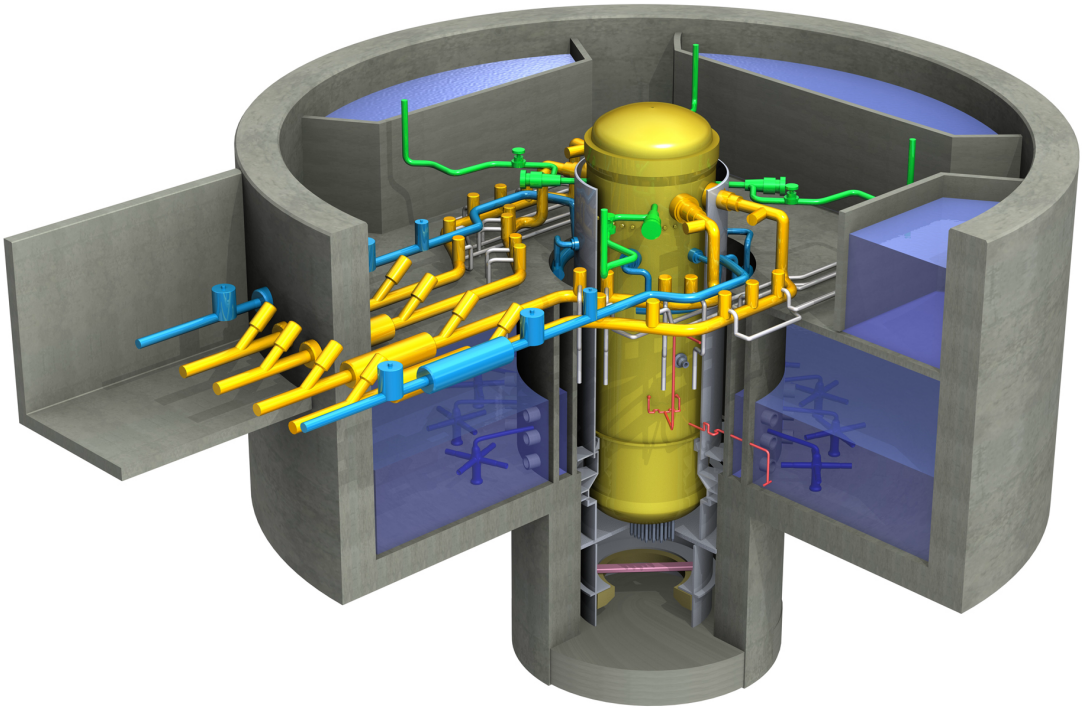
GE Hitachi Nuclear Energy

26A6642BW
Revision 5
May 2008



ESBWR Design Control Document
Tier 2

Chapter 17
Quality Assurance

Contents

17. Quality Assurance 17.0-1
17.0 Introduction 17.0-1
17.0.1 COL Information 17.0-2
17.0.2 References 17.0-2
17.1 Quality Assurance During Design 17.1-1
17.1.1 Organization 17.1-1
17.1.2 Quality Assurance Program 17.1-1
17.1.3 Design Control and Verification 17.1-1
17.1.4 Procurement Document Control 17.1-1
17.1.5 Instructions, Procedures, and Drawings 17.1-1
17.1.6 Document Control 17.1-1
17.1.7 Control of Purchased Material, Equipment, and Services 17.1-2
17.1.8 Identification and Control of Materials, Parts, and Components 17.1-2
17.1.9 Control of Special Processes 17.1-2
17.1.10 Inspection 17.1-2
17.1.11 Test Control 17.1-2
17.1.12 Control of Measuring and Test Equipment 17.1-2
17.1.13 Handling, Storage and Shipping 17.1-2
17.1.14 Inspection, Test, and Operating Status 17.1-2
17.1.15 Nonconforming Materials, Parts, or Components 17.1-2
17.1.16 Corrective Action 17.1-3
17.1.17 Quality Assurance Records 17.1-3
17.1.18 Audits 17.1-3
17.1.19 Training and Qualification Criteria – Quality Assurance 17.1-3
17.1.20 Training and Qualification – Inspection and Test 17.1-3
17.1.21 QA Program Commitments 17.1-3
17.1.22 Nonsafety-Related SSC Quality Controls 17.1-3
17.1.23 Independent Review 17.1-3
17.1.24 COL Information 17.1-3
17.1.25 References 17.1-4
17.2 Quality Assurance During Construction and Operations 17.2-1
17.2.1 COL Information 17.2-1
17.2.2 References 17.2-1
17.3 Quality Assurance Program Description 17.3-1
17.3.1 COL Information 17.3-1
17.3.2 References 17.3-1
17.4 Reliability Assurance Program During Design Phase 17.4-1
17.4.1 Introduction 17.4-1
17.4.2 Scope 17.4-2
17.4.3 Purpose 17.4-2
17.4.4 Objective 17.4-2
17.4.5 GEH Organization for D-RAP 17.4-3
17.4.6 SSC Identification/Prioritization 17.4-4
17.4.7 Design Considerations 17.4-4
17.4.8 Defining Failure Modes 17.4-5
17.4.9 Operational Reliability Assurance Activities 17.4-5
17.4.10 Owner/Operator's Reliability Assurance Program 17.4-6
17.4.11 D-RAP Implementation – Example Case 17.4-7

17.4.11.1 System Description....17.4-7
17.4.11.2 Identifying Risk Information....17.4-8
17.4.11.3 Failure Mode Identification....17.4-8
17.4.11.4 Identification of Maintenance Requirements....17.4-9
17.4.12 Glossary of Terms....17.4-9
17.4.13 COL Information....17.4-9
17.4.14 References....17.4-10

List of Tables

Table 17.0-1 Compliance With Quality Assurance Program Commitments..... 17.0-3
Table 17.4-1 D-RAP Example Case - ICS Importance Analysis 17.4-11
Table 17.4-2 D-RAP Example Case - ICS Failure Modes and Reliability Strategy 17.4-11

17. QUALITY ASSURANCE

17.0 INTRODUCTION

Section 17.1 describes the Quality Assurance (QA) Program used by GE Hitachi Nuclear Energy (GEH) for the ESBWR. The program is based on the standard QA Program, documented in topical report NEDO-11209-04A (Reference 17.0-1) and the additional information in this chapter, which describes and clarifies GEH interfaces and responsibilities with its ESBWR project participants. The ESBWR project participants are domestic and international organizations that have extensive independent experience in the design, development, construction and operation of nuclear power plants.

The standard QA Program is used on all nuclear power plant work, and is Nuclear Regulatory Commission (NRC) accepted. The QA Program complies with 10 CFR 50, Appendix B, the implementing ANSI/ASME N45.2 series daughter standards and the Regulatory Guides (RG) shown in NEDO-11209-04A, Table 2-1 (Reference 17.0-1) with some NRC-accepted GEH alternate positions. Regulatory Guides and Standards and their respective revisions, including exceptions, alternatives and clarifications are addressed in the appropriate Design Control Document (DCD) sections and in Table 17.0-1. The QA Program meets Regulatory Guide 1.28, and is organized to show its relationship to ANSI/ASME NQA-1-1983 and NQA-1a-1983.

GEH ESBWR work is controlled through the NP 2010 COL Demonstration Project Quality Assurance Plan, NEDO-33181 (Reference 17.0-2). NEDO-33181 provides the description of the quality assurance plan scope, which GEH, as supplier for ESBWR engineering services, will implement in support of the DOE NP-2010 COL Demonstration Project.

Suppliers' and sub-tier suppliers' work is controlled through the Supplier QA Requirements (SQAR) – Quality Assurance Requirements for Suppliers of Equipment and Services to the GEH ESBWR Project, NEDO-33260 (Reference 17.0-3). NEDO-33260 defines relationships, responsibilities, and requirements for the supplier's quality program. All safety-related suppliers and sub-tier suppliers must have QA plans to meet the applicable requirements of ANSI/ASME NQA-1-1994.

The evolution of the ESBWR Design and the use of Simplified Boiling Water Reactor (SBWR) test programs conducted at supplier test facilities for the GIRAFFE, PANTHERS, and PANDA tests are discussed in detail in DCD Section 1.5. Each of these test programs was conducted under the appropriate provisions of NEDG-31831 (Reference 17.0-4), and implemented using GEH approved supplier QA Plans. It was required that all of these supplier QA plans either met the requirements of ANSI/ASME NQA-1-1983 and NQA-1a-1983 addenda as endorsed by the NRC in RG 1.28, or the intent of these requirements by reference to equivalent national standards (such as the use of Japanese standard JEAG 4101-1990 for GIRAFFE). Additionally, NEDG-31831 (Reference 17.0-4) provides that design and testing work performed by international technical associates will be performed to their internal QA programs acceptable to the regulatory authorities of their respective countries as evaluated by GEH for compliance with the provisions of ANSI/ASME NQA-1-1983 and NQA-1a-1983. The NRC has participated in oversight activities related to the testing as documented in NRC Inspection Report (Reference 17.0-5). The NRC staff has conducted QA inspections of all of GEH's major design certification test programs (GIST, PANTHERS/PCC, PANTHERS/IC, GIRAFFE, and PANDA) and has concluded that for GIST, PANTHERS, and GIRAFFE, NQA-1 standards were met, or

that appropriate remedial actions were taken to correct deficiencies found during those inspections (Reference 17.0-6).

17.0.1 COL Information

None.

17.0.2 References

17.0-1 GE Nuclear Energy, "GE Nuclear Energy Quality Assurance Program Description," NEDO-11209 04A (NRC accepted), Revision 8, March 1989.

17.0-2 GE Hitachi Nuclear Energy, "NP 2010 COL Demonstration Project Quality Assurance Plan," NEDO-33181, Revision 5, February 2008.

17.0-3 GE Hitachi Nuclear Energy, "Quality Assurance Requirements for Suppliers of Equipment and Services to the GEH ESBWR Project," NEDO-33260, Revision 5, April 2008.

17.0-4 GE Nuclear Energy, "SBWR Design and Certification Program Quality Assurance Plan," NEDG-31831, May 1990.

17.0-5 USNRC, "NRC Inspection Report No. 99900404/95-02," MFN-196-95, September 25, 1995.

17.0-6 USNRC, "Staff Evaluation of General Electric's (GE's) Test and Analysis Program Description, NEDC-32391 Rev. C", MFN-119-96, July 11, 1996.

Table 17.0-1

Compliance With Quality Assurance Program Commitments

Commitment	Revision	Comments
RG 1.8	3	Not applicable for GEH QA Program
RG 1.21	1	Not applicable for GEH QA Program
RG 1.26	3	Except for the alternate Quality Group Classification for the Hydraulic Control Unit per Note 8 of Table 3.2-1
RG 1.28	3	Except for NRC-accepted alternate positions in Table 2-1 of Reference 17.0-1
RG 1.29	3	Except for Main Steam Piping from seismic interface restraint to turbine stop valves as identified in Table 3.2-1 and Figure 3.2-1
RG 1.30	0	No exception
RG 1.33	2	Not applicable for GEH QA Program
RG 1.37	0	Except for NRC-accepted alternate positions in Table 2-1 of Reference 17.0-1
RG 1.38	2	Except for NRC-accepted alternate positions in Table 2-1 of Reference 17.0-1
RG 1.39	2	No exception
RG 1.54	1	No exception
RG 1.58	Withdrawn	Superseded by RG 1.28, Rev. 3
RG 1.64	Withdrawn	Superseded by RG 1.28, Rev. 3, except for NRC-accepted alternate positions in Table 2-1 of Reference 17.0-1
RG 1.74	Withdrawn	Superseded by RG 1.28, Rev. 3
RG 1.88	Withdrawn	Superseded by RG 1.28, Rev. 3
RG 1.94	1	Not applicable for GEH QA Program
RG 1.97	4	No exception
RG 1.116	0-R	No exception
RG 1.123	Withdrawn	Superseded by RG 1.28, Rev. 3
RG 1.143	2	No exception
RG 1.144	Withdrawn	Superseded by RG 1.28, Rev. 3
RG 1.146	Withdrawn	Superseded by RG 1.28, Rev. 3
RG 1.152	2	No exception

Commitment	Revision	Comments
RG 1.168	1	No exception
RG 1.169	0	No exception
RG 1.170	0	No exception
RG 1.171	0	No exception
RG 1.172	0	No exception
RG 1.173	0	No exception
RG 1.176	0	Not applicable for GEH QA Program
RG 4.15	1	No exception
RG 7.10	2	No exception
Subpart 2.1 of ASME NQA-1-1994	1994	Commitment through ESBWR commitment to ASME NQA-2-1983
Subpart 2.2 of ASME NQA-1-1994	1994	Commitment through ESBWR commitment to ASME NQA-2-1983
Subpart 2.4 of ASME NQA-1-1994	1994	Commitment through ESBWR commitment to IEEE 336-1985
Subpart 2.5 of ASME NQA-1-1994	1994	Commitment through ESBWR commitment to ASME NQA-2-1983
Subpart 2.7 of ASME NQA-1-1994	1994	Commitment through ESBWR commitment to IEEE 1012-2004
Subpart 2.8 of ASME NQA-1-1994	1994	Commitment through ESBWR commitment to ASME NQA-2-1983
Subpart 2.15 of ASME NQA-1-1994	1994	Commitment through ESBWR commitment to ASME NQA-2-1983
Subpart 2.20 of ASME NQA-1-1994	1994	Commitment through ESBWR commitment to ASME NQA-2-1983

Commitment	Revision	Comments
RG 1.189, Regulatory Position 1.7 "Quality Assurance"	0	No exception
NRC Generic Letter 85-06	1985	No exception
NRC Generic Letter 89-02	1989	No exception
NRC Generic Letter 91-05	1991	Not applicable for GEH QA Program
Regulatory Position 3.5 and Appendix A of RG 1.155	0	No exception
NIRMA TG 11-1998	1998	No exception
NIRMA TG 15-1998	1998	No exception
NIRMA TG 16-1998	1998	No exception
NIRMA TG 21-1998	1998	No exception

17.1 QUALITY ASSURANCE DURING DESIGN

The QA Program described in Section 17.1 is applicable to the ESBWR design activities supporting the standard design certification. Quality assurance is the responsibility of the DCD applicant for these design activities. The QA Program for design activities related to a specific plant is defined in Section 17.2.

17.1.1 Organization

"GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 1, establishes requirements for the Organization structure used during design of the ESBWR.

17.1.2 Quality Assurance Program

"GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 2, establishes requirements for the Quality Assurance Program used during design of the ESBWR.

The identification of safety-related structures, systems and components (Q list) to be controlled by the GEH QA Program is shown in Table 3.2-1.

"GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 2, establishes a 10 CFR Part 21 notification and posting system which is procedurally controlled. The requirement of 10 CFR Part 21 is imposed on all safety-related purchase documents.

17.1.3 Design Control and Verification

"GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 3, establishes requirements for Design Control used during design of ESBWR. Minimum design requirements are identified in Table 3.2-2.

ESBWR Instrumentation & Control (I&C) Software Quality Assurance Plan, NEDO-33245 (Reference 17.1-2), establishes the requirements for Software Verification and Validation Quality Controls. Software Design Verification and Validation is discussed in Subsection 7.8.2.1 and Appendix 7B.

17.1.4 Procurement Document Control

"GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 4, establishes requirements for Procurement Document Control used during design of the ESBWR.

17.1.5 Instructions, Procedures, and Drawings

"GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 5, establishes requirements for Instructions, Procedures, and Drawings used during design of the ESBWR.

17.1.6 Document Control

"GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 6, establishes requirements for Document Control used during design of the ESBWR.

17.1.7 Control of Purchased Material, Equipment, and Services

"GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 7, establishes requirements for Control of Purchased Material, Equipment, and Services used during design of the ESBWR. GEH has procedurally established a Commercial Grade dedication program, which meets the requirements of 10 CFR Part 21.

17.1.8 Identification and Control of Materials, Parts, and Components

"GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 8, establishes requirements for Identification and Control of Materials, Parts, and Components during design of the ESBWR.

17.1.9 Control of Special Processes

"GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 9, establishes requirements for Control of Special Processes used during design of the ESBWR.

17.1.10 Inspection

"GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 10, establishes requirements for Inspection used during design of the ESBWR.

17.1.11 Test Control

"GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 11, establishes requirements for Test Control used during design of the ESBWR.

17.1.12 Control of Measuring and Test Equipment

"GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 12, establishes requirements for Control of Measuring and Test Equipment during design of the ESBWR.

17.1.13 Handling, Storage and Shipping

"GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 13, establishes requirements for Handling, Storage, and Shipping used during design of the ESBWR.

17.1.14 Inspection, Test, and Operating Status

"GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 14, establishes the control of Inspection, Test, and Operating Status used during design of the ESBWR.

17.1.15 Nonconforming Materials, Parts, or Components

"GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 15, establishes requirements for the control of Nonconforming Materials, Parts, or Components used during design of ESBWR.

17.1.16 Corrective Action

"GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 16, establishes requirements for the Corrective Action program used during design of the ESBWR.

17.1.17 Quality Assurance Records

"GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 17, establishes requirements for control of Quality Assurance Records used during design of the ESBWR.

17.1.18 Audits

"GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 18, establishes requirements for a comprehensive system of QA Audits used during design of the ESBWR.

17.1.19 Training and Qualification Criteria – Quality Assurance

In accordance with "GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 2, Training and Qualification of QA personnel is procedurally established and maintained.

17.1.20 Training and Qualification – Inspection and Test

In accordance with "GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 2, Training and Qualification of Inspection and Test personnel is procedurally established and maintained.

17.1.21 QA Program Commitments

Regulatory Guides and Standards and their respective revisions, including exceptions, alternatives and clarifications are addressed in the appropriate DCD sections and in Table 17.0-1.

17.1.22 Nonsafety-Related SSC Quality Controls

Nonsafety-related Structure, System and Components (SSCs) that perform safety significant functions have QA requirements applied commensurate with the importance of the item's function. The identification of nonsafety-related structures, systems and components is shown in Table 3.2-1. Reference 17.1-3 describes the QA requirements that are applied to nonsafety-related SSCs.

17.1.23 Independent Review

Not applicable for GEH QA Program.

17.1.24 COL Information

None.

17.1.25 References

17.1-1 GE Nuclear Energy, "GE Nuclear Energy Quality Assurance Program Description," NEDO-11209-04A (NRC accepted), Revision 8, March 1989.

17.1-2 GE Energy Nuclear, "ESBWR I&C Software Quality Assurance Plan," NEDO-33245, Revision 2, July 2007.

17.1-3 GE Hitachi Nuclear Energy, "NP-2010 COL Demonstration Project Quality Assurance Program," NEDO-33181, Revision 5, February 2008.

17.2 QUALITY ASSURANCE DURING CONSTRUCTION AND OPERATIONS

QA responsibilities during construction and operations are Combined Operating License (COL) applicant scope. The COL Applicant shall describe the QA Program for the Construction and Operations phases (COL 17.2-1-A). Quality assurance during design activities necessary to adapt the certified standard plant design to the specific plant implementation is the responsibility of the COL Applicant. The COL Applicant shall describe the QA Program for design activities that are necessary to adapt the certified standard plant design to a specific plant implementation (COL 17.2-2-A).

17.2.1 COL Information

17.2-1-A QA Program for the Construction and Operations Phases

The COL Applicant shall describe the QA Program for the Construction and Operations phases (Section 17.2).

17.2-2-A QA Program for Design Activities

The COL Applicant shall describe the QA Program for design activities that are necessary to adapt the certified standard plant design to a specific plant implementation (Section 17.2).

17.2.2 References

None.

17.3 QUALITY ASSURANCE PROGRAM DESCRIPTION

The project overall Quality Assurance Program Description (QAPD) is a COL Applicant/Holder responsibility. The COL Applicant shall provide a QAPD describing the overall project QA program (COL 17.3-1-A). The QAPD applied by the Design Team during the design certification phase is described in Section 17.1.

17.3.1 COL Information

17.3-1-A Quality Assurance Program Document

The COL Applicant shall provide a QAPD describing the overall project QA program (Section 17.3).

17.3.2 References

None.

17.4 RELIABILITY ASSURANCE PROGRAM DURING DESIGN PHASE

This section presents the ESBWR Design Reliability Assurance Program (D-RAP).

17.4.1 Introduction

The GEH ESBWR D-RAP is a program utilized during detailed design and specific equipment selection phases to assure that the important ESBWR reliability assumptions of the Probabilistic Risk Assessment (PRA) are considered throughout the plant life. The PRA is used to evaluate the plant response to initiating events and mitigation to ensure potential plant damage scenarios pose a very low risk to the public.

The D-RAP identifies relevant aspects of plant operation, maintenance, and performance monitoring of important plant SSCs for owner/operator consideration in assuring safety of the equipment and limiting risk to the public. An example is provided in Subsection 17.4.11 to demonstrate how the D-RAP applies to the Isolation Condenser System (ICS). The ICS example shows how the principles of D-RAP are applied to other systems identified by the PRA as being risk-significant.

The COL Holder will provide a description of operational reliability assurance activities (COL 17.4-1-H). These activities are consistent with the following requirements:

- Integrate the objectives of operational reliability assurance activities into the QA program, including addressing failures of nonsafety-related, risk-significant SSCs that result from design and operational errors in accordance with SECY 95-132, Item E.
- Establish PRA importance measures, the expert panel process, and deterministic methods to determine the site-specific list of risk-significant SSCs under the scope of the D-RAP.
- Evaluate and maintain the reliability of risk-significant SSCs as identified in the D-RAP. The program may cite, for example, reliability analysis, cost-effective maintenance enhancements, such as condition monitoring and using condition-directed maintenance as well as time directed or planned periodic maintenance.
- Use the Maintenance Rule (10 CFR 50.65) program to monitor the effectiveness of maintenance activities needed for operational reliability assurance.
- Consider all SSCs that are in the scope of the D-RAP as high-safety-significant (HSS) within the scope of the Maintenance Rule program, or provide Expert Panel justification for any exceptions.

  Note: The Expert Panel, in accordance with common industry practice and guidance in NUMARC 93-01, develops the final list of risk significant SSCs from various inputs, including the PRA risk importance calculations and industry operating experience. It is necessary for the Expert Panel to include all SSCs that are in the scope of the RAP to be included in the HSS category of SSCs within the scope of the Maintenance Rule. However, risk importance calculations, plant specifics and other factors may change the risk significance of certain SSCs in the operational RAP that were previously determined to be risk-significant within the bounds of the D-RAP. Therefore, exceptions between the D-RAP and operational RAP risk significance may exist, and should be evaluated and justified by the Expert Panel.

- Establish a reliability database using historical data on equipment performance as available. The compilation and reduction of this data provides the plant with source of component reliability information. Data used in PRA fault-tree analyses may also be a viable initial source.
- Use surveillance and testing to establish the level of performance or condition being maintained for SSCs within the scope of the RAP and identifies declining trends in between surveillances prior to performance or condition degrading to unacceptable levels undetected (or failure) to the extent possible.
- Develop a maintenance plan to describe the nature and frequency of maintenance activities to be performed on plant equipment. The plan includes the selected SSCs identified in the D-RAP.

17.4.2 Scope

The scope of the ESBWR D-RAP includes risk-significant SSCs, both safety-related and nonsafety-related, that provide defense-in-depth or result in significant improvement in the PRA evaluations.

A preliminary list of risk-significant SSCs within the scope of the D-RAP is developed in the design phase.

The list is updated, using a blended approach and an Expert Panel when plant-specific information is available. This updated list forms part of the basis for the HSS category, as described in NUMARC 93-01, and as endorsed by RG 1.160, of the SSCs within the scope of the Maintenance Rule program, as prescribed by 10 CFR 50.65(b). The Maintenance Rule Program ensures that risk-significant SSCs operate throughout plant life with reliable performance that is consistent with the PRA. The HSS category within the Maintenance Rule Program scope must encompass the SSCs in the RAP scope as modified for the operations phase if the Maintenance Rule Program is to be used along with the QA and maintenance and surveillance programs in implementation of the RAP in the operations phase. The PRA for the ESBWR, and other sources, such as historical records of Boiling Water Reactor (BWR) system and components are used to identify and prioritize those SSCs that are important to prevent or mitigate plant AOOs or other events that could present a risk to the public.

17.4.3 Purpose

The purpose of the D-RAP is to ensure that the plant safety, as estimated by the PRA, is maintained as the detailed design evolves through the implementation and procurement phases, and that pertinent information is provided in the design documentation to the future owner/operator so that equipment reliability, as it affects plant safety, is maintained through operation and maintenance during the entire plant life.

17.4.4 Objective

The objective of the D-RAP is to identify those plant SSCs that are significant contributors to risk, as shown by the PRA or other sources, and to assure that, during the implementation phase, the plant design continues to utilize risk-significant SSCs whose reliability is commensurate with the PRA assumptions. Reliability includes ensuring that risk-significant SSCs do not degrade to

an unacceptable level during plant operations, and that the frequency of initiating events posing challenges to risk-significant SSCs is minimized. The D-RAP also identifies key assumptions regarding any operation, maintenance and monitoring activities that the owner/operator should consider in implementing operational reliability assurance activities to assure that such SSCs function when challenged throughout plant life with reliability consistent with that assumed in the PRA.

17.4.5 GEH Organization for D-RAP

The GEH ESBWR Engineering section is an integrated design and engineering organization that is responsible for formulating and implementing the D-RAP. The Manager, ESBWR Engineering is responsible for the design and licensing of the ESBWR, and for development of the D-RAP.

The ESBWR Engineering organization is responsible for the design analysis and PRA engineering that is necessary to support the development of the D-RAP. PRA personnel are directly involved with the design organization and keep the design staff cognizant of risk-significant items, program needs, and project status. PRA personnel participate in the design change control process, which includes providing D-RAP related inputs in the design process.

GEH ESBWR Engineering design procedural controls are applied to the D-RAP. Specific procedures provide guidance on the design process, control of design changes, and storage and retrieval controls.

The design control procedure defines the process for performing, documenting, and verifying design activities. This includes developing or modifying the design of systems, engineering evaluations, analyses, calculations and documents, (e.g., specifications, drawings, reports).

The procedure for design change control defines the process for evaluating design changes in engineering controlled documents to ensure that the total effect is considered before a change is approved, and that the affected documents are identified and changed accordingly. The procedure identifies interfaces and organizations responsible for these interfaces, including PRA review. If a proposed change could affect the safety, availability or capacity factor of the ESBWR plant, system reliability is analyzed.

Several design control procedures provide guidance for developing a high quality process for reliability assurance. The documentation procedure establishes the requirements and responsibilities for the preparation, approval, and issue of documents controlled by the engineering design organizations. The quality assurance records procedure provides requirements for quality assurance record retention. The self-assessment, corrective action and audits procedure specifies the responsibilities for performing self-assessments; internal audits of the engineering organization, and prompt identification, documentation, and corrective actions on conditions that are adverse to quality.

In addition to the standard engineering design processes and quality controls, specific guidance is used to define and implement an effective RAP. Reference 17.4-1 describes the D-RAP processes for identifying and prioritizing risk significance, implementing reliability assurance strategies, and monitoring program effectiveness.

17.4.6 SSC Identification/Prioritization

A list of risk-significant SSCs is developed and controlled as a topical report (Reference 17.4-7). The preliminary list is based on the results of the generic PRA. The list is updated when the plant-specific PRA is developed. At this point, a blended approach is used for identifying and prioritizing risk significant SSCs. This approach combines the various PRA analytical results with operating experience and an expert panel process to develop a comprehensive risk analysis.

The Level 1 PRA is used to evaluate accident sequences from initiating events and failures of safety functions that lead to core damage. An assessment is performed for operating and shutdown conditions. The external events analysis considers events whose cause is external to systems associated with normal plant operations, including internal flooding, fire, high winds, and seismic events. The seismic events are analyzed using a seismic margins approach that provides qualitative conclusions on the ability of ESBWR SSCs to cope with seismic events. The other external events are quantified using the Level 1 PRA.

Level 1 basic events representing component failures are identified as risk-significant if their importance values for Risk Achievement Worth (RAW) are greater than or equal to 5.0, or Fussell-Vesely Importance are greater than or equal to 0.01.

Level 2 risk significance is determined by identifying the dominant contributors to severe accidents and offsite release of fission products. This qualitative analysis, which is performed by the expert panel, includes the evaluation of severe accident phenomena and fission product source terms, and containment integrity strategies including pressure suppression, decay heat removal, and hydrogen generation.

SSC functions relied upon under power-operating and shutdown conditions to meet the NRC's safety goal guidelines of a Core Damage Frequency (CDF) of less than 1.0E-4 per reactor year and Large Release Frequency of less than 1.0E-6 per reactor year are risk-significant. SSC functions needed to meet the containment performance goal, including containment bypass, during severe accidents are also risk-significant.

Operating experience identifies previous failures of components in similar applications, and also reveals situations where inappropriate human actions have led to functional failures of SSCs. The expert panel assesses component operating history and industry operating experience when it can be applied to assessing risk significance.

Safety-related SSCs are controlled by plant Technical Specifications. If a nonsafety-related SSC is shown through operating experience or PRA to be significant to public health and safety, then it should be controlled by Technical Specifications. In this case, “significant” equates to an SSC that is required to meet the NRC Safety Goals. If it is determined that an SSC is risk significant, but is not required for meeting the NRC Safety Goals, then performance controls should be implemented through the RAP. If the SSC is not significant, then normal controls would be implemented through the site Maintenance Rule and corrective action programs.

17.4.7 Design Considerations

The reliability of risk-significant SSCs, which are identified by the PRA and other sources, are evaluated at the detailed design stage by appropriate design reviews and reliability analyses. The procedure for design change control defines the process for evaluating design changes in

engineering controlled documents to ensure that the total effect is considered before a change is approved, and the affected documents are identified and changed accordingly.

A design reliability assessment is a process in which the design engineer builds quality and reliability into the SSC, while ensuring that the basis for SSC design is properly modeled in the PRA. Due to the preliminary nature of the PRA model during the design phase, the model relies on generic information, bounding assumptions, or design requirements as a basis for model development. This design assessment can be performed for changes that occur during the plant design phase, as well as during normal plant operations. It is a systematic method to evaluate the proposed design details with respect to PRA insights. The assessment considers reliability concepts, such as redundancy, diversity, human factors, spatial interactions, external events, etc., to enhance the system design, and considers PRA insights and assumptions. If the assessment reveals that the proposed design could conflict with results and insights calculated in the PRA, or could cause significant unavailability of a safety function, then a design change is pursued.

Proposed design changes are processed by the design change control procedure, which requires PRA review. If a design change affects the PRA model, then the PRA is revised in accordance with the PRA update process described in the PRA procedure.

17.4.8 Defining Failure Modes

The determination of dominant failure modes of risk-significant SSCs includes historical information, analytical models and existing requirements. Many BWR systems and components have compiled a significant historical record, so an evaluation of that record is performed. For those SSCs for which there is not an adequate historical basis to identify critical failure modes, an analytical approach is necessary.

Inputs may include PRA importance analysis, root cause analysis, failure modes and effects analysis, and review of operating experience. In addition, equipment performance information, including vendor manuals, ASME Section XI, technical specifications, Regulatory Treatment of Non-Safety Systems (RTNSS), and other regulatory requirements are reviewed to identify important safety functions.

The design engineer analyzes this information to identify dominant failure modes, such as single failures, latent failures not detected by routine monitoring, common cause failures, or failures that could cascade into more significant safety functional failures.

17.4.9 Operational Reliability Assurance Activities

Once the dominant failure modes are determined for risk-significant SSCs, an assessment is performed to identify operational reliability assurance activities that assure acceptable performance during plant life. Such activities may consist of periodic surveillance inspections or tests, monitoring of SSC performance, and/or periodic preventive maintenance. Some SSCs may require a combination of activities to assure that their performance is consistent with that assumed in the PRA.

Operational reliability assurance activities, including integration of D-RAP objectives into operational programs, is the responsibility of the COL Holder (see Subsection 17.4.1). Guidance documents used to implement these activities include: RG 1.160, “Monitoring the Effectiveness of Maintenance at Nuclear Power Plants,” (Reference 17.4-3) NUMARC 93-01, “Industry

Guidance for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," (Reference 17.4-5), the February 22, 2000 Revision to Section 11 of NUMARC 93-01 (Reference 17.4-6) and, if still effective at the time of the COL application, RG 1.182, "Assessing and Managing the Risk Before Maintenance at Nuclear Power Plants." (Reference 17.4-4)

Periodic testing of SSCs may include startup of standby systems, surveillance testing of instrument circuits to assure that they respond to appropriate signals, and inspection of SSCs (such as tanks and pipes) to show that they are available to perform as designed. Performance monitoring, including condition monitoring, can consist of measurement of output (such as pump flow rate or heat exchanger temperatures), measurement of magnitude of an important variable (such as vibration or temperature), and testing for abnormal conditions (such as oil degradation or local hot spots).

Periodic preventive maintenance is an activity performed at regular intervals to preclude problems that could occur before the next preventive maintenance (PM) interval. This could be regular oil changes, replacement of seals and gaskets, or refurbishment of equipment subject to wear or age related degradation.

Planned maintenance activities are integrated with the regular operating plans so that they do not disrupt normal operation. Maintenance that is performed more frequently than refueling outages is planned so as to not disrupt operation or be likely to cause reactor scram, engineered safety feature actuation or AOOs. Maintenance planned for performance during refueling outages is conducted in such a way that it has little or no effect on plant safety, outage length or other maintenance work.

Reliability monitoring information is collected from sources such as Technical Specification surveillance test data and industry operating data, if applicable. Similar reliability data is collected for RTNSS SSCs, which are within the scope of the D-RAP. Reliability estimates are also developed from basic event fault trees for risk-significant (that is, HSS) systems and components modeled in ESBWR PRA.

17.4.10 Owner/Operator's Reliability Assurance Program

Operational reliability assurance activities are implemented by the ESBWR owner/operator, and use the information provided by GEH. Elements include:

- **Problem Prioritization:** Identification for each of the risk-significant SSCs of the importance of that item as a contributor to its system unavailability and assignment of priorities to problems that are detected with such equipment.
- **Corrective Action Implementation:** Carrying out identified corrective action on risk-significant equipment to restore equipment to its intended function in such a way that plant safety is not compromised during work.
- **Plant Aging:** Some of the risk-significant equipment is expected to undergo age related degradation and require equipment replacement or refurbishment.
- **Programmatic Interfaces:** Reliability assurance interfaces related to the work of the several organizations and personnel groups working on risk-significant SSCs.

- **Maintenance Rule Program:** A procedure is developed by the COL Holder to implement a Maintenance Rule program with the following scope:
  - Selecting SSCs for inclusion;
  - Establishing and applying safety significant criteria;
  - Setting performance monitoring criteria;
  - Trending the performance of applicable SSCs to demonstrate the effectiveness of maintenance activities;
  - Taking corrective action when SSC performance degrades;
  - Periodically assessing program performance;
  - Identifying documentation that is required to support the program; and
  - Performing Maintenance Rule (a)(4) assessment of real-time risk profile.

Plant operational reliability assurance activities address the interfaces with construction, startup testing, operations, maintenance, engineering, safety, licensing, quality assurance and procurement of initial and replacement equipment. See Subsection 17.4.1 for COL information requirements.

17.4.11 D-RAP Implementation – Example Case

The following example case is provided to illustrate the D-RAP process. It is based upon design and PRA details of the Isolation Condenser System (ICS) that were available at a particular time during the design phase. As such, it is not intended to be updated if design or PRA details of the ICS change.

17.4.11.1 System Description

The ICS is used as an example to demonstrate how the reliability assurance processes are used to identify, analyze, and develop effective reliability assurance strategies. ICS is a safety-related system that removes reactor decay heat following events involving reactor shutdown and containment isolation. It also prevents unnecessary reactor depressurization, and precludes the need for operation of other Engineered Safety Features to bring the reactor to a safe and stable condition. In the event of a loss-of-coolant-accident (LOCA), ICS provides additional liquid inventory by opening the condensate return valves to actuate the system. ICS also assists with initial depressurization of the reactor before Automatic Depressurization System (ADS) in event of loss of feedwater, so that the automatic depressurization can take place from a lower pressure.

The ICS consists of four totally independent trains, each containing an isolation condenser that condenses steam on the tube side and transfers heat to the Isolation Condenser/Passive Containment Cooling (IC/PCC) pool, which is vented to the atmosphere. The isolation condensers are connected by piping to the reactor pressure vessel, and are placed at an elevation above the source of steam (that is, vessel). When the steam is condensed, the condensate is returned to the vessel via a condensate return line. A detailed description of ICS is located in Subsection 5.4.6.

The major differences between the ESBWR ICS and the conventional BWR ICS are:

- Use of four heat exchangers instead of one or two in conventional BWRs;
- Parallel path for condensate return to the vessel instead of single injection path;
- Use of both Nitrogen-Operated and Motor-Operated Valves (MOVs) for condensate return instead of only MOVs; and
- Use of large cooling pools instead of shell-side heat exchangers.

The design features of the ESBWR ICS contain significant improvements in reliability and availability that are risk-based. The number of heat exchangers is increased for redundancy. The condensate return line to the vessel has two paths for success and each path uses a diverse isolation valve. The large capacity IC pools provide cooling capacity for 72 hours following a reactor scram. Conventional BWRs typically have 20 to 30 minutes of cooling water capacity.

17.4.11.2 Identifying Risk Information

In order to examine the relative importance or dominance of failures of ICS components, a fault tree has been developed with the top gate defined as failure of the ICS to inject water into the RPV upon demand. This tree considers the worst-case scenario with respect to AOOs and accidents, which involves a success criterion that three-of-four ICS subsystems must function. This requires a condensate return path and a vent path for non-condensables for each functioning subsystem. This fault tree is quantified to identify the relative importance of ICS components as they contribute to system unreliability.

A risk ranking of the ICS basic events has been performed to identify SSCs with the greatest importance. The ranking is performed using the ICS top event model, described above. In addition, a risk ranking is performed using the CDF top event (PRA) model to provide further perspective on the importance of ICS components. The results of the risk rankings are provided in Table 17.4-1.

17.4.11.3 Failure Mode Identification

The importance analysis results indicate that no single SSC has a dominant effect on ICS system unavailability. Therefore, the design and selection of ICS components appears to be reasonable.

The dominant failures, as shown in Table 17.4-1, involve valves. Operating experience indicates that valves, in general, are subject to mechanical problems such as valve stem failure, separation of stem from disk, and failure to stroke. In addition, remote actuated valves can experience actuator failures, electrical failures in the motor winding or motor internals, and problem with torque limit switches and switch settings.

For ICS, the dominant failures involve the condensate return nitrogen-operated isolation valves (B32-F006A, B, C, D). The parallel condensate return valves, B32-F005A, B, C, D have lower risk importance values and are thus not considered to be dominant failures.

According to the design specifications, the condensate return valve, (F006) is a spring-loaded, pneumatic, piston-operated globe valve, designed to fail open on loss of pneumatic pressure to the valve actuator. This valve is also signaled to open when reactor water level drops to Level 2. A pneumatic accumulator is located close to the valve to provide pneumatic pressure for the

purpose of assisting in valve closure when both pilots are energized or in the event of failure of pneumatic supply pressure to the valve operator. Examples of the types of failure that could affect valve reliability are shown in Table 17.4-2.

17.4.11.4 Identification of Maintenance Requirements

Maintenance activities are developed to assure that the dominant failure modes are reduced, or kept to an acceptably low probability. The types of maintenance and the maintenance frequencies are both important aspects of ensuring that the equipment failure rate is consistent with that assumed in the PRA model. The designer considers periodic or condition-based testing and maintenance activities to keep the unreliability to an acceptable level.

In this example, the D-RAP analytical process results in a preliminary recommendation for quarterly valve testing of the B32-F006 valves, along with flow testing during each refueling outage. This helps to preserve the unreliability values used in the PRA model. In addition, the B32-F005 valves, which are in the parallel path, are recommended to receive the same testing requirements. This will ensure that these valves do not experience degraded performance that could increase their risk significance.

The recommended maintenance activities and performance monitoring will be governed by the QA and Maintenance Rule Program.

17.4.12 Glossary of Terms

Design Reliability Assurance Program — Performed by the plant designer to assure the plant is designed so that it can be operated and maintained in such a way that the reliability assumptions of the probabilistic risk assessment apply throughout plant life.

Fussell-Vesely Importance — A measure of the component contribution to core damage frequency. Numerically, the percentage contribution of the component to CDF.

Owner/Operator — The utility or other organization that owns and operates the ESBWR following construction.

Operational Reliability Assurance Program — Performed by the plant owner/operator to assure the plant is operated and maintained safely and in such a way that the reliability assumptions of the PRA apply throughout plant life.

Regulatory Treatment of Non-Safety Systems (RTNSS) — A process to determine whether regulatory oversight for certain nonsafety-related systems is needed, and to determine an appropriate level of regulatory oversight commensurate with their risk significance.

Risk-Significant — Those structures, systems and components that are identified as contributing significantly to the core damage frequency.

17.4.13 COL Information

17.4-1-H Operation Reliability Assurance Activities

The COL Holder will provide a description of operational reliability assurance activities (Subsection 17.4.1).

17.4.14 References

17.4-1 GE Energy Nuclear, "Reliability Assurance Program Plan", NEDO-33289, Revision 1, December 2007.

17.4-2 US Nuclear Regulatory Commission, "Policy and Technical Issues Associated With the Regulatory Treatment of Non-Safety Systems (RTNSS) in Passive Plant Designs (SECY-94-084)", SECY-95-132, May 1995.

17.4-3 US Nuclear Regulatory Commission, "Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," Regulatory Guide 1.160, March 1997.

17.4-4 US Nuclear Regulatory Commission, "Assessing and Managing the Risk Before Maintenance at Nuclear Power Plants," Regulatory Guide 1.182, May 2000.

17.4-5 NEI, "Industry Guidance for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," NUMARC 93-01 April 1996.

17.4-6 NEI, "Industry Guidance for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," Revision to Section 11 of NUMARC 93-01 February 22, 2000.

17.4-7 GE Hitachi Nuclear Energy, "Risk Significance of Structures, Systems and Components for the Design Phase of the ESBWR," NEDO-33411, Revision 0, March 2008.

Table 17.4-1

D-RAP Example Case - ICS Importance Analysis

Component	Description	Fussell-Vesely Importance	Risk Achievement Worth
B32-F006B	Air Operated Valve F006B Fails To Open	8.27E-04	1.41
B32-F006C	Air Operated Valve F006C Fails To Open	8.27E-04	1.41
B32-F006D	Air Operated Valve F006D Fails To Open	8.27E-04	1.41
B32-F006A	Air Operated Valve F006A Fails To Open	1.04E-04	1.05

Table 17.4-2

D-RAP Example Case - ICS Failure Modes and Reliability Strategy

Component	Failure Mode	Cause	Reliability Strategy
B32-F006A, B, C, D	Failure to Open due to mechanical problems	Binding, fatigue failure, foreign material	Inspect Valve Internals, System Flow Test, Valve Stroke Test
	Failure to Open due to electrical problems with valve operator	Windings, Wiring, Relays, Contacts	Logic System Functional Test, Valve Stroke Test