit or monitor
EIS	Environmental Impact Statement
FMEA	Failure Modes and Effects Analysis
FSAR, or SAR	Final (or Facility) Safety Analysis Report, or Safety Analysis Report
HVAC	Heating, Ventilation, Air Conditioning system
MEL	Master Equipment List
OSR	Operational Safety Requirements
P&ID	Piping and Instrumentation Diagram
QA	Quality Assurance
SDD	System Design Description
SNM	Special Nuclear Material
SSC(s)	Structure, System, or Component(s)
TSR(s)	Technical Safety Requirement(s)

References

This standard does not mandate or otherwise depend on other documents. Reference documents that were considered during the development of this standard are identified in Attachment 3 to this standard.

INTENTIONALLY BLANK

CONTENT OF SYSTEM DESIGN DESCRIPTIONS

Outline of an SDD

SDDs shall adhere to the following outline to the extent that it is relevant to the system being described. When a section of the outline below is not applicable to the system, the section should be retained in the SDD with a simple statement that the section is not applicable. It is preferred that a brief explanation of its non-applicability also be provided, especially if the reason for the non-applicability might not be immediately obvious to some readers. Conversely, the outline might need to be expanded to address aspects of some systems not covered by the outline.

> Note: The outline below is not intended to define some 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 (for example, ventilation/confinement systems, electrical power systems, chemical processes).

CHAPTER 1

Introduction

- **1.1 System Identification**
- **1.2 Limitations of this SDD**
- **1.3 Ownership of this SDD**
- **1.4 Definitions/Glossary**
- **1.5 Acronyms**

CHAPTER 2

General Overview

- **2.1 System Functions**
- **2.2 System Classification**
- **2.3 Basic Operational Overview**

CHAPTER 3

Requirements and Bases

- **3.1 General Requirements**
  - 3.1.1 System Functional Requirements
  - 3.1.2 Subsystem and Major Components
  - 3.1.3 Boundaries and Interfaces
  - 3.1.4 Codes, Standards, and Regulations
  - 3.1.5 Operability
- **3.2 Special Requirements**
  - 3.2.1 Radiation and Other Hazards
  - 3.2.2 ALARA
  - 3.2.3 Nuclear Criticality Safety
  - 3.2.4 Industrial Hazards
  - 3.2.5 Operating Environment and Natural Phenomena
  - 3.2.6 Human Interface Requirements
  - 3.2.7 Specific Commitments
- **3.3 Engineering Disciplinary Requirements**
  - 3.3.1 Civil and Structural
  - 3.3.2 Mechanical and Materials
  - 3.3.3 Chemical and Process
  - 3.3.4 Electrical Power
  - 3.3.5 Instrumentation and Control
  - 3.3.6 Computer Hardware and Software
  - 3.3.7 Fire Protection
- **3.4 Testing and Maintenance Requirements**
  - 3.4.1 Testability
  - 3.4.2 TSR-Required Surveillances
  - 3.4.3 Non-TSR Inspections and Testing
  - 3.4.4 Maintenance
- **3.5 Other Requirements**
  - 3.5.1 Security and SNM Protection
  - 3.5.2 Special Installation Requirements
  - 3.5.3 Reliability, Availability, and Preferred Failure Modes
  - 3.5.4 Quality Assurance
  - 3.5.5 Miscellaneous

(Continued on next page)

CHAPTER 4

System Description

4.1 Configuration Information

- 4.1.1 Description of System, Subsystems, and Major Components
- 4.1.2 Boundaries and Interfaces
- 4.1.3 Physical Location and Layout
- 4.1.4 Principles of Operation
- 4.1.5 System Reliability Features
- 4.1.6 System Control Features

4.2 Operations

- 4.2.1 Initial Configuration (Pre-startup)
- 4.2.2 System Startup
- 4.2.3 Normal Operations
- 4.2.4 Off-Normal Operations
- 4.2.5 System Shutdown
- 4.2.6 Safety Management Programs and Administrative Controls

4.3 Testing and Maintenance

- 4.3.1 Temporary Configurations
- 4.3.2 TSR-Required Surveillances
- 4.3.3 Non-TSR Inspections, and Testing
- 4.3.4 Maintenance

Appendices

- Appendix A Source Documents
- Appendix B System Drawings
- Appendix C System Procedures

Technical Content Guidance

Chapter 1
Introduction of an SDD

The purpose of this section of the SDD is to provide 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 shall identify the boundaries of the system concisely and only to the extent necessary to explain the physical scope of the system that is covered by this SDD and shall identify the interfacing systems that are not covered by this SDD. This subsection is anticipated to be only about one paragraph or so long.

1.2 Limitations of this SDD

This section shall explain any limitations that may exist on the SDD (i.e., on this latest version). 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 at this time, the reader should be informed of this limitation.

1.3 Ownership of this SDD

This section shall identify the owner of the SDD and state that the owner is responsible for the technical content of, and for reviewing changes to, the SDD. The owner is expected in most cases to be the system engineer, but this could vary in different organizational structures. The owner should not be identified by name, because assignments could change. Rather, the SDD should point the reader to a place or document that would identify the specific individual assigned as SDD owner.

1.4 Definitions/Glossary

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

1.5 Acronyms

This section shall define the acronyms used in the SDD.

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 that information necessary to establish a foundation for understanding the requirements and bases information that follows in the SDD. This is a preliminary section; details on the system will be provided later.

2.1 System 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 shall address the areas of safety (protection of onsite and offsite personnel from radiological and other type hazards), environmental protection, programmatic mission, and general functions. Statements of the functions of the system shall 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 authorization basis documents and supporting documents. As discussed in Reference

12, the essential constituents of statements of safety function are:

a. The situations, and any specific accidents, during which the system may be called upon to perform its safety function(s).

b. The specific objective of the system in its role of preventing, detecting, or mitigating undesirable occurrences.

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

Statements of safety functions in the SDD shall be consistent with the corresponding information in the facility authorization basis and specific references to the authorization basis documents shall be provided.

> 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 criteria, safety assessments, evaluation of system performance capabilities, and evaluation of changes.

If all the system functions have been defined, then the overall function or purpose of the system has been defined indirectly also. To avoid potential misunderstandings due to this definition being only implicit, the SDD shall explicitly state the overall function or purpose of the system.

2.2 System Classification

The SDD shall state the overall classification that has been assigned to the system. This classification should have been based on the highest ranking (most important) requirements identified for the system, using the hierarchy presented in Section 3 of this standard. For example, if a system were to have Safety-Significant, Mission-Critical, and General requirements, but no Safety-Class 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 is the subject of the facility OSRs/TSRs.

2.3 Basic Operational Overview

This section shall include a simplified system diagram, including boundaries and interfaces. Where subsystems exist, they shall be illustrated on the simplified system diagram.

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 Section 3.

Chapter 3
Requirements and Bases

This section of the SDD identifies both the requirements on the system and the bases for those requirements. This section shall also present the classification of those requirements with regard to importance, and shall refer to the source documents from which the requirements and bases were obtained.

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: ...." and providing the explanation for this requirement as part of the basis information. In addition, the bases statements should be informative and provide value-added instead of merely re-stating the requirement in different words.

Requirements

System requirements build on and logically support the system functions. For example, a system 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 plus redundancy and diversity requirements, that provide the high reliability for the system.

The requirements and bases to 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 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 can have different levels of importance. For example, some requirements are part of the DOE authorization basis for a facility, and operation of that facility is allowed only if those requirements are complied with (such a requirement can be changed only if prior approval is obtained from DOE). Other requirements may be designer options considered desirable for various reasons and have no bearing on the facility authorization basis. Such requirements may or may not affect operations directly, and may be changed as deemed appropriate by the design authority (which may be the facility management) without approval from others such as site-level contractor management or a regulatory authority. It is important to include all requirements and their bases in the SDD regardless of their source or importance, because the SDD is intended to identify all requirements and bases for a system so that operations and maintenance personnel will have the complete understanding necessary for safe, reliable, and efficient operation of the system.

Categorizing requirements by type, as shown in the outline on page 1, has been found to be useful for identifying information that may be sought quickly for making decisions concerning system Operability and compliance with the authorization basis. This categorization is also helpful for routine searches, for example, it might be necessary to find 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, as shown in the outline on page 1 of this standard. For example, a requirement might say that certain components must go to specified positions (open, or closed) upon loss of electrical power. From one perspective, this might be considered to be an electrical power engineering requirement (Section 3.3.4). From another perspective, 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 and then that section referenced in other sections where the same information becomes pertinent. One approach is simply to place the requirement in the first section in the SDD in which it becomes relevant. Another approach is use engineering judgement to select the most fitting section for the requirement.

Requirements shall 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, shall be used.

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

Requirements classified as Safety-Class or Safety-Significant are those identified as necessary for Safety-Class and Safety-Significant SSCs to accomplish their safety functions, as established as established by the hazards analysis and safety analysis processes. The "Other 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 or the defense-in-depth safety basis for the facility.

The safety requirements statements shall be consistent with, and be explicitly correlated back to, the corresponding statements of functional requirements and performance criteria in the facility FSAR, TSRs/OSRs, and other authorization basis documents, if the authorization basis has already been established for the facility. One convenient way to correlate these requirements is to use footnotes. For example, 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 FSAR (Reference 3 in Appendix A)." An alternate way to correlate these requirements is with a table (for example, a requirements matrix) in a separate Appendix or Attachment to the SDD.

Often the Environmental Protection category is omitted from requirement classification lists. Sometimes environmental protection is taken to be a subset of safety in general. The environmental protection category should be considered separately and explicitly in the SDD in order to make sure that this important set of requirements is not overlooked and to address requirements related to environmental permits.

Mission-critical functions are those that are necessary to prevent or mitigate substantial interruptions of facility operations or severe cost or other adverse impacts, or are necessary to 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 nuclear facilities. This set of classifications, a modified set, or a completely new set of classifications may be used for nonnuclear facilities.

Bases

A major function of the SDD is not only to state the engineering requirements on 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 it is highly desirable that the bases for all requirements be documented in the SDD, it is imperative that the basis information for safety requirements be stated in the SDD.

Technical basis information shall be included directly in the body of the SDD immediately after the requirement, rather than relegate such information to an appendix or refer to another document. However, the basis may be provided in one place for a group of related requirements. 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 175-185°F.

Basis: The setpoint was chosen high enough above 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.

Basis information can take different forms. Specific engineering documents (such as studies, analyses, calculations, and reports) are important basis references. In addition, appropriate and specific references to national codes and standards should be included in the basis references, when appropriate. Operational experience and standard engineering practices are valid reasons that could justify a requirement.

References

Specific references are essential to understanding and using the SDD. References 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 shall 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, that document should be included as a reference.

In some cases, the requirement or basis information is not recorded in a separate document, the documentation no longer exists, or it is not feasible to retrieve such a document. In those cases, the reference should state that a documented reference is not available, so as to avoid potential confusion and wasted effort.

One method of referencing the source documents that has been found to be user friendly is to provide the bibliographical information on the source documents in an Appendix to the SDD. Then footnotes 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. In addition, this technique can 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.

The following sections of this standard have been numbered purposely to correspond to the sections of an SDD, as shown in the outline on page 1, to make this standard easier to use.

3.1 General Requirements

3.1.1 System Functional Requirements

This subsection shall state those functional requirements and their bases, for both safety requirements and non-safety requirements, that are necessary to fulfill the system function statements. If the requirements and bases have already been presented earlier in the SDD (see for example, item c. in Section 2.1), refer to that section rather than repeat the information.

Note: Functional requirements in general relate to how the system functions, performs, behaves, or responds to particular conditions. Non-functional requirements should be addressed in other subsections 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 shall address the system or facility situations to which the system is designed to respond, the expected ambient operating conditions related to those situations under which it must perform its assigned function(s), and the sequence in which certain actions are to be accomplished.

These requirement 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.")

3.1.2 Subsystems and Major Components

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

3.1.3 Boundaries and Interfaces

This section shall identify any requirements (and their bases) that might exist concerning the boundaries of the system being described, with emphasis on the components at the boundaries (for example, 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. Referring to the simplified system diagram in Chapter 2 of the SDD may be useful for this purpose.

The SDD shall identify any requirements (and their bases) that might exist regarding interfacing systems, especially "support systems" (see Glossary, page xi). For example, it might be required that the system be operated on the smooth and reliable electric power available only from an uninterruptible power system. The SDD shall also identify those interface requirements (and their bases) that might exist regarding the need for the system being described to provide support to another system, especially if that support is necessary to the other system.

3.1.4 Codes, Standards, and Regulations

This subsection shall identify those codes, standards, or portions thereof that have been applied to the system. This section shall identify those 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.

To the extent practical, the bases associated with codes and standards shall 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 shall 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.

> Note: In the future, the 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.

A system may need to meet a particular section of, but not the entire, code or standard. Identify only those sections that will be or have been complied with 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 subsection shall similarly identify government regulations that are applicable to the system being described. These include: the Code of Federal Regulations (CFRs), DOE nuclear safety management rules and orders, regulations from other Federal agencies such as the EPA, court orders (if applicable), state laws and regulations, and state permit requirements.

3.1.5 Operability

When the system being described is the subject of TSRs (or OSRs) that require the system to be Operable, this subsection shall state the specific definition of system Operability (i.e., what aspects of this system are required to be capable of performing as intended in order for this system to be formally considered Operable). To the extent that the facility authorization basis, including the OSRs/TSRs, defines Operability specifically for the system, that definition shall be the one stated in the SDD. This subsection shall 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 authorization basis documents such as the FSAR 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).

The purpose of this section is to state the specific Operability conditions that result from applying the general definition of Operability to the system being described. In some cases, a certain portion or feature of a system may be disabled or unavailable, but the system is still capable of successfully completing its required safety function(s) despite the failed portion or feature. Statements of Operability should not be restrictive to the point of requiring the system to be declared inoperable in such a case.

If the system has additional Operability requirements that may have been established by facility management that go beyond those requirements included in the OSRs/TSRs, these shall also be included in this section, but in a manner distinctive from the TSR Operability requirements.

3.2 Specific Requirements

3.2.1 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 necessary level of protection for facility workers, other employees located at the site, and the public. This is the jurisdiction of the facility authorization basis. All system functional requirements assumed in facility authorization basis documents shall be identified if they have not already been presented in the SDD.

This section includes those radiological safety requirements that must be met 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), which is addressed in the next section.

3.2.2 ALARA

This subsection shall identify those requirements that might exist to include 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.

3.2.3 Nuclear Criticality Safety

This subsection shall identify those requirements (and 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 subsection should also reflect things 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.

3.2.4 Industrial Hazards

This subsection shall identify requirements for safety features for hazards that are typically accepted at commercial industrial workplaces. This subsection shall identify Environmental, Safety, and Health (ES&H) requirements pertaining to the system being described related to personnel safety and OSHA considerations.

This subsection is not intended to generate a research project to identify all the features of a piece of equipment that may be related to the safety of personnel operating the equipment. However, 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 subsection provides the information that would help preclude potential future modifications that might compromise features important to protecting employees.

3.2.5 Operating Environment and Natural Phenomena

This subsection shall identify requirements (and their bases) related to the normal environment that the system must be capable of operating under, for example, ambient temperature, humidity, altitude, noise, radiation, electromagnetic or radio frequency interference (EMI/RFI) and vibration.

This section shall 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 Uniform Building Code. This section should address extraordinary design requirements for protection from natural phenomena such as tornadoes, floods, or seismic events. For example, if the system must operate during or following an earthquake, the associated acceleration spectra should be identified.

3.2.6 Human Interface Requirements

This subsection shall 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.

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.

Requirements for alarms that are related to non-safety actions should be similarly described.

This section should identify those requirements that may exist for the design to distinguish indications and alarms that promote the prompt and effective performance of necessary operator safety actions from other indications and alarms. Similarly, this section should identify requirements that may have arisen related to factors such as shapes, colors, or locations of particular indicators, controls, or displays because such features had been identified as important to success by a human interface task analysis or similar types of evaluations.

3.2.7 Specific Commitments

This subsection shall identify commitments that have been made to the DOE or another regulatory agency such as the EPA, and in some cases, 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.

3.3 Engineering Disciplinary Requirements

This section should identify those requirements and bases that are typically related to particular disciplines of engineering.

3.3.1 Civil and Structural

This subsection shall 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 Uniform Building Code. Examples of requirements to be included are anchorage, bracing, or support requirements for equipment (for example, to prevent damage to equipment or injury to personnel).

3.3.2 Mechanical and Materials

This subsection shall identify those mechanical or materials engineering requirements (and their bases) related to the system being described. Such requirements may relate to pumps (for example, type, net positive suction head, flow capacity, discharge pressure), valves (for example, 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.

3.3.3 Chemical and Process

This subsection shall 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, chemical compositions (for example, amount or concentration of impurities allowable). Other requirements might relate to the type of process (that is, continuous or batch, reactive or non-reactive), waste generation considerations, or necessary process evolutions (for example, hold times, agitation rates).

3.3.4 Electrical Power

This subsection shall 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, however, 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 must be capable of performing its function(s) following the loss of normal utility power, and fail-safe states that equipment must assume upon loss of power. Another example is power quality requirements. 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.

3.3.5 Instrumentation and Control

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

This section of the SDD shall 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 shall 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 shall identify the required nominal values of the setpoints associated with the system and ranges of acceptable setpoint values. The basis information shall explain any limitations, either administrative, design, and limits important to safety, that may exist on the system or its components.

3.3.6 Computer Hardware and Software

This subsection shall 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 3.3.5 are also relevant to computer hardware and software. The topics addressed in section 3.3.6 should be those unique to computer hardware and software. Examples of such types of requirements 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 (for example, verification and validation, or qualitative reliability goals), they should be described in this section of the SDD. 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 of the SDD.

> 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 there are requirements related to reliability of commercial off-the-shelf (COTS) hardware or software, they should be described. Such requirements may, for example, 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). Another example would be 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.

3.3.7 Fire Protection

This subsection shall 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 subsection should also identify special types of fire suppression materials, such as the need to use halon in a particular area rather than a water sprinkler system.

3.4 Testing and Maintenance Requirements

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

3.4.1 Testability

This section shall 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 (for example, every 12 months or more often). 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 is addressed in Section 4.3.1.

3.4.2 TSR-Required Surveillances

When the system being described is the subject of TSR/OSR Surveillance Requirements, this subsection shall identify the type(s) of surveillance required (that is, checks, inspections, functional tests, or calibrations); identify how often the surveillance is required to be performed (including any grace period that may be allowed); state the acceptance criteria for each surveillance; and describe those features provided in the design to facilitate those surveillance actions.

3.4.3 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 beyond those specified in the TSRs/OSRs, this subsection shall 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 shall 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 need to be included in this section.

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

3.4.4 Maintenance

This subsection shall identify maintenance activities required to comply with the manufacturer's recommendations or otherwise required to ensure continued reliability. An example is a requirement to periodically replace specified components such as seals or replace lubricants that degrade over time or to replace certain parts that wear out-of-tolerances after a number of cycles or operations, in order to prevent a failure.

3.5 Other Requirements

3.5.1 Security and SNM Protection

This subsection shall identify those requirements (and their bases) that might exist related to general security of the facility or to the need to protect special nuclear materials (SNM). These requirements may impact the design of certain systems. For example, the design of a vault to store special materials 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.

When security or SNM protection requirements apply to a system, their existence shall be identified in the SDD and appropriate references provided for the documents that explain those requirements, subject to the restrictions of classified documents.

3.5.2 Special Installation Requirements

This subsection 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, some equipment may be required to be wall mounted, instead of floor mounted, or to be oriented in a particular direction, or to maintain a minimum bend radius for interconnecting equipment, or locating certain types of components in a fluid system (liquid or air) a minimum distance from a bend or other flow-perturbing component.

3.5.3 Reliability, Availability, and Preferred Failure Modes

This subsection shall 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).

3.5.4 Quality Assurance

This section of the SDD shall 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 deemed to be necessary. When the general QA category provides for options related to specific QA activities, the SDD shall 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.

3.5.5 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 subsections.

Chapter 4
System Description

The SDD shall include a comprehensive description of the system, including both its safety features and non-safety features. The SDD description shall emphasize those features provided to meet the requirements on the system.

This section of the SDD shall 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 must 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 such as the MEL or Bill of Materials that contains this configuration information.

Describe the system with specific values, rather than simply repeating the requirements. For example, suppose a requirement on the system is 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. In describing the system, do not simply repeat the 8 to 14inches requirement, but rather describe the actual installation more specifically, such as the centerline of the suction pipe is 11.25 inches above the bottom of the tank. For a requirement that a valve be provided with position indication that is displayed in the control room, do not simply say that valve indication is provided in the control room. State more specifically that, for example, 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 shall be correlated. One method for this correlation which has been found effective and convenient is to use 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.”

4.1 Configuration Information

4.1.1 Description of System, Subsystems, and Major Components

The detailed system diagram shall 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.

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, bistable 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.

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, 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.

4.1.2 Boundaries and Interfaces

It is important to define the boundaries of the system 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 should encompass all components necessary 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 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 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 is assigned with the pump motor to the pump system. The system boundary for the pump system would 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 that are necessary for the system being described to accomplish its functions are usually considered to 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 are usually not designated as separate systems but rather are most often considered integral portions of

the system being controlled. The system boundaries are then usually 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, signals to actuated equipment, and alarms. For example, an I&C system might include a flow sensor, a signal comparator, and a control signal that would open a valve more if the flow were to be below the desired value, or close the valve if the flow were to be above the desired value. 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.

Interfacing systems need to be defined with the level of detail necessary to ensure proper functioning and necessary support. The most critical of these interfacing systems are "support systems" because they provide services that are necessary to the system being 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 shall 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 shall 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, but 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. This discussion should not be so detailed as to approach an engineering analysis or so simplistic as to not add value to the SDD. This discussion should be developed in coordination with the discussion of the system operational considerations to be provided in Section 4.2 "Operations" in a manner that avoids unnecessary 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, its operation should be summarized because many readers may need to be educated on this type of controller or at least reminded.

4.1.5 System Reliability Features

This section shall 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 shall be discussed. This section should discuss other known failure modes of the system and their affects 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 shall be described.

Where the system includes redundant subsystems or components, the SDD description shall identify these redundant features. The SDD shall 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 necessary, each might be a 50% capacity fan, with two additional 50% fans in standby ready for operation. Also, discuss independence of the redundant features. Any technical limitations on the use of the redundant features shall also be described. For example, while 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 shall 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.

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 shall be described, including types, ranges, and accuracies. This may include indicators, recorders, status lights, CRT 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 provide information to verify compliance with TSRs shall be identified as such.

4.1.6.2 Control Capability and Locations

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

4.1.6.3 Automatic and Manual Actions

The SDD shall 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 must be closely monitored

Where alarms are provided that are intended to trigger manual safety actions, the SDD shall 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. Here again, 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 unnecessary overlap and repetition.

4.1.6.4 Setpoints and Ranges

This section of the SDD shall identify setpoints associated with the system (including pre-trip

alarms) and the purpose of the setpoints. The values of setpoints and other system limitations shall be correlated with the system requirements, especially TSR-required setpoints.

> Note: It is common practice to include 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 needs to 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 need to be specified in actual values, not as tolerances, percentages, or other approaches that necessitate calculations.

It may be advantageous not to repeat setpoint data in the SDD 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, a reference shall be provided to the separate document that contains 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. It is not necessary to identify all adjustments in the SDD; however, some setpoints will affect the limits of performance of the equipment and should be made known to the operators. 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 shall 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 shall be listed. Provisions for manually disabling, bypassing or otherwise altering system performance, and the conditions and limitations under which they are to be used shall be identified and explained.

4.2 Operations

In this section, where operations personnel have voluntarily adopted good practices related to the operation of the system, those practices should be identified. 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 must be verified (for example, by system walkdown or status checks) to be 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: Previously, the use of footnotes and bibliographical information in an Appendix has been discussed with regard to referring to system requirements and source documents. In a similar manner, footnotes should be used to refer to procedures for system operations.

4.2.2 System Startup

This section shall 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 generally how mode changes are accomplished. A reference shall 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 describe the most frequently used mode of operations, including routine checks on system performance and performance data logging that are performed by the operations staff to verify that the system is operating normally, including the key parameters and their nominal values. Those surveillance actions preformed by maintenance staff should be identified in Section 4.3.

This section should also 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 subsection shall identify off-normal conditions for 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, the impact on the facility).

This section should briefly summarize 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 those less urgent follow-up actions that are appropriate to that alarm. This section should provide a reference to the appropriate documents for recovery actions.

4.2.5 System Shutdown

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

4.2.6 Safety Management Programs and Administrative Controls

This subsection shall 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 shall be identified in general terms.

4.3 Testing and Maintenance

In this section, where maintenance personnel have voluntarily adopted good practices related to the system, those practices should be identified. 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 shall be identified and described in the SDD. The SDD shall state the operational limitations on the use of those configurations and shall refer to the applicable governing procedures.

In some cases, it is necessary to use temporary configurations in order 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, there are operational limitations on the use of such temporary configurations that 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. It might be necessary to provide compensatory measures during the time some equipment is not operable or 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/OSR 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/OSR inspection, testing, or 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 shall provide references to the implementing procedures.

4.3.4 Maintenance

This subsection of the SDD 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 system engineer in the role of being responsible for all aspects of the system, which includes testing and maintenance actions.

The SDD shall summarize the routine actions required by preventive maintenance procedures and post-maintenance testing procedures. This section may also provide references to appropriate maintenance procedures.

4.3.4.1 Post-Maintenance Testing

This section shall explain the extent to which a post-maintenance testing program is applied to the system being described. Key performance or acceptance criteria that must be satisfied or verified during post-maintenance testing (for the system to fulfill its functions such as those identified in the hazards and accident analyses) shall be identified. The SDD should also provide appropriate references to post-maintenance testing procedures.

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, extreme care is necessary to ensure that change activities are recognized as different from maintenance. The SDD shall explain the extent to which a post-modification testing program applies to the system being described.

4.4 Supplemental Information

Some contractors 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 of the SDD may include the following topics:

a. Summary of potential system and component failures (and reference to a Failure Modes and Effects Analysis (FMEA) or similar analysis if one exists)
    - Failure Modes
    - Probability/Likelihood
    - Consequences (effects of failures)
    - 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 shall contain the bibliographical information for documents that are referenced in the body of the SDD. It may be decided to provide separate appendices for documents of various types, such as: design documents, procurement documents, vendor documents, etc. or it may be decided to subdivide a single appendix into subsections that address different document types.

Appendix B: System Drawings and Lists

This appendix shall 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 might 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.

Additionally, Master Equipment Lists, Parts Lists, Bill of Materials, and lists showing the hierarchy of drawings that are pertinent to the system being described should be identified.

To avoid unnecessary revisions of the SDD, this tabulation of the system drawings should not include specific revision numbers/letters nor 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. 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 (such as, design change packages or work packages) referenced. System history information may be kept

in separate referenced files or in the SDD, but it should be kept.

INTENTIONALLY BLANK

Attachment 1

Application of the Graded Approach to the Development of SDDs

The graded approach provides substantial flexibility for the development of SDDs that can be meshed with the 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 the phased approach to such developments.

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 categorization 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, it might be decided, 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, it might be decided, for example, that SDDs will be developed only for safety SSCs. At a Hazard Category 3 nuclear facility, it might be decided, for example, that separate SDDs would not be developed, but instead an FDD would be developed which 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.

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 operational lifetime of the facility is only a couple years, it might be concluded that the development of SDDs is not worthwhile.

SSC CLASSIFICATION

The systems within the facility should be classified in accordance with DOE-STD-3009. The system importance classification should be used to determine which systems need to have SDDs developed. All safety SSCs should have SDDs developed (Safety SSCs include both Safety-Class SSCs and Safety-Significant SSCs). Serious consideration should also be given to developing SDDs for environmental-protection and mission-critical Systems.

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 involved in developing 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 its requirements, bases, and operational aspects.

Another way in which the graded approach can be applied to the development of SDDs is the level of effort that would be expended in retrieving, compiling, and assembling existing design information (that is, requirements and bases information). See Attachment 2 to this standard.

The topics that need to be addressed in an SDD may be adjusted using the graded approach. The most important systems would have SDDs that are the most comprehensive. Less important systems might not warrant the cost of developing such comprehensive SDDs. For example, sections of the outline such as "Operations" (Section 4.2) and "Testing and Maintenance" (Section 4.3) might be considered for omission.

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 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 only one short paragraph or simply a reference to appropriate procedures. This is particularly pertinent with regard to Section 4 of the SDD.

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

PHASED APPROACH

In addition to the decisions regarding which systems warrant SDDs and the extent of the content of particular SDDs, another important 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.

The content of the SDDs might be scheduled for development in stages. For example, the most important sections of the SDD (such as the System Requirements and Bases) would be developed for all SDDs during the first phase and issued as Revision 0 of those SDDs. Then during the subsequent phase, those SDDs would be revised (completed) by developing the remaining sections (such as the System Description) and issuing them as Revision 1 of the SDDs.

Attachment 2

Compiling Technical Information for the Development of SDDs

A key variable in determining the level of effort that the development of an SDD will involve is the amount of effort that goes toward locating, screening, reviewing source documents, and extracting the desired information from them. This effort could range from almost nothing to a project that requires substantial effort. Obviously, the more technical information that is used, the better the quality and usefulness of the resulting SDD. However, because the costs and schedule will tend to grow, facility management will need to make a decision regarding the level of effort. This attachment provides information that can help with that decision.

AVAILABILITY OF DESIGN INFORMATION

There may be a perception that existing DOE nuclear facilities have little or no design information available (that is, requirements and basis), that it would be prohibitively expensive to retrieve, and would probably not be relevant to the current facility configuration. There may also be the perception that only new facilities have any design information available.

These perceptions are not completely accurate. 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 have a fair amount of design information still on-hand or reasonably retrievable. In some cases, 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 is true for modifications to existing facilities. The situation varies widely, however. At a few facilities, there is almost no information available. At some, 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, a vast amount of information is available that is highly trustworthy.

Whether a facility is a new facility or an "existing" facility is not a significant factor, but rather more directly the amount of design information necessary, and whether that information is on-hand or can be retrieved within reasonable efforts.

THE DOE-STD-3009 APPROACH

DOE-STD-3009-94 provides a sound approach to establishing the important technical requirements for safety SSCs that are used in the development of upgraded FSARs to meet DOE 5480.23. 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 necessary functional requirements as part of the process hazards analysis effort in sufficient detail to support the safety analysis. Documented engineering judgements (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 strongly recommended.

DOCUMENT RETRIEVAL

Efforts to retrieve design information have sometimes been limited to search 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 not 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. This is the concept of a “smart search.” With a very small effort, it is usually possible to identify those locations that are most likely to have the desired information. A few telephone calls could be made to long-term employees to find out where the most fruitful places to look are. For example, someone may remember a packrat engineer who never throws away anything and his file cabinets are rich; someone in program management who has the files on old projects; or someone in document control center. When these few most productive locations have been searched, the “smart search” is complete.

An important management consideration is to know when to stop. How will we know when we have searched long enough? To facilitate answering this question, it is necessary to understand the information that is needed and the types of documents that are likely to contain the information. The information required is indicated by "shall" statements in the body of this standard. Engineers who have had design experience with large engineering firms can usually tell us what types of documents are typically 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 information.

REVIEWING RETRIEVED DOCUMENTS

The system engineer (cognizant facility engineer) can easily and quickly ascertain which of the retrieved documents contain information that is applicable to the current configuration of the facility. This can sometimes be accomplished on the basis of the date of the document and a knowledge of previous system modifications.

A question arises about what would we do with the documents that are not related to the current SDD task. Some suggest merely casting those documents aside or sending them to Records Management for storage. A better approach might be to make a list of the documents found, to avoid having to re-scan this location during future tasks. For example, when the next SDD is being developed, we might need some more information from that location. An even better approach 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.

Having retrieved some documents related to the system at hand, how might we sort that information? One approach is to 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).

The next step would be to review the documents and extract the design information. Experience indicates that when important relevant design information is found, it will likely contain both requirement information and basis information.

The information is not likely segregated as safety design information and non-safety design information. So what do we do with the non-safety information? Having completed the search and located the information in

specific documents, it would seem senseless not to use it just because it is not-safety-related. The majority of the cost of retrieving the information has already been spent, so it would be very cost-effective to include this non-safety information in the SDD, also. Besides, SDDs are not limited in scope to safety-related information.

RESOLVING CONFLICTING INFORMATION

Invariably it seems, we will find that some information in one source document does not agree with information in another source document. Fortunately, most of the time, these conflicts can be quickly resolved. For example, 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 these cases the conflict should be formally documented and tracked until it is resolved. It is recommended that a log of Open Items for the SDD be kept for this purpose.

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. The discrepancies need to be reviewed also to determine if any impact "Operability" of any systems, or might be "reportable occurrences." Open Items that are not safety-significant, but involve critical information that could have an adverse impact on facility operations should also be formally tracked to closure.

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, do not invest any more time and money into perfecting the data bank. If the missing information is truly critical, a plan must be developed to recover that information. Here again, the DOE-STD-3009 approach to the problem may be valuable. In a few cases, calculations or analyses might have to be regenerated.

INTENTIONALLY BLANK

Attachment 3

Developmental References

This Attachment identifies documents that are considered during the development of this standard, either directly or indirectly, and provides the bibliographical information that might be needed to retrieve these documents for background information purposes.

1. DOE 5480.19 "Conduct of Operations Requirements For DOE Facilities," 7-9-90, Change 1: 5-18-92.

2. DOE 5480.21 "Unreviewed Safety Questions," 12-24-91.

3. DOE 5480.22 "Technical Safety Requirements," 2-25-92, Change 1: 9-15-92, Change 2: 1-23-96.

4. DOE 5480.23 "Nuclear Safety Analysis Reports," 4-10-92, Effective Date: 4-30-92, Chg 1: 3/10/94.

5. DOE 5700.6C "Quality Assurance," 8-21-91.

6. 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.

7. DOE-STD-1073-93 "Guide for Operational Configuration Management Program," Part 1 and Part 2, November 1993.

8. DOE-STD-3009-94 "Preparation Guide for U. S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports," July 1994

9. DOE Office of Field Management Good Practice Guide GPG-FM-012 "Configuration and Data Management," April 1996.

10. DOE Office of Defense Programs "Interim Guidance on Authorization Basis," Revision 1, August 21, 1995.

11. DOE Office of Defense Programs Safety Information Letter (SIL) No. 95-04 "Management of Safety Analysis Report Information Using Standard Configuration Management Practices," June 1995.

12. DOE Office of Defense Programs Safety Information Letter (SIL) No. 96-04 "Improved Safety Function Definition in Safety Documentation For Nuclear Facilities," September 1996

13. Electronic Industries Association (EIA) document EIA/IS-632 "EIA Interim Standard: System Engineering," December 1994

14. Electronic Industries Association (EIA) document EIA/IS-649 "EIA Interim Standard: National Consensus Standard for Configuration Management," August 1995.

15. International Organization for Standardization (ISO) document ISO 10007:1995 "Quality Management — Guidelines for Configuration Management," First Edition, April 15, 1995.

INTENTIONALLY BLANK

CONCLUDING MATERIAL

Project Number:	Preparing Activity:	Preparing Agent:
EDCO-0001	DOE-DP-45 Mr. John Fredlund Mr. Rick Kendall	J. T. BEARD, INC. ENGINEERING CONSULTANT

Review Activity:

DOE-HQ	DOE Field Offices	DOE Area Offices	DOE Other
EE	ALO	Amarillo	Bonneville Power Administration
EH	CHO	Fermi	Fernald Environmental Management
EM	GFO	Kansas City	Grand Junction Project Office
ER	IDO	Kirtland	Morgantown Energy Technology Center
FE	OAK	Los Alamos	Pittsburgh Energy Technology Center
GC	OHO	Miamisburg	Western Area Power Administration
IG	ORO	Sandia	
NE	RFO	West Valley	
NN	RLO		
PO	SRO		
RW	NVO		

National Laboratories

Ames Laboratory
Argonne National Laboratory
Brookhaven National Laboratory
Energy Technology Engineering Center
Fermi National Accelerator Laboratory
Idaho National Energy & Environmental Laboratory
Lawrence Berkeley National Laboratory
Lawrence Livermore National Laboratory
Oak Ridge National Laboratory
Pacific Northwest National Laboratory
Princeton Plasma Physics Laboratory
Stanford Linear Accelerator Laboratory

DOE M&O Contractors

Lockheed Martin Energy Services
Mason & Hangar Company
Oak Ridge Associated Universities
Westinghouse Savannah River Company

DOE F 1300.3
(01-94)

U.S. DEPARTMENT OF ENERGY

DOCUMENT IMPROVEMENT PROPOSAL

(Instructions on Reverse)

OMB Control No.
1910-0900
OMB Burden Disclosure
Statement on Reverse

1. Document Number	2. Document Title

3a. Name of Submitting Organization	4. Type of Organization *(Mark one)*
	☐ Vendor ☐ User ☐ Manufacturer ☐ Other (Specify: _____)
3b. Address *(Street, City, Zip Code)*	

5. Problem Areas (Attach extra sheets as needed.)

a. Paragraph Number and Wording

b. Recommended Wording

c. Reason/Rationale for Recommendation

6. Remarks

7a. Name of Submitter *(Last, First, MI)*	7b. Work Telephone Number *(Include Area Code)*
7c. Mailing Address *(Street, City, State, Zip Code)*	8. Date of Submission