
SYSTEM DESIGN DESCRIPTIONS	Manual	Engineering
	Document	TFC-ENG-DESIGN-P-07, REV C-2
	Page	1 of 18
	Issue Date	September 29, 2015

TABLE OF CONTENTS

1.0 PURPOSE AND SCOPE 2

2.0 IMPLEMENTATION 2

3.0 RESPONSIBILITIES 2

4.0 PROCEDURE 2

 4.1 General 2

 4.2 System Design Description Development 2

 4.3 Preparation of System Design Description Changes 4

 4.4 System Design Description Revisions 4

5.0 DEFINITIONS 5

6.0 RECORDS 5

7.0 SOURCES 5

 7.1 Requirements 5

 7.2 References 5

LIST OF FIGURES

Figure 1. Flowchart of System Design Descriptions. 6

LIST OF ATTACHMENTS

ATTACHMENT A - APPLICATION OF THE GRADED APPROACH TO THE DEVELOPMENT OF
SDDs 7

ATTACHMENT B – REVIEW CRITERIA FOR SDD REVIEWS 9

1.0 PURPOSE AND SCOPE

(7.1.1, 7.1.2, 7.1.3)

This procedure establishes the responsibilities and methods for the development and control of system design descriptions (SDDs) and the change control of SDDs.

2.0 IMPLEMENTATION

This procedure is effective on the date shown in the header. System Design Descriptions that have been prepared or are in process may continue according to the previous revision. Refer to TFC-ENG-DESIGN-C-25 for other implementation considerations such as document numbers, reviews, approvals and document release.

3.0 RESPONSIBILITIES

Responsibilities are contained within Section 4.0.

4.0 PROCEDURE

4.1 General

SDD text, figures, and drawings are created and maintained by the assigned system engineer. Any revisions to text, figures, or drawings shall be processed using a change document prepared in accordance with TFC-ENG-DESIGN-C-25.

4.2 System Design Description Development

- | | |
|---------------------|---|
| Chief Engineer | 1. Determine systems for which an SDD must be prepared using the Application of the Graded Approach to the Development of SDDs contained in Attachment A. |
| Engineering Manager | 2. Assign the responsible system engineer for each SDD to be prepared. |

NOTE: DOE-STD-3024-98 can be used as a guide for identification of system boundaries.

- | | |
|---------------------------|---|
| Cognizant System Engineer | 3. Identify the appropriate boundaries for the system. |
| | 4. Interface with other responsible system engineers, as necessary, to ensure all interface equipment is covered based upon boundaries. |
| | 5. Create a system boundary illustration ensuring that associated SDD equipment boundaries are identified and incorporated. |

6. Gather appropriate information to develop the SDD, including, but not be limited to:
 - Drawings
 - Calculations
 - Specifications
 - Documented Safety Analysis
 - Technical Safety Requirements
 - Safety Analysis documentation
 - Operational Specification Documents
 - Authorization Basis Agreement information on Safety Basis, Requirements Basis and Environmental Basis.

NOTE: This template was developed for the WRPS SDDs using DOE-STD-3024-98 as a guide.

7. Develop the SDD using the template on the SDD web page.
8. Identify the appropriate technical reviewers and/or subject matter experts in accordance with TFC-ENG-DESIGN-C-52, and distribute the document for review.

NOTE: Reviewers must include appropriate Engineering Discipline Leads, Nuclear Safety staff, and alternate (back-up) assigned system engineer. Comments may be in the form of a redline markup of the document.

- | | |
|---------------------------|---|
| Reviewers | 9. Review the SDD in accordance with the review criteria provided in Attachment A, and provide comments to the responsible system engineer. |
| Cognizant System Engineer | 10. Resolve comments with reviewers and incorporate changes, as necessary. |
| Engineering Manager | 11. Review and approve the SDD. |
| Cognizant System Engineer | 12. Issue the SDD in accordance with TFC-ENG-DESIGN-C-25. |

4.3 System Design Description Revisions

- | | |
|---------------------------|--|
| Cognizant System Engineer | <ol style="list-style-type: none">1. Determine the requirement for revision of the SDD using the following criteria:<ul style="list-style-type: none">• There are more than three Document Modification and/or work-completed Facility Modification engineering change documents outstanding against the SDD,• A Document Modification, work-completed Facility Modification, or other change document (e.g., safety basis change, regulatory requirement change, or technical basis change) has been issued which impacts the SDD and which is significant enough to require immediate revision of the SDD, or• It has been more than two years since the last revision and there is at least one implemented change document outstanding against the SDD.2. Develop the SDD revision ensuring compliance with the template on the SDD web page.3. Ensure boundaries have not changed as a result of the revision or revise boundary illustrations to ensure consistency.4. Ensure the SDD revision is consistent with the following but not limited to:<ul style="list-style-type: none">• Drawings• Calculations• Specifications• Documented Safety Analysis• Technical Safety Requirements• Safety Analysis documentation• Operational Specification Documents• Other interfacing SDDs.5. Send the SDD revision out for review. |
|---------------------------|--|

NOTE: Reviewers must include appropriate Engineering Discipline Leads and Nuclear Safety.

- | | |
|---------------------|--|
| Reviewers | <ol style="list-style-type: none">6. Review the SDD in accordance with the review criteria provided in Attachment A and resolve any comments with the responsible system engineer. |
| Engineering Manager | <ol style="list-style-type: none">7. Review and approve the SDD and resolve any comments with the responsible system engineer. |

Cognizant System
Engineer

8. Issue the SDD in accordance with TFC-ENG-DESIGN-C-25.

5.0 DEFINITIONS

No terms or phrases unique to this procedure are used.

6.0 RECORDS

The following records are generated during the performance of the procedure:

- System Design Description.

The records custodian identified in the Company Level Records Inventory and Disposition Schedule (RIDS) is responsible for record retention in accordance with TFC-BSM-IRM_DC-C-02.

7.0 SOURCES

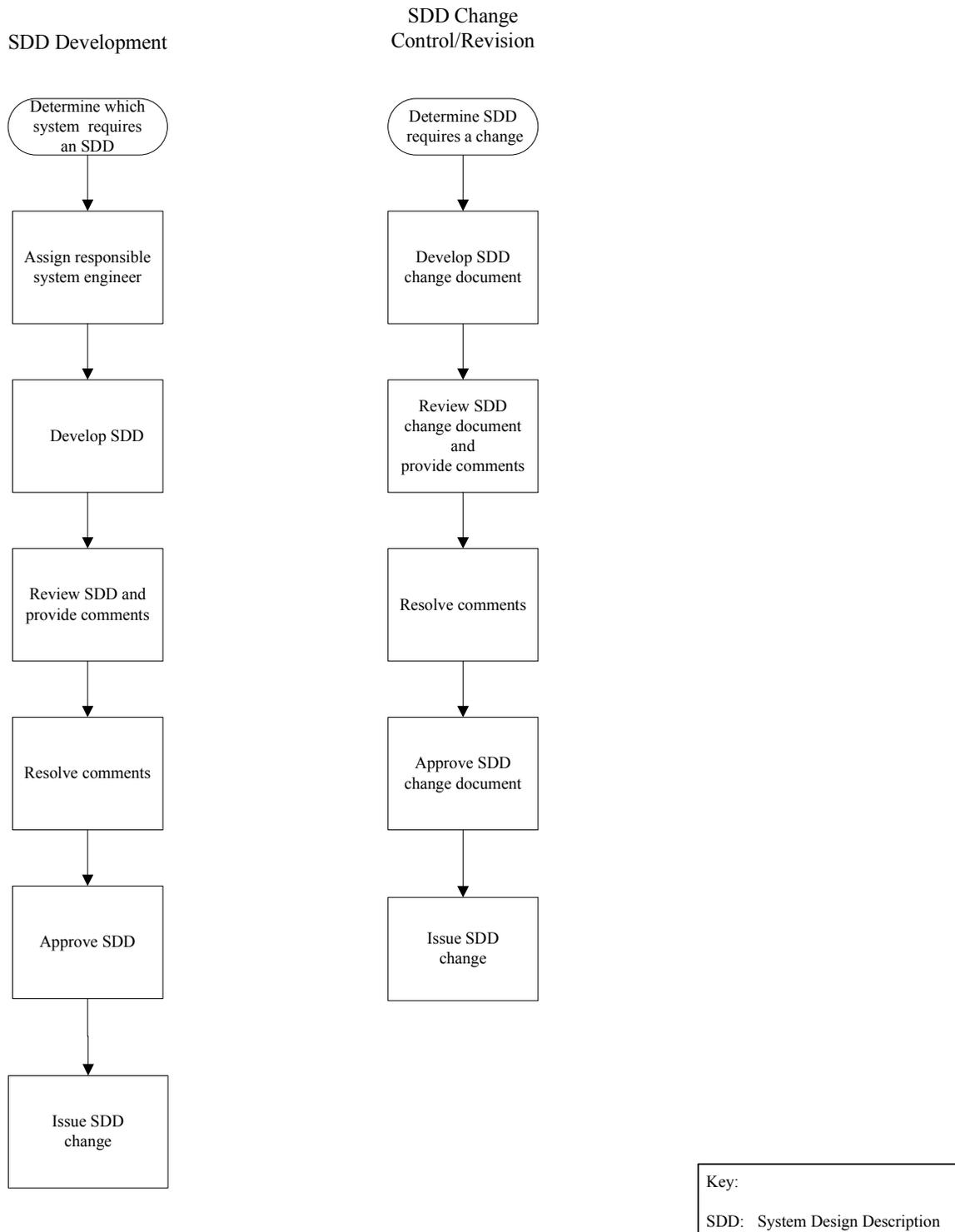
7.1 Requirements

1. RPP-13033, "Tank Farms Documented Safety Analysis."
2. DOE-STD-1189-2008, "Integration of Safety into the Design Process."
3. DOE O 420.1B, "Facility Safety."

7.2 References

1. DOE-STD-3024-98, "Content of System Design Descriptions."
2. TFC-BSM-IRM_DC-C-02, "Records Management."
3. DOE-STD-3009-94, Change Notice No. 3, "Preparation Guide for U. S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses."
4. TFC-ENG-DESIGN-C-06, "Engineering Change Control."
5. TFC-ENG-DESIGN-C-25, "Technical Document Control."
6. TFC-ENG-DESIGN-C-52, "Technical Reviews."

Figure 1. Flowchart of System Design Descriptions.



ATTACHMENT A - APPLICATION OF THE GRADED APPROACH TO THE DEVELOPMENT OF SDDs

INTRODUCTION

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.

**ATTACHMENT A - APPLICATION OF THE GRADED APPROACH TO THE
DEVELOPMENT OF SDDs (cont.)**

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). 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” and “Testing and Maintenance” 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 be addressed. For important systems, a particular topic in the outline may warrant a page or more of discussion. For a less important system, that same topic may warrant 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 B – REVIEW CRITERIA FOR SDD REVIEWS

Introduction

This document identifies the review criteria to be used by the reviewers of system design descriptions (SDDs). The criteria presented in this attachment were developed using the guidance contained in DOE-STD-3024-98 for content of SDDs. The chapter notes identify the content required in each of the SDD chapters/sections and lists the required order of contents. In the text that precedes each chapter, notes have been added identifying the particular focus areas to be used by each of the reviewers when reviewing the SDDs.

REVIEW CRITERIA

Notes to reviewers for table of contents and chapters 1 and 2:

- a) *System engineers and Engineering Discipline Leads – review all aspects of the text for correctness.*
- b) *All other reviewers confirm system overview (chapter 2) is correct.*

Table of Contents

- Confirm table of contents goes down to the fourth level of detail, e.g., 4.3.1.1
- Confirm table of contents, appendices, and figures are correctly numbered.

Chapter 1, Introduction

- Ensure correct system is identified and described. Sections 1.2, 1.3, 1.4, and 1.5 are boilerplate and should not need checking.

Chapter 2, General Overview

- Section 2.1 – Confirm major system functions are correctly identified and are sequenced - process, safety, environmental, and support.
- Section 2.2 – Ensure the system classification is correct, clearly identified, and that the current classification is the first bullet in the section. This section should also include a simple positive or negative statement indicating whether the system is subject to TSRs.
- Section 2.3 – Basic Operational Overview. This should be a simplified “overview” of the system provided to give the reader enough information to facilitate understanding of chapters 3 and 4. It should include (or reference) a simplified System Boundary Drawing that clearly identifies the extent of the system being described.

ATTACHMENT B – REVIEW CRITERIA FOR SDD REVIEWS (cont.)**Notes to Reviewers (Initial Review) – Chapter 3:**

- a. *System engineers, Engineering Discipline Leads, process engineers, and Nuclear Safety engineer – review all aspects of the text for correctness.*
- b. *Nuclear Safety - general overview, particular attention to 3.1 and 3.2.*
- c. *Environmental - general overview, particular attention to 3.1.4.*
- d. *Operations - general overview, particular attention to 3.1.5.*
- e. *Maintenance/Work Control - general overview, particular attention to 3.4.*

Chapter 3, Requirements

Section is to describe the system requirements, basis for these requirements, and how the design satisfies these requirements. Note that requirements are to start at a high level (imposed requirements) in Sections 3.1 and 3.2 (functional requirements etc.) and flow to derived design requirements in Sections 3.3, 3.4, and 3.5.

- **Section 3.1 – General Requirements**

Confirm this section states the general functional requirements and basis to fulfill the system functional statements stated in section 2.1. Functional requirements are to describe how the system functions, behaves, or responds to particular conditions and should include acceptance criteria/limits to determine if the requirement has been met. General functional requirements are to be listed in the following order:

- Section 3.1.1 – System functional requirements. These must support the system functions identified in Section 2.
- Section 3.1.2 – Subsystems and major components. List all the subsystems and major components.
- Section 3.1.3 – Boundaries and interfaces. Identify any requirements concerning boundaries with emphasis on components (e.g., boundary to be upstream of instrument air valve).
- Section 3.1.4 – Codes, standards, and regulations. Identify codes and standards that have been applied. If the requirements of applicable standards were tailored, include a justification that demonstrates the adequacy of the final design with the tailored requirements. (7.1.2)
- Section 3.1.5 – Operability. Where applicable state TSR definition of operability. TSR definition may be expanded if additional guidance is needed.

ATTACHMENT B – REVIEW CRITERIA FOR SDD REVIEWS (cont.)

- **Section 3.2 – Specific Requirements**

- Section 3.2.1 – Radiation and other hazards. Confirm this section states the safety requirements and their basis for radiation/chemical hazards over and above normal OSHA requirements. (These will be identified in the DSA).
- Section 3.2.2 – ALARA. Confirm identification of any specific ALARA requirements (increased shielding, etc.) identified by cost benefit analysis.
- Section 3.2.3 – Nuclear criticality safety. Confirm identification of any requirements relating to design features included to prevent nuclear criticality. Ensure the Criticality Safety Representative reviews this section for completeness.
- Section 3.2.4 – Industrial hazards. Confirm identification of requirements for any prominent safety features (ES&H or OSHA), e.g., guards on rotating equipment, NFPA classified flammable gas hazards (see TFC-ENG-STD-45).
- Section 3.2.5 – Operating environment and natural phenomena. Confirm identification of requirements for normal operating environment (temperature, humidity, noise, radiation, vibration etc.). List is to contain those requirement above and beyond UBC codes, i.e., seismic, floods, tornadoes.
- Section 3.2.6 – Human interface requirements. Confirm identification of requirements for enhanced system/operator interface (alarms that trigger human intervention, etc.). Should include details of alarm significance (e.g., red, yellow, green, audible).
- Section 3.2.7 – Specific commitments. Confirm identification of any specific commitments made (to ORP or EPA etc.). These should be listed as requirements. For example (due to a past incident) all valves will have positive position indicators.

- **Section 3.3 – Engineering Requirements**

In this section confirm the identification of requirements specific to an engineering discipline.

- Section 3.3.1 – Civil and structural. Typical requirements might be those in the uniform building code.
- Section 3.3.2 – Mechanical and materials. Typical requirements for pumps might include construction materials, net positive suction head, flow rate, discharge pressure, etc.
- Section 3.3.3 – Chemical and process. Typical requirements might include temperature/pressure limits, concentrations, chemical composition, ph, and feed rates.
- Section 3.3.4 – Electrical power. Typical requirements might include distribution requirements, uninterrupted service, AC/DC voltage, current, frequency, or quality.

ATTACHMENT B – REVIEW CRITERIA FOR SDD REVIEWS (cont.)

- Section 3.3.5 – Instrumentation and control. Focus is to be on hardware I&C controls (see section 3.3.6 for computer hardware/software). Typical requirements might include manual/automatic actions for system initiation and control, indicators, alarms, etc., including required ranges and accuracies. Specifically identify instrumentation that is subject to TSRs. Also identified should be setpoints associated with the system and ranges of acceptable setpoint values. The basis information should explain any limitations, either administrative, design, or limits important to safety, that may exist on the system or its components.
- Section 3.3.6 – Computer hardware and software. Review computer hardware and software requirements. Examples of such types of requirements include: sample rates, real-time performance, data communications, and provisions for backing up programs and data. Requirements for the design and development process for computer hardware and software aspects of the system being described (e.g., verification and validation, or qualitative reliability goals), should be described here. Key design documentation (i.e., the software requirements specification) should be referenced.
- Section 3.3.7 – Fire protection. Review 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.
- **Section 3.4 – Testing and Maintenance Requirements**
 - Section 3.4.1 – Testability. Review any identified requirements (and bases) that exist for features that make the system testable, especially those that preclude the need to install temporary configurations. 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. When the system being described is the subject of TSR Surveillance Requirements, this subsection should 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.
 - Section 3.4.1 – Maintainability. Review identified maintenance activities required to comply with the manufacturer’s recommendations or otherwise required to ensure continued reliability. Typical example is a requirement to periodically replace specified components such as seals or replace lubricants that degrade over time.

ATTACHMENT B – REVIEW CRITERIA FOR PHASE 1 SDD REVIEWS (cont.)

- **Section 3.5 – Other Requirements**

- Section 3.5.1 – Security and SNM protection. Review any requirements related to general security of the facility or to the need to protect special nuclear materials (SNM). 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.
- Section 3.5.2 – Special installation requirements. Review 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, physical separation between redundant equipment, location requirements to minimize equipment interferences, and “free space” requirements for maintenance access.
- Section 3.5.3 – Reliability, availability, and preferred failure modes. Review requirements for any design elements provided to 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. Typical examples include equipment redundancy, diversity, physical separation, and electrical isolation.
- Section 3.5.4 – Quality assurance. Review any identified general category of QA to be applied to the system as a whole and to components of the system. Also identified should be any specific QA activities. When specific QA requirements, such as witnessing vendor testing, are applicable only to certain components, those requirements should be identified.
- Section 3.5.5 – Miscellaneous Requirements. Review any miscellaneous requirements.

Notes to reviewers – Chapter 4:

- System engineers, Engineering Discipline Leads, Operations - Review all aspects of the text for correctness.*
- Nuclear Safety - General review, particular attention to 4.1.5, 4.1.6, 4.2.4, 4.2.5, 4.2.6, 4.3.2 and 4.4.*
- Environmental - General review, particular attention to 4.1.4, 4.1.5, 4.1.6, and 4.2.*
- Process - General review, particular attention to 4.1.6, 4.2, and 4.4.*
- Maintenance/Work Control - General review, particular attention to 4.3.*

ATTACHMENT B – REVIEW CRITERIA FOR PHASE 1 SDD REVIEWS (cont.)**Chapter 4 – System Description**

Confirm this chapter includes a comprehensive description of the system, including both its safety features and non-safety features. The text should emphasize those features provided to meet the requirements of the system. Components should be identified including their physical layout and interconnection with other components. The system flow paths, indicators, controls, and alarms should be described including acceptable ranges for system performance and setpoints. System operation should also be described. The MEL should be referenced as the source of detailed component information (e.g., manufacturer/model number).

- **Section 4.1 – Configuration Information**

- Section 4.1.1 – Description of system, subsystems, and major components. Confirm a system diagram is included in this section to identify the components and interconnections. The diagram must include interfacing equipment and systems. A P&ID (or similar) may serve as a system diagram.
- Section 4.1.2 – Boundaries and interfaces. Confirm the precise boundaries of the system are stated. These 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 control boundaries. Mechanical boundaries should be based on components and should be isolation points (valves and dampers etc.). System boundaries should extend out to and include isolation devices. Electrical boundaries are usually located at circuit breakers. Interfacing systems, particularly support systems, need to be defined with the level of detail sufficient to ensure correct functioning and necessary support are provided.
- Section 4.1.3 – Physical layout. Confirm this section describes where the equipment is installed (tank farm, building, room number, etc.) and its physical arrangement within that space. Any special features regarding the installation, location or arrangement of the equipment should be explained.
- Section 4.1.4 – Principles of operation. Confirm this section describes how the system operates with an emphasis on how the system accomplishes its required functions. Description should use the walk-down approach referring to and following the system and subsystem flow paths in the diagram. The full capacities of the installed system should be described.
- Section 4.1.5 – System reliability features. Confirm text describes all attributes, features, design or operating characteristics, and other information important to the reliability of the system. Typical examples would be preferred failure modes, fail-safe mechanisms, installed redundant plant etc. Any failure modes and effects analysis should be referenced.

ATTACHMENT B – REVIEW CRITERIA FOR PHASE 1 SDD REVIEWS (cont.)

- Section 4.1.6 – System control features. Confirm this section describes the indication, alarm, and control features used to operate the system and monitor its performance. Control logic diagrams should be provided. Location of items should be clearly identified including types, ranges, accuracies, and setpoints. Instrumentation subject to TSRs or provides information to verify compliance to TSRs shall be identified as such.
- **Section 4.2 – Operations**

Confirm this section summarizes the startup, normal, abnormal, and emergency operating processes/procedures. Assigned equipment nomenclatures and equipment labeling should also be defined.

 - Section 4.2.1 – Initial configuration (pre-startup). Confirm text describes if systems must be verified (for example, by system walkdown or status checks) to be in the correct configuration for system operation prior to those systems being started. When this is the case, confirm SDD describes the pre-startup configuration in general terms and provides a reference to the applicable procedure(s).
 - Section 4.2.2 – System startup. Confirm this section summarizes the key steps in the startup procedure and refers 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.
 - Section 4.2.3 – Normal operations. Confirm this section identifies all the normal operating modes of the system, describes when each mode is appropriate, and generally how mode changes are accomplished. A reference should be provided to the procedures that cover system operations, including operational mode changes. A footnote referring to a procedure reference in the appropriate SDD appendix may be used. 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 performed 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. It 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 the system is functioning might be required (if so reference procedure).

ATTACHMENT B – REVIEW CRITERIA FOR PHASE 1 SDD REVIEWS (cont.)

– Section 4.2.4 - Off-normal Operations

Confirm this subsection identifies 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). Confirm the section briefly summarizes 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. It should also provide a reference to the appropriate documents for recovery actions.

– Section 4.2.5 - System shutdown. Confirm that if it is necessary to shut down the system in a particular sequence or with special timing, the system shutdown actions are summarized and a reference to the corresponding procedure provided.

– Section 4.2.6 - Safety management programs and administrative controls. This subsection should identify aspects of the safety management programs that apply to the system. Text should discuss 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.

• **Section 4.3 – Testing and Maintenance**

Review for design features that enable temporary configurations to support corrective maintenance or modifications as well as required testing and preventative maintenance activities.

– Section 4.3.1 – Temporary configurations. Review for situations under which temporary configurations will be used during surveillance or maintenance. The SDD should state the operational limitations on the use of those configurations and should refer to the applicable procedures.

– Section 4.3.2 – TSR required surveillances. Confirm when the system being described is the subject of TSR surveillance requirements. The SDD should summarize the methods used to meet the requirements (including confirmation that the acceptance criteria have been met), and refer to the procedures used to implement these requirements.

ATTACHMENT B – REVIEW CRITERIA FOR PHASE 1 SDD REVIEWS (cont.)

- Section 4.3.3 – Non-TSR inspections and testing. Confirm that when the system being described is the subject of non-TSR inspection, testing, or surveillance requirements, the SDD summarizes the methods used to meet the requirements (including confirmation that acceptance criteria have been met), and provides references to the implementing procedures.
 - Section 4.3.4 – Maintenance. This subsection of the SDD is to be useful for maintenance personnel, operating personnel and system engineers. Confirm the SDD summarizes the routine actions required by preventive maintenance procedures and post-maintenance testing procedures. This section should also reference appropriate maintenance procedures.
 - Section 4.3.4.1 – Post maintenance testing. Review 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) must be identified. The SDD should also provide appropriate references to post-maintenance testing procedures.
- **Section 4.4 – Supplemental Information**

Confirm text includes any supplemental topics 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.

Chapter 5, References

Only system engineers are required to review this section.

ATTACHMENT B – REVIEW CRITERIA FOR PHASE 1 SDD REVIEWS (cont.)

Appendices

Notes to reviewers – Appendices

- a. *Engineering Discipline Leads and system engineers – Review all appendices for correctness.*
- b. *All others - General review.*

Appendix A - Drawings necessary to maintain Configuration Control of the Design Baseline

Confirm Table A-1 contains the Essential drawings for the system.

Confirm Table A-2 contains the Support drawings for the system.

Confirm Table A-3 lists any reference or historical drawings that are relevant from a historical perspective but are not required for the operation and maintenance of the system, and are not maintained consistent with the field configuration. These documents are for information only and should be used with caution, as they may not reflect current field configuration.

Confirm Table A-4 lists other documents that are related to the system but are not active, nor are they maintained consistent with the field configuration. These documents are for information only and should be used with caution, as they may not reflect current field configuration.

Appendix B - System Procedures

Confirm the appendix contains a list of applicable operating and maintenance procedures.

Appendix C - Vendor Information Files

Confirm that Appendix C contains a list of vendor information files.

Other Appendixes may be added at the discretion of the system engineer.