HITACHI

GE Hitachi Nuclear Energy

Richard E. Kingston

Vice President, ESBWR Licensing
PO Box 780 M/C A-65
Wilmington, NC 28402-0780

USA

T 910 819 6192
F 910 362 6192
rick.kingston@ge.com

MFN 10-026

Docket No. 52-010

February 3, 2010

U.S. Nuclear Regulatory Commission
Document Control Desk
Washington, D.C. 20555-0001

Subject: Submittal of Licensing Topical Report NEDO-33219, "ESBWR Human Factors Engineering Functional Requirements Analysis Implementation Plan," Revision 4

The purpose of this letter is to submit Revision 4 of the GE Hitachi Nuclear Energy (GEH) Licensing Topical Report NEDO-33219, "ESBWR Human Factors Engineering Functional Requirements Analysis Implementation Plan" in accordance with the corresponding HFE program element identified in Reference 1.

Enclosure 1 contains Licensing Topical Report NEDO-33219, "ESBWR Human Factors Engineering Functional Requirements Analysis Implementation Plan," Revision 4.

If you have any questions or require additional information, please contact me.

Sincerely,

Richard E. Kingston

Richard E. Kingston

Vice President, ESBWR Licensing

Reference:

1. NUREG-0711, Revision 2, Human Factors Engineering Program Review Model, issued February 2004

Enclosure:

1. MFN 10-026 - Licensing Topical Report NEDO-33219, "ESBWR Human Factors Engineering Functional Requirements Analysis Implementation Plan," Revision 4

cc:

AE Cubbage	USNRC (with enclosure)
JG Head	GEH/Wilmington (with enclosure)
DH Hinds	GEH/Wilmington (with enclosure)
DF Taylor	GEH/Wilmington (with enclosure)
eDRF Section	0000-0050-0877 R6

MFN 10-026

Enclosure 1

Licensing Topical Report NEDO-33219
ESBWR Human Factors Engineering Functional Requirements Analysis Implementation Plan
Revision 4

HITACHI

GE Hitachi Nuclear Energy

NEDO-33219
Revision 4
Class I
DRF Section 0000-0050-0877 R6
February 2010

Licensing Topical Report

ESBWR HUMAN FACTORS ENGINEERING FUNCTIONAL REQUIREMENTS ANALYSIS IMPLEMENTATION PLAN

PROPRIETARY INFORMATION NOTICE

This document NEDO-33219, Revision 4, contains no proprietary information.

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT

Please read carefully

The information contained in this document is furnished as reference to the NRC Staff for the purpose of obtaining NRC approval of the ESBWR Certification and implementation. The only undertakings of GE Hitachi Nuclear Energy (GEH) with respect to information in this document are contained in contracts between GEH and participating utilities, and nothing contained in this document shall be construed as changing those contracts. The use of this information by anyone other than that for which it is intended is not authorized; and with respect to any unauthorized use, GEH makes no representation or warranty, and assumes no liability as to the completeness, accuracy, or usefulness of the information contained in this document.

Table of Contents

List of Tables

List of Figures

1. OVERVIEW

The ESBWR Man-Machine Interface System And Human Factors Engineering Implementation Plan, Reference 2.1.1(5), illustrated in Figure 1, establishes three specific activities that support operational analysis:

- Functional Requirements Analysis (FRA)
- Allocation of Functions (AOF)
- Task Analysis (TA)

These steps determine:

- Functions required to achieve plant goals and system functions
- Distribution of functions among manual, remote manual, automatic, plant automation, and shared control
- The integrated human actions (HAs) required at the task level

The overall operational analysis is an iterative integration of the three elements of functional requirements, function allocation, and task analysis to establish requirements for the Human-System Interface (HSI) design. Plant equipment, software, personnel, and procedural requirements are systematically defined. As a result, functional objectives are met.

FRA contributes to the design of ESBWR equipment and associated HSIs. HSI development focuses on the control room and safe shutdown locations outside the control room. The operational analysis consists of collecting plant and system parameter data. Parameters required for crew monitoring, cues for action, and operator feedback are determined. The analysis identifies the control and operating options available for safe and economic plant operation. The plant processes assigned to operators are defined.

Benefits of the integrated operational analysis include:

- Systematic bases for HSI design requirements
- A control environment based on plant functions and human abilities instead of physical systems
- A sound basis for future HSI assessments
- The prevention or mitigation of human error

This FRA Implementation Plan supports the operational analysis as delineated.

Tables and Appendices are provided as generic examples. The numbering methods (i.e. system configuration, component IDs, etc.) may change during the design process, however, the intent will not be affected. The item identification, for example PFL-1, is provided only for relating items within this document.

1.1 PURPOSE

The purpose of this implementation plan is to prescribe and guide FRA conduct for the ESBWR plant design in accordance with the requirements of the ESBWR MMIS and HFE Implementation Plan [Reference 2.1.1(5)].

The FRA Plan establishes methods to:

- Conduct the FRA consistent with accepted Human Factors Engineering (HFE) methods
- Denote the ESBWR mission, goals, and operating states
- Identify Critical Safety Functions
- Validate system functions identified in the ESBWR System Design Specifications (SDS) from an HFE perspective
- Define the relationships between high-level functions and plant systems
- Reconcile any differences between Plant-level analyses and the SDS
- Develop a functional structure that can be used to assess the impact of design, staffing, training, procedure, and HSI changes on the ability of operators to monitor and coordinate activities

1.2 SCOPE

This Plan establishes the following scope elements for the analysis:

- Objectives, performance requirements, and constraints
- Methods and criteria for conducting the Plant-level Functional Requirements Analysis (PFRA) in accordance with accepted human factors principles and practices
- Methods and criteria for conducting the System Functional Requirements Analysis (SFRA) in accordance with accepted human factors principles and practices
- System requirements that define the system functions
- Resultant system configuration changes which lead to Human System Interface (HSI) requirements
- Critical Safety Functions resulting from Probabilistic Risk Assessment (PRA), HRA, and deterministic evaluations
- Descriptions for each identified function
- Overall system configuration design

To accomplish these objectives, plant-level and system-level goals and functions are systematically analyzed concurrently. The functional relationships between plant functions and system functions are then reconciled through system function gap analysis. The output of this gap analysis is used to ensure that plant-level and system level goals are both met.

FRA results are entered into a data structure during initial design. This data structure is shared with PRA and plant simulation efforts during the pre-operational and operational phases to evaluate the impact of design changes on the HFE aspects of ESBWR.

1.3 DEFINITIONS AND ACRONYMS

1.3.1 Definitions

Configuration Change: An allowable realignment of system components from one configuration to another.

Function (Sub function): An activity or role performed by man, structure or automated system to fulfill an objective.

Functional analysis: The examination of the functional goals of a system with respect to available manpower, technology, and other resources, to provide the basis for determining how the function may be assigned and executed.

Functional goal: The performance objectives that shall be satisfied by the corresponding function(s).

HFE Issue Tracking System (HFEITS): An electronic database used to document human factors engineering issues not resolved through the normal HFE process and human engineering discrepancies (HEDs) from the design verification and validation activities. Additionally, the database is used to document the problem resolutions.

Operational analysis: A structured, documented study and evaluation of plant goals to identify a hierarchy of system functions for operations, and the optimal means by which these functions can be accomplished.

Physical system (Subsystem): An organization of components working together to achieve a common goal(s), such as a function.

System Operating Configuration: A prescribed lineup of system components to complete a function under specified conditions.

System Process: An action or set of actions that must take place to complete a system operation or task.

System Process Element: An individual part or piece of a process whose availability or service is necessary for completion of the process.

System Component Requirement: An individual component required to complete the availability or service of a system process element.

System Support Requirement: A condition, not necessarily a part of the system, that is required to maintain a component available, (i.e. electrical power, isolation signal, etc.).

Systems analysis: A structured, documented study and evaluation of system goals to identify a hierarchy of functions for operations, and the optimal means by which these functions can be accomplished.

1.3.2 Acronyms

The following is a list of acronyms used in this plan:

Acronym	Description
AOF	Allocation of Function
AOO	Anticipated Operational Occurrence
AOP	Abnormal Operating Procedure
BRR	Baseline Review Record
COL	Combined Operating License
D3	Defense-in-Depth and Diversity
DCIS	Distributed Control and Information System
EOP	Emergency Operating Procedure
FRA	Functional Requirements Analysis
HA	Human Action
HFE	Human Factors Engineering
HFEITS	Human Factors Engineering Issues Tracking System
HRA	Human Reliability Analysis
HSI	Human System Interface
IOP	Integrated Operating Procedure
MMIS	Man-Machine Interface System
MPL	Master Parts List
NPP	Nuclear Power Plant (ESBWR)
OER	Operating Experience Review
P&ID	Piping and Instrumentation Drawing
PFRA	Plant-level Functional Requirements Analysis
PRA	Probabilistic Risk Assessment
RSR	Results Summary Report
RWCU	Reactor Water Cleanup
S&Q	Staffing and Qualifications
SDC	Shutdown Cooling
SDS	System Design Specification
SFGA	System Function Gap Analysis
SFRA	System Functional Requirements Analysis

TA	Task Analysis

2. APPLICABLE DOCUMENTS

Applicable documents include supporting documents, supplemental documents, codes and standards and are given in this section. Supporting documents provide the input requirements to this plan. Supplemental documents are used in conjunction with this plan. Codes and standards are applicable to this plan to the extent specified herein.

2.1 SUPPORTING AND SUPPLEMENTAL GE DOCUMENTS

2.1.1 Supporting Documents

The following supporting documents were used as the controlling documents in the production of this plan. These documents form the design basis traceability for the requirements outlined in this plan.

(1) ESBWR DCD Chapter 6 (GE26A6642AT)

(2) ESBWR DCD Chapter 18 (GE26A6642BX)

(3) ESBWR DCD Chapter 15 (GE26A6642BP)

(4) ESBWR DCD Chapter 19 (GE26A6642BY)

(5) NEDE-33217P and NEDO-33217, ESBWR Man-Machine Interface System and Human Factors Engineering Implementation Plan

2.1.2 Supplemental Documents

The following supplemental documents are used in conjunction with this document plan:

(1) NEDE-33220P and NEDO-33220, ESBWR HFE Allocation of Function Implementation Plan.

(2) NEDE-33221P and NEDO-33221, ESBWR HFE Task Analysis Implementation Plan.

(3) NEDO-33251, ESBWR Defense-in-Depth and Diversity Plan.

(4) NEDO-33262, ESBWR HFE Operating Experience Review Implementation Plan.

(5) NEDO-33267, ESBWR HFE Human Reliability Analysis Implementation Plan.

(6) NEDE-33268P and NEDO-33268, ESBWR HFE Human-System Interface Design Implementation Plan.

(7) NEDO-33274, ESBWR HFE Procedures Development Implementation Plan.

(8) NEDO-33275, ESBWR HFE Training Program Development Implementation Plan.

(9) NEDE-33276P and NEDO-33276, ESBWR HFE Verification and Validation Implementation Plan.

2.2 CODES AND STANDARDS

The following codes and standards are applicable to the HFE program to the extent specified herein.

(1) IEEE Std 1023-2004, Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities, 2004.

2.3 REGULATORY GUIDELINES

(1) NUREG-0700, Rev 2, Human System Interface Design Review Guidelines, 2002.

(2) NUREG-0711, Rev 2, Human Factors Engineering Program Review Model, 2004.

(3) NUREG-0800, Rev 1, Standard Review Plan, Chapter 18 – Human Factors Engineering, 2004.

(4) 10 CFR 20, Standards for Protection Against Radiation.

(5) 10 CFR 50, Appendix A, General Design Criteria for Nuclear Power Plants.

(6) 10 CFR 100, Reactor Site Criteria.

2.4 DOD AND DOE DOCUMENTS

None.

2.5 INDUSTRY/OTHER DOCUMENTS

None.

3. METHODS

The Functional Requirements Analysis (FRA):

(1) Coordinates and implements plans in accordance with NRC guidelines

(2) Performs a "top down" plant-level analysis of the plant functions

(3) Performs a per-system analysis of the design functions

(4) Performs a gap analyses to reconcile the top-down and per-system analyses

(5) Executes the HFE plans iteratively from the early design phase through turnover to the COL Applicants

(6) Follows accepted HFE and I&C practices and processes

(7) Follows the activities for HSI design and system hardware/software design

(8) Meets the commitments of ESBWR DCD Chapter 18

3.1 PLANT-LEVEL FUNCTIONAL REQUIREMENTS ANALYSIS

The PFRA addresses defense-in-depth, system interdependence, and interaction. PFRA is performed in three phases:

(1) High-level PFRA

(2) Design PFRA

(3) Detailed PFRA

The High-level PFRA is performed early in the design process and identifies critical safety functions, Emergency Operating Procedure (EOP) outlines, and an inventory of accident monitoring parameters. The Design PFRA includes plant goals and functions that support the ESBWR mission of generating safe economic electric power during all plant operating modes (shutdown, refueling, startup, and run) and provide the basis for the plant operating procedures. The Detailed PFRA, the third iteration of FRA, provides high-level Abnormal Operating Procedure (AOP) outlines.

3.1.1 Background

The PFRA is the first step of the "top down" approach to the HFE design, as illustrated in Figure 3, Functional Requirements Analyses Flowchart. The process begins with the ESBWR mission and analyzes plant functions for all operating modes to determine functions that must be completed to meet the plant goals.

3.1.2 Goals

The PFRA yields a data structure that describes the plant function requirements. This data structure is rendered to provide inventories of required parameters and outlines for EOPs and AOPs. PFRA provides required inputs to AOF and TA.

3.1.3 Basis and Requirements

The PFRA incorporates the following:

- Plant experts to perform the PFRA
- Concurrent performance with SFRA
- Integration of HFE early in the design process
- Creation and maintenance of a data structure that demonstrates the interdependence of plant functions

The PFRA meets the functional requirements analysis guidance of NUREG 0711, Rev 2, Section 4, and NUREG 0800, Rev 1, Chapter 18.

3.1.4 General Approach

The PFRA provides an integrated top down approach to functional analyses by linking plant-level goals, functions, interdependencies, and redundancies with system level functions.

3.1.5 Application

The results of the PFRA and the SFRA are used in the System Function Gap Analysis (SFGA). The SFGA ensures the plant performance requirements are met by the system functions. Any differences between the system functions, used as inputs to the SFRA and the PFRA results, are either reconciled or become design inputs, as shown in Figure 6, System Function Gap Analyses.

The analysis tool is a data structure that can be rendered as functional diagrams. These diagrams illustrate the different combinations of system functions, sub-functions, equipment, and components required to support the plant goals under analysis.

The data structure is shared between the HFE, PRA, and simulation activities to minimize the amount of duplicated efforts, and to ensure inter-group consistency of data. The data structure will be transformable to the presentation and content required by each different activity. Examples of included information are:

- ESBWR mission
- Plant goals
- System functions
- System dependencies
- System actuation requirements
- Plant-level functions

3.2 SYSTEM FUNCTIONAL REQUIREMENTS ANALYSIS METHOD

The SFRA creates a data structure that links system functions described in the SDS to subsystems, equipment and components. The process also develops system alignments and alignment changes required to support system functions. The SFRA is performed in phases with the other elements of operational analysis as illustrated by Figure 2.

3.2.1 Background

The SFRA is the second step of the "top down" approach to FRA. This approach is illustrated in Figure 3, Functional Requirements Analyses Flowchart. The SFRA process analyzes each system and its functions to determine individual task requirements necessary to meet the plant objectives.

3.2.2 Goals

The SFRA yields a data structure that describes the functional dependencies within systems and the relationship between systems. The data structure provides system lineups and component manipulations as inputs to the AOF and TA.

3.2.3 Basis and Requirements

The SFRA incorporates the following:

- System experts to perform the SFRA
- Concurrent performance with PFRA
- HFE input early in the design process

The SFRA meets the functional guidance of NUREG 0711, Rev 2, Section 4, and NUREG 0800, Rev 1, Chapter 18.

3.2.4 General Approach

This method is similar to methods developed to determine the plant functional requirements. The analysis progresses from the system functions, as described in the System Design Specification (SDS), and moves toward determination of the system performance requirements.

The SFRA is performed concurrently with the PFRA. Systems, as a group of functions, are analyzed instead of by individual functions because:

- Information available for analysis is provided by the SDS.
- All the functions of a system are performed within the system components.
- Local control is designed on the basis of systems rather than functions.

When the SFRA is linked to the PFRA, a data structure linking the plant mission to individual components such as pump, valve, and heat exchanger is created.

The results provide input to the AOF, which determines whether the functions are assigned to the human, the machine, or shared (both human and machine). These functional assignments are studied during TA and HSI design.

3.2.5 Application

The results of the PFRA and the SFRA are inputs for the gap analyses. Together, the PFRA, SFRA, and SFGA ensure that plant performance requirements are met by the system functions. Any differences between the system functions (as input to the SFRA and the PFRA results) are

either reconciled or become design inputs (see Figure 3, Functional Requirements Analyses Flowchart).

3.3 SYSTEM FUNCTION GAP ANALYSIS METHOD

The System Function Gap Analysis (SFGA) addresses discontinuities between the Design PFRA and the SFRA. The High-level PFRA is performed during the design process and identifies an inventory of accident monitoring parameters. The SFGA ensures that plant goals are supported by system functions.

3.3.1 Background

The SFGA is the third step of the "top-down" approach to FRA. This is illustrated in Figure 6, System Function Gap Analyses. The process looks at each process function produced by the PFRA and the system functions from the SDS that are used as inputs to SFRA. Any differences are analyzed to ensure that the system functions required to support plant-level requirements meet the plant safety objectives.

Functional differences that cannot be reconciled are entered into HFE Issue Tracking System (HFEITS) or become design inputs into the ESBWR engineering change process, as described in the MMIS and HFE Implementation Plan, Reference 2.1.1(5).

3.3.2 Goals

The SFGA links the PFRA and SFRA data structures creating a data structure that describes the plant function requirements down to the component level. The SFGA generates design inputs to ensure that the design fulfills the ESBWR mission and goals. This data structure provides inventories of required parameters, indication and controls, and outlines for EOPs and AOPs. The FRA provides required inputs to the ESBWR engineering change process, AOF and TA.

3.3.3 Basis and Requirements

The SFGA incorporates the following:

- Plant operation and integration experts to perform the SFGA
- Provide design inputs to resolve differences between PFRA outputs and SFRA inputs
- Document and track system function differences to resolution using the HFEITS
- Reconcile the PFRA to the SFRA
- Integrate HFE principles early in the design process

The SFGA meets the functional requirements analysis of NUREG 0711, Rev 2, Section 4, and NUREG 0800, Rev 1, Chapter 18.

3.3.4 General Approach

The SFGA supports an integrated top-down approach to functional analyses by linking plant-level function, interdependencies, and redundancies with system level functions. The SFGA is performed subsequent to the plant-level and system-level functional analyses. The differences

between functional requirements and system design are provided to the system engineers as design inputs to align system design with plant functional requirements.

3.3.5 Application

The SFGA ensures that the PFRA results are reconciled to the SFRA at the system function level and that plant performance requirements are met by the system functions. Any differences between the functions used as inputs to the SFRA and the PFRA results are either reconciled or become design inputs (Refer to Figure 6, System Function Gap Analyses) to recommend additional required functions to systems or remove extraneous features that do not support a required function.

4. IMPLEMENTATION

4.1 PLANT-LEVEL FUNCTIONAL REQUIREMENTS ANALYSIS IMPLEMENTATION

The HFE team performs the PFRA and employs a data structure to record and render system functions and interfaces.

4.1.1 Assumptions

This analysis assumes:

- The ESBWR mission is safe economical power generation
- Plant-level performance requirements support the ESBWR mission
- Plant-level functions satisfy the plant-level performance requirements
- System functions support plant-level functions
- Single failures leading to a plant scram, turbine trip, or unplanned power change are minimized
- Gap analysis reconciles differences in plant and system requirements between PFRA and SFRA
- Gap analysis provides feedback into the design process ensuring the plant performance requirements are satisfied

4.1.2 Inputs

PFRA inputs include:

- OER and BRR
- PRA and HRA
- ESBWR plant specific analyses, as described in the DCD
- FRA, AOF, and TA Results Summary Reports from previous iterations
- Design changes

4.1.3 Process

Each step of the PFRA process is documented in an organized data structure. The elements of the data structure are linked by logic operators such as “AND” and “OR.”

4.1.3.1 *Plant Goal Identification (PFL-1)*

Develop plant goals that support the ESBWR mission of safe economical power generation. Plant goals that support the ESBWR mission include:

- Limit Radionuclide Release
- Operate Economically and Protect Economic Operation

4.1.3.2 *Nuclear Power Plant Condition Identification (PFL-2)*

NPP conditions provide the operational framework for evaluating associated Sub Goals. For example, the Plant Goal of Limit Radionuclide Release includes the three NPP conditions:

- Accident (maintain less than 10 CFR 100 dose limits)
- Anticipated Operational Occurrences including Normal Operation (maintain less than 10 CFR 20 dose limits)
- Severe Accident (mitigate dose release to maximum extent possible)

4.1.3.3 *Plant State Identification (PFL-3)*

Develop lists of plant states applicable to each plant goal. For example, the plant states for economic operation include:

- Power operation
- Startup
- Shutdown
- Refueling

4.1.3.4 *Plant Sub Goal Identification (PFL-4)*

The Plant Goals are divided into two categories; a Plant Safety Goal (Limit Radionuclide Release) and a Plant Generation and Availability Goal (Operate Economically and Protect Economic Operation).

The Plant Safety Sub Goals that support the Plant Safety Goal to limit radionuclide release are developed from 10 CFR 50 Appendix A "General Design Criteria for Nuclear Power Plants (GDC)". The detailed PFRA will also review DCD Chapter 6 "Engineered Safety Features", DCD Chapter 15 "Safety Analysis" and DCD Chapter 19 "Probabilistic Risk Assessment and Severe Accidents".

The Plant Generation and Availability Sub Goals are developed from the basic steam power cycle as applied to the NPP Process and energy transformations. The startup, power operations, shutdown and refueling states required for plant operation are considered in the development of Availability and Generation Sub Goals.

4.1.3.5 *Plant Function Identification (PFL-5)*

High-level functions for safe operation are developed from the Safety Sub Goals and Plant Generation and Availability Sub Goals. Plant Functions that support the Plant Sub Goals are developed and identified and Plant Process Functions (Sub Functions) that support the Plant Functions are developed and identified.

As stated previously, the Plant Goals are divided into two categories; a Plant Safety Goal (Limit Radionuclide Release) and a Plant Generation and Availability Goal (Operate Economically and Protect Economic Operation). The two categories for plant Goals are broken down to obtain Plant Sub Goals and high-level Plant Functions (Safety and Availability).

The requirements of the high-level function are identified at the Process Function (Sub Function) level where control and/or monitoring capability of the parameters that support the high level function are identified.

4.1.3.6 *Plant Redundancy Identification (PFL-6)*

Identify if train, channel, and division redundancy is required to support plant functions. The bases for redundancy include:

- General Design Criteria
- Defense-in-Depth and Diversity
- Desired reliability
- Redundancy for maintenance of subsystems and components

4.1.3.7 *Critical Safety Function Identification (PFL-7)*

Identify Critical Safety Functions that support the Plant Safety Sub Goals. A plant function will be considered a Critical Safety Function if it meets any of the following criteria:

- A Function will be considered a Critical Safety Function, when it's failure would not allow achievement of safety system performance requirements, OR
- When it's failure could pose a safety hazard to plant personnel or to the general public, OR
- If that function prevents or mitigates any of the criteria in ESBWR DCD Chapter 15/Tier 2 Rev. 5, Tables 15.0-3, 4, 5, 6. These Tables list the safety analysis acceptance criteria required for Normal Operation, including Anticipated Operational Occurrences (AOO) and AOO in combination with an additional single active component failure or single operator error, Infrequent Events and Accidents, OR
- If the Plant Function prevents or mitigates the following DCD Chapter 19 Probabilistic Risk Assessment and Severe Accidents Acceptance Criteria for internal events:
  - **Reactivity Control** - The acceptance criterion is to achieve sub-criticality and maintain the reactor in a sub-critical state.
  - **RPV Overpressure Protection -** A pressure of 150 percent of the reactor coolant pressure boundary design pressure is defined as the acceptance criteria for the RPV overpressure protection.
  - **Core Cooling** - A peak cladding temperature of 2200ºF is defined as the criterion for establishing the adequacy of core cooling.
  - **Containment Heat Removal** - The acceptance criterion for the containment cooling function is to maintain the pressure below the ultimate containment failure pressure, which is provided in Appendix 19C.

4.1.3.8 *Plant Process Function Identification (PFL-8)*

Identify those Plant Process Functions that are required to support Plant Functions. Plant Process Functions monitor and control parameters supporting the Plant Functions.

4.1.4 Outputs

The results of the PFRA produce inputs to the Allocation of Functions as well as the Task Analysis. This process produces an organized data structure containing the following:

- Plant goals
- Plant states
- Plant processes
- Procedure process (EOP, IOP, and AOP) outlines
- Plant process and function redundancies
- Critical Safety Functions
- Plant functions and sub-functions
- Inventory of critical safety parameters
- Requirements for HSI design
- Outlines for simulator scenarios

4.2 SYSTEM FUNCTIONAL REQUIREMENTS ANALYSIS IMPLEMENTATION

The SFRA is the responsibility of the responsible system engineer and is facilitated by the HFE team. The system engineers ensure that the SFRAs accurately model function and sub-function interdependence. The HFE team provides:

- Training and process oversight
- Plant operations experience
- Data structure to record and render system functions and interfaces
- Human behavioral science expertise
- Consistency among SFRAs

4.2.1 Assumptions

This analysis assumes:

- The System design satisfies the plant performance requirements
- The Gap analysis reconciles differences in plant and system requirements between PFRA and SFRA
- The Gap analysis provides feedback into the design process ensuring the Plant Performance Requirements are satisfied

4.2.2 Inputs

The SFRA inputs include:

- OER and BRR
- PRA and HRA
- FRA, AOF, and TA data structures from previous iterations
- ESBWR System Design Specification (SDS)
- Design changes

4.2.3 Process

4.2.3.1 *System Redundancy Identification (SFL-1)*

Identify trains, divisions and/or channels that perform the same function. Systems are designed with identical redundant trains to satisfy plant operational maintenance requirements as well as defense-in-depth and diversity requirements. This redundant train design is stipulated in the SDS and is documented in this step of the SFRA. Identifying the trains simplifies the data structure generated by this process. The function identification step follows due to independent train redundancy being system-dependent and not function-dependent.

This is represented in the following block diagram:

4.2.3.2 *System Function Identification (SFL-2)*

Extract the system functions from the System Design Specifications (SDS) and re-state them in terms of the SFRA. Some of these functions may be performed concurrently, or independently, as necessary to support the various modes of Reactor operation; therefore, the Reactor mode applicability is delineated for each function. An example of functions derived from the SDS, analysis of the RWCU/SDC system for the ESBWR, is presented in Appendix A.

4.2.3.3 *System Process Identification (SFL-3)*

Determine the basic process steps necessary for the system to satisfactorily complete the function for each function identified in the System Function Identification (SFL-2) level. Functions may not require all the system processes. For example, the reheat process, which is necessary for RWCU during power operation, is not required during refueling operation. Use the following criteria to break down the system processes:

- The processes are required to accomplish the function
- The processes are as basic as possible
- The processes are independent of one another

The example in Appendix B shows how the criteria above is applied using the ESBWR RWCU system function of “Control reactor water chemistry.”

4.2.3.4 *System Processing Elements Identification (SFL-4)*

Identify the support elements necessary to achieve the process using the following criteria:

- The system elements considered are related to the function and process
- The requirements of the process provide the bases for availability
- The alternatives are considered to accomplish the process

For example, if the return path of a hydraulic circuit may be established via two parallel valves, then two process elements exist, one for each valve. This arrangement is represented in the data structure as an OR gate.

An example of the transport reactor water process, using the criteria listed above, is provided in Appendix C.

4.2.3.5 *System Component Requirements Identification (SFL-5)*

Identify the required components for each process element, including the status of each required component:

- P&IDs identify the necessary components required to complete the process elements identified above.
- Components are grouped to constitute Functional Equipment Groups.
- Analyses of these components and their required status (to complete process elements) result in the identification of the system alignments required to perform the function.

The following criteria are considered while performing SFRA component requirement identification:

- All system components, including locally operated components. Each component should be specified clearly. Referenced components are identified by their type of function (LCV, PCV, TCV, etc.), Master Parts List (MPL) or equivalent identifier, and component number.
- The status of the components performing the function.
- Special operations such as equipment tests, conditioning, and maintenance. These are only studied during the economic SFRA. For example, changing of the filter element in the RWCU system is not analyzed during the Design SFRA.
- During Design SFRA, local operations are viewed at a global level. Status such as heat exchanger vented and filled, or pump start prerequisites met, express the availability of these components. The necessary maintenance operations are analyzed during economic SFRA as part of the requirements relating to component operability.

An example of the component requirements process using the criteria listed above is provided in Appendix D.

4.2.3.6 *System Support Requirements Identification (SFL-6)*

Identify the conditions required for each of the process element components.

The support level matches with the low-level logic diagrams for components. These supports should include motive force requirements (i.e. pneumatics, electricity, hydraulics, etc.), control signal requirements, cooling, etc.

An example of support requirements are necessary to maintain the RWCU pump in an operable status is provided in Appendix E.

4.2.3.7 *System Alignment Identification (SFL-7)*

Identify system alignments that are capable of performing each function.

System alignments are identified by a unique letter number combination. A result derived from level SFL-5 is the acquisition of all the system component alignments possible for performance of the function to be achieved. Correct interpretation of the logic gates used in the functional logic diagram makes it possible to identify all the possible component alignments capable of ensuring the function.

Examples of system alignments and alignment changes are provided in Appendix F.

4.2.3.8 *Configuration Change Identification (SFL-8)*

Identify all allowable transitions between the system configurations and create a matrix of all component status changes that are required to change alignments.

4.2.4 Outputs

The results of the SFRA are documented in the applicable SDS appendices and provide inputs to the Allocation of Function and Task Analysis Plans. This process produces the following output:

- System Operating Configurations
- System Configuration Changes
- Component Lineups
- Component manipulations required to change configurations, as defined for normal and abnormal system operating procedure development
- Functional logic diagrams

4.3 SYSTEM FUNCTION GAP ANALYSIS IMPLEMENTATION

The HFE team performs the SFGA and employs a data structure to record and render the plant process function to system function links.

4.3.1 Assumptions

This analysis assumes:

- Plant performance requirements are captured by the PFRA
- System functions are accurately identified by SFRA
- Gap analysis provides feedback into the design process ensuring the Plant Performance Requirements are satisfied

4.3.2 Inputs

SFGA inputs include PFRA results and functions derived from the SDS by the SFRA in the "System Function Identification" step.

4.3.3 Process

4.3.3.1 *Function Comparison*

Compare and match plant process functions and system functions.

4.3.3.2 *Link PFRA to SFRA*

Tie the PFRA data structure to the SFRA data structure where system function(s) can perform the PFRA plant process function.

4.3.3.3 *Determine Differences*

Identify plant process functions that are not supported by a system function.

4.3.3.4 *Validate Systems Functions*

Identify system functions that do not support plant functions.

4.3.3.5 *Resolve Differences*

Reconcile discontinuities between PFRA and SFRA where possible.

4.3.3.6 *Create Design Inputs*

When plant functions are not supported by system functions:

- Verify that the plant requirements are necessary
- Process the design input according to the MMIS and HFE Implementation Plan
- Provide the Responsible System engineer with design inputs
- Re-perform the applicable portion of the FRA to confirm resolution
- Document the out of process issues in HFEITS

4.3.3.7 *Validate Design Input Effectiveness*

When system functions are not required based on the PFRA:

- Verify that the system functions are required or are justified
- Process the design input according to the MMIS and HFE Implementation Plan
- Provide the Responsible System engineer with design inputs
- Re-perform the applicable portion of the FRA to confirm resolution
- Document the out of process issues in HFEITS

4.3.3.8 *Plant Function Operational Summary*

Determine the following for each high-level plant function related to the plant safety goal.

- Purpose of the plant function
- The plant condition(s) which require the plant function
- Parameter(s) that represent the availability of the plant system designated to support the plant function
- Parameter(s) that represent operation of the plant system in support of the plant function
- Parameter(s) that represent the success of the plant system in support of the function
- Parameter(s) that represent when support of the function from the plant system can or should be terminated.

4.3.4 Outputs

The results of the SFGA generate:

- Design inputs
- Links between the PFRA and SFRA data structures
- Inputs to subsequent iterations of the FRA, AOF, and TA
- A relationship between FRA and requirements for HSI design
- A Plant function operational summary for high-level functions that support plant safety

5. RESULTS

5.1 RESULTS SUMMARY REPORT

The results of the Functional Requirements Analysis are summarized in a Results Summary Report (RSR). This report is the main source of information used to demonstrate that efforts conducted in accordance with the implementation plan satisfy the applicable review criteria of NUREG-0800. The report contains the following:

- General approach including the purpose and scope of the Functional Requirements Analysis.
- The functional hierarchy for each plant safety function including the identification of Critical Safety Functions.
- The plant systems and configurations that support each plant safety function
- The plant function operational summary for each high-level plant function that specifies when support of the function is required and specifies the parameters necessary to monitor availability, operation, and success of this support.

The FRA RSR may be combined with the AOF and/or TA RSRs.

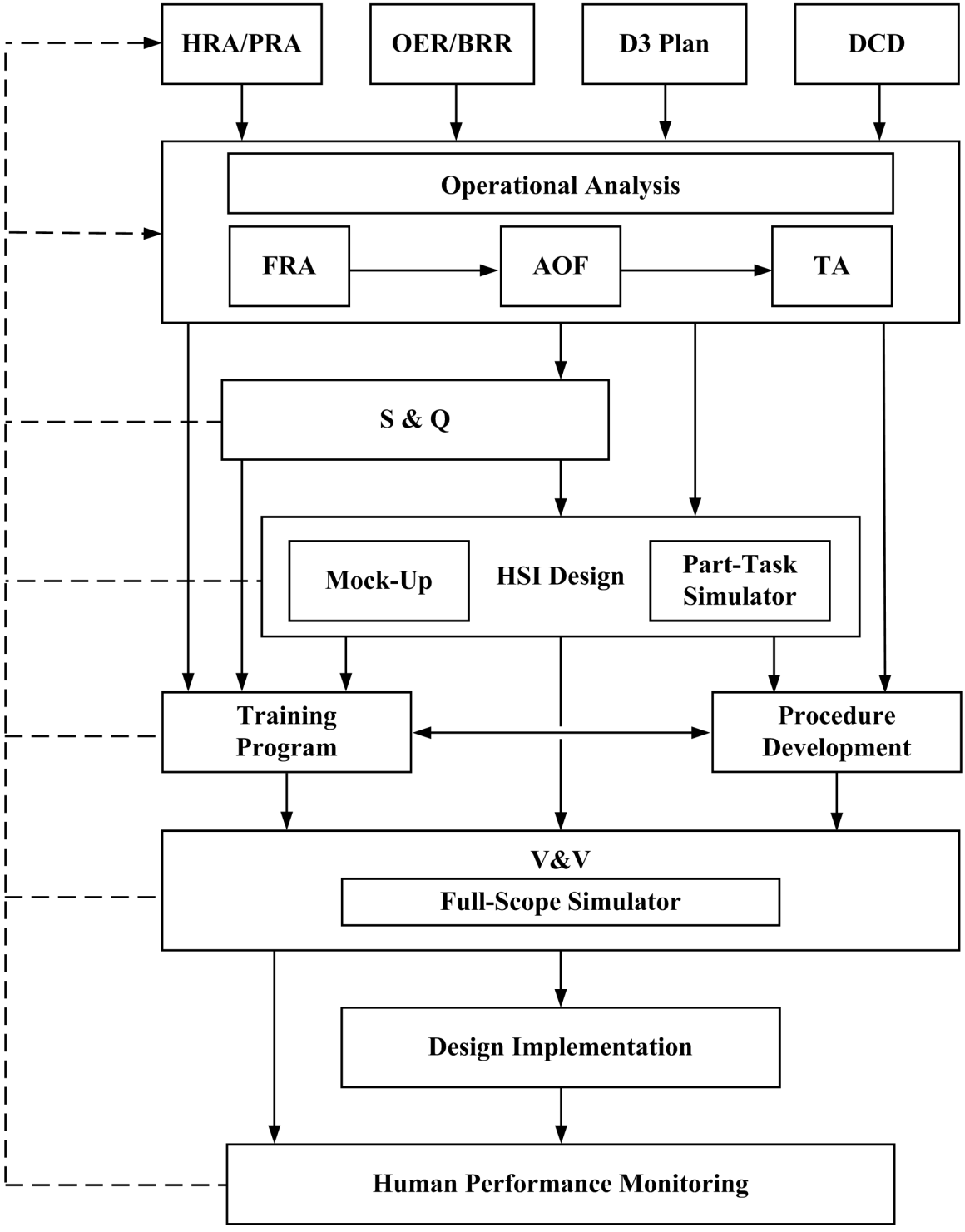
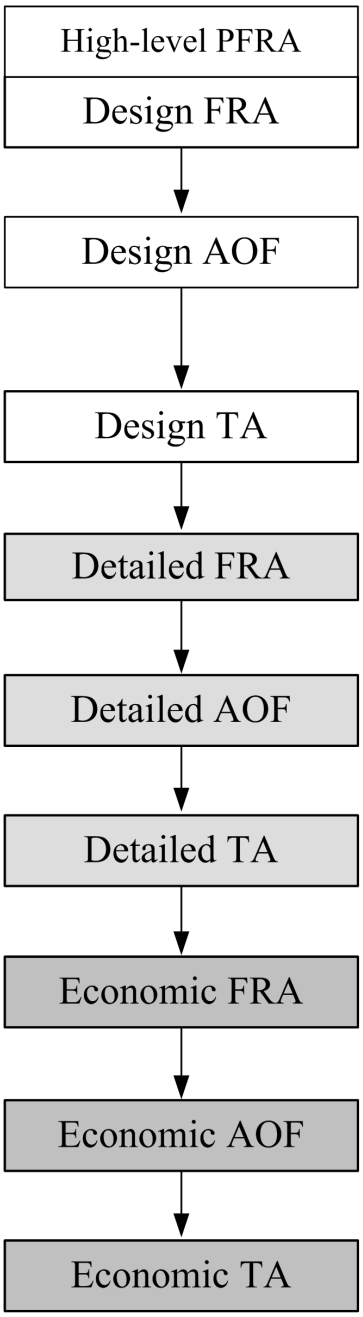


Figure 1. HFE Implementation Process



Outputs

- Critical safety functions & system functions
- Design inputs logic, SDS, P&ID
- System alignments/alignment changes
- Identification of high-level functions and tasks

- Safety/Non-safety
- Automation
- Auto
- Human

- Task description and sequence
- Procedure outlines
- Inventory of indication and controls

- Inventory of indication and controls
- Support function and task identification
- Maintenance and testing functions

- Control hierarchy
- Alarm presentation and priority
- DCIS diagnostics

- Task sequence priority
- Procedure outlines

- Identification of testing and maintenance functions
- Incorporation of design, analysis and task changes

- Auto tasks for surveillance, testing and calibration
- Human tasks for surveillance, testing and calibration

- Integration of maintenance and testing with operation
- Surveillance procedure development
- Maintenance procedure development
- Tagout/Lockout process

Figure 2. Operational Analysis Iterations

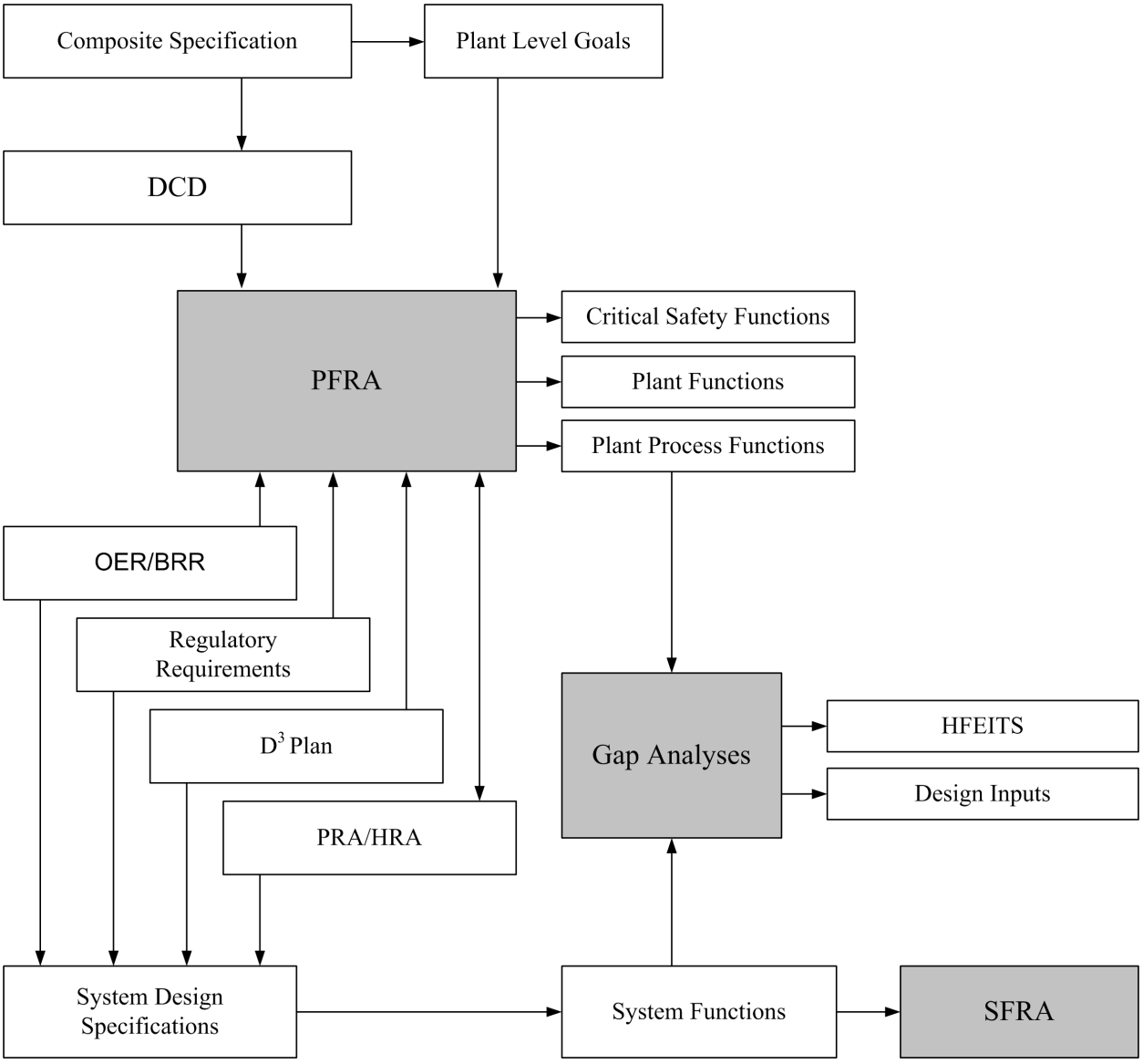


Figure 3. Functional Requirements Analyses Flowchart

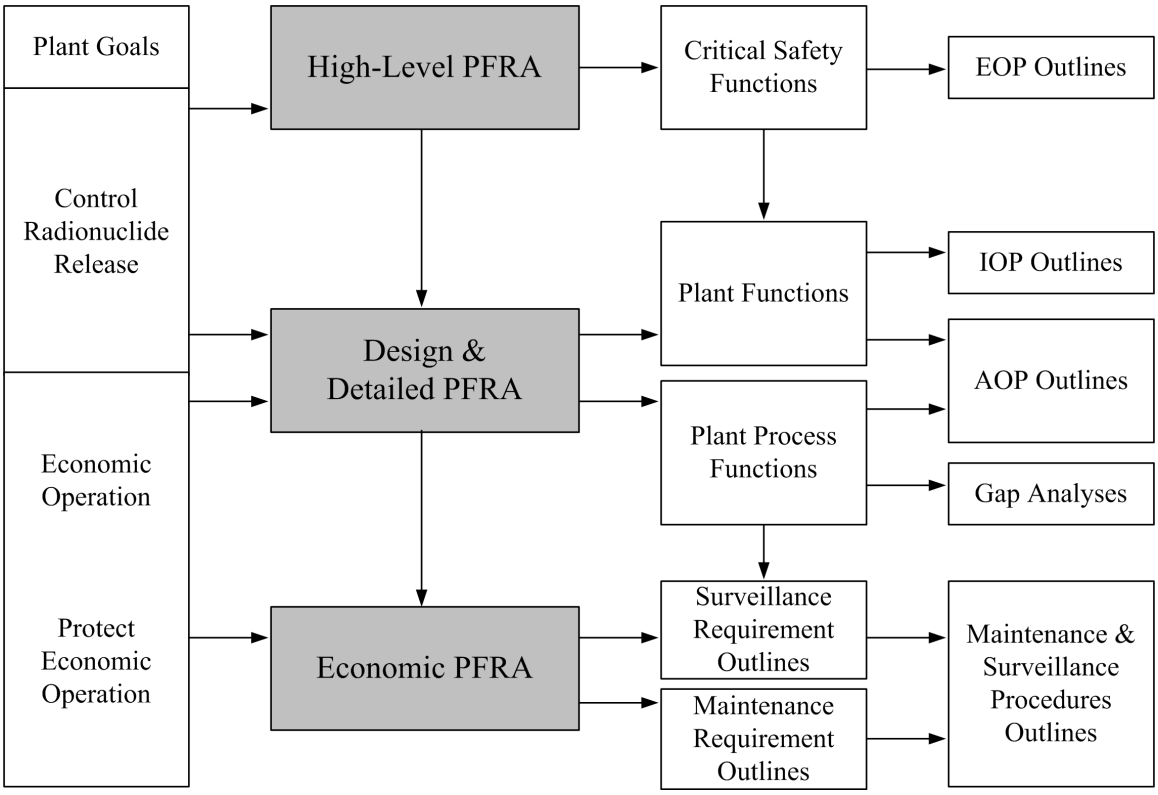


Figure 4. Plant-level FRA Iterations

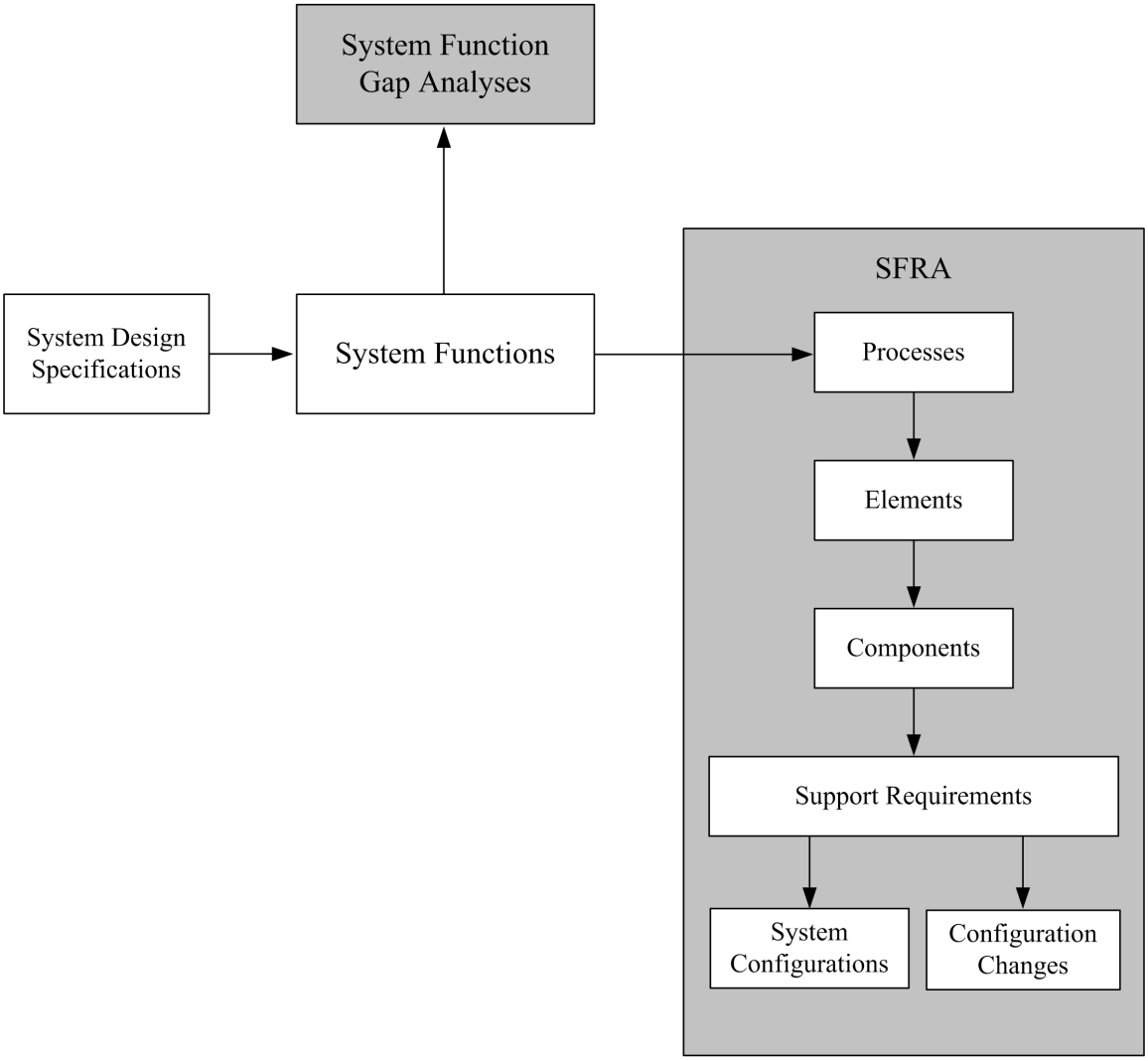


Figure 5. System Functional Requirements Analyses

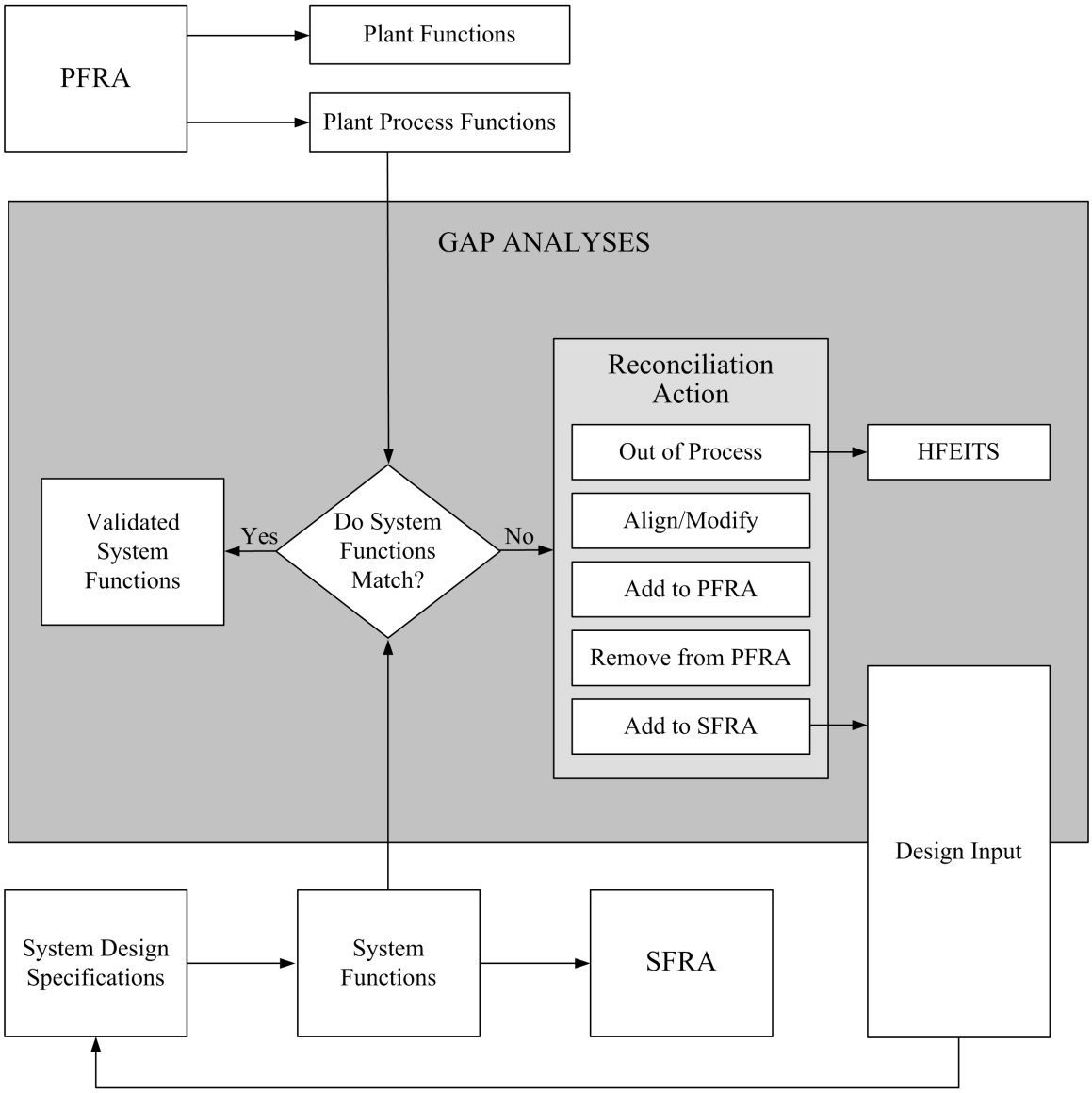


Figure 6. System Function Gap Analyses

Table 1
ESBWR RWCU System Configuration Table - Example

Component	Description	System Configuration					
		0	A1	A2	A3	B1	B2
F001A	Mid Vessel Manual Suction Valve	Closed	Open	Open	Open	Open	Open
F002A	Mid Vessel Inbd Isolation Valve	Closed	Open	Closed	Closed	Closed	Open
F003A	Mid Vessel Outbd Isolation Valve	Closed	Open	Closed	Closed	Closed	Open
F004A	Mid Vessel Flow Control Valve	Closed	Open	Closed	Closed	Closed	Open
F005A	Bottom Vessel Manual Suction Vlv	Closed	Open	Open	Open	Open	Open
F006A	Bottom Vessel Manual Suction Vlv	Closed	Open	Open	Open	Open	Open
F007A	Bottom Vessel Inbd Isolation Valve	Closed	Open	Open	Open	Open	Open
F008A	Bottom Vessel Outbd Isolation Vlv	Closed	Open	Open	Open	Open	Open
F044A	Bottom Vessel Suction MOV	Closed	Open	Open	Open	Open	Open
F009A	RHX Tube Side Bypass Valve	Closed	Open	Open	Open	Open	Open
F010A	Low Capacity Pump Suction Valve	Closed	Open	Open	Open	Open	Open
F012A	Low Capacity Pump Discharge Vlv	Closed	Open	Open	Open	Open	Open
F013A	High Capacity Pump Suction Valve	Closed	Closed	Closed	Closed	Closed	Closed
F015A	High Capacity Pump Discharge Vlv	Closed	Closed	Closed	Closed	Closed	Closed
F016A	Filter/Demin Inlet Valve	Closed	Open	Closed	Open	Open	Closed
F018A	Filter/Demin Outlet Valve	Closed	Open	Closed	Open	Open	Closed
F019A	Filter/Demin Bypass Valve	Auto	Auto	Auto	Auto	Auto	Auto
F020A	RHX Shell Side Inlet Valve	Closed	Closed	Closed	Closed	Closed	Closed
F021A	RHX Shell Side Bypass Valve	Closed	Closed	Closed	Open	Open	Closed
F022A	Injection Line Isolation Valve	Closed	Closed	Closed	Open	Open	Closed
F025A	Overboard Isolation Valve	Closed	Open	Open	Open	Open	Open
F030A	Train B Crosstie Isolation Valve	Closed	Closed	Closed	Closed	Closed	Closed
C001A	Lower Capacity Pump	OFF	ON	ON	ON	ON	ON
C002A	Higher Capacity Pump	OFF	OFF	OFF	OFF	OFF	OFF
D004A	Filter/Demin	OOS	I/S	OOS	I/S	I/S	OOS

Legend: I/S: In Service OOS: Out of service

Note: This table is provided as an example only of the ESBWR RWCU system according to the information available at the time of document revision and does not necessarily reflect the actual final system components.

Table 2
ESBWR RWCU Configuration Change Table Example

Component	Description	System Configurations		Configuration Change
		A1	A2	A1→A2
F001A	Mid Vessel Manual Suction Valve	Open	Open	
F002A	Mid Vessel Inboard Isolation Valve	Open	Closed	Close
F003A	Mid Vessel Outboard Isolation Valve	Open	Closed	Close
F004A	Mid Vessel Flow Control Valve	Open	Closed	Close
F005A	Bottom Vessel Manual Suction Vlv	Open	Open	
F006A	Bottom Vessel Manual Suction Vlv	Open	Open	
F007A	Bottom Vessel Inbd Isolation Valve	Open	Open	
F008A	Bottom Vessel Outbd Isolation Vlv	Open	Open	
F044A	Bottom Vessel Suction MOV	Open	Open	
F009A	RHX Tube Side Bypass Valve	Open	Open	
F010A	Low Capacity Pump Suction Valve	Open	Open	
F012A	Low Capacity Pump Discharge Vlv	Open	Open	
F013A	High Capacity Pump Suction Valve	Closed	Closed	
F015A	High Capacity Pump Discharge Vlv	Closed	Closed	
F016A	Filter/Demin Inlet Valve	Open	Closed	Close
F018A	Filter/Demin Outlet Valve	Open	Closed	Close
F019A	Filter/Demin Bypass Valve	Auto	Auto	
F020A	RHX Shell Side Inlet Valve	Closed	Closed	
F021A	RHX Shell Side Bypass Valve	Closed	Closed	
F022A	Injection Line Isolation Valve	Closed	Closed	
F025A	Overboard Isolation Valve	Open	Open	
F030A	Train B Crosstie Isolation Valve	Closed	Closed	
C001A	Lower Capacity Pump	ON	ON	
C002A	Higher Capacity Pump	OFF	OFF	
D004A	Filter/Demin	I/S	OOS	Remove

Table 3
ESBWR RWCU Configuration Change Matrix Example

		FROM									
		A1	A2	A3	B1	B2	C1	D1	D2	D3	D4
TO	A1		YES	YES	YES	YES	YES	YES	YES	YES	YES
	A2	YES		YES	YES	YES	YES	YES	YES	YES	YES
	A3	YES	YES		YES	YES	YES	YES	YES	YES	YES
	B1	YES	YES	YES		YES	YES	YES	YES	YES	YES
	B2	YES	YES	YES	YES		YES	YES	YES	YES	YES
	C1	YES	YES	YES	YES	YES		YES	YES	YES	YES
	D1	YES	YES	YES	YES	YES	YES		YES	YES	YES
	D2	YES	YES	YES	YES	YES	YES	YES		YES	YES
	D3	YES	YES	YES	YES	YES	YES	YES	YES		YES
	D4	YES	YES	YES	YES	YES	YES	YES	YES	YES	

Appendix A System Function Identification (SFL-2) Example

Function as Described in the SDS	Applicable Reactor Modes					
Control reactor water chemistry	1	2	3	4	5	6
Control reactor water level during startup, shutdown, and hot standby		2	3	4	5	
Control reactor vessel cool-down and temperature while shutdown			3	4	5	6
Control reactor vessel heat-up for hydrostatic testing and reactor startup		2			5	

Appendix B System Function Processes Identification Example (SFL-3)

Function Processes Identification

What basic processes must the system perform in order to meet the system function?

In order for the RWCU system to control reactor water chemistry it must perform the following:

(1) Remove the water from the Reactor Vessel.

(2) Move the water through the system.

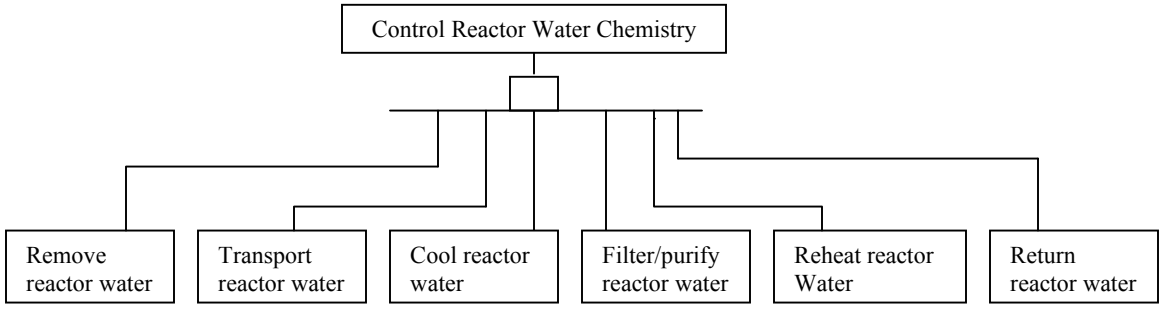
(3) Cool the reactor water.

(4) Filter/purify the reactor water.

(5) Reheat the reactor water.

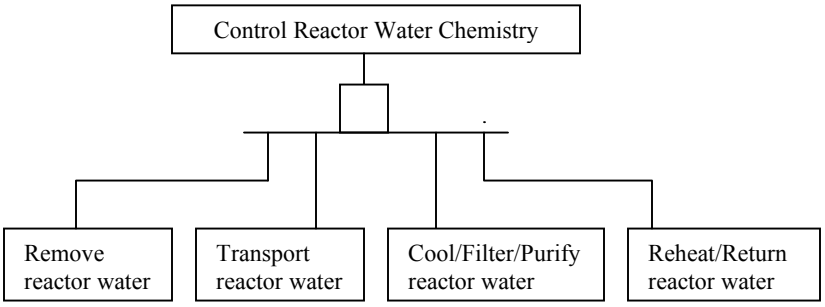
(6) Return water to the Reactor Vessel.

This may be demonstrated in the following logic diagram:



Now the processes are analyzed to verify that they are mutually independent. For our example, this analysis shows that the cooling process is required because of the physical characteristics of the deep bed demineralizer resins. These resins are not capable of withstanding temperatures in excess of 60°C. Therefore, the cooling process is included as part of the filter/purify process as a dependent process.

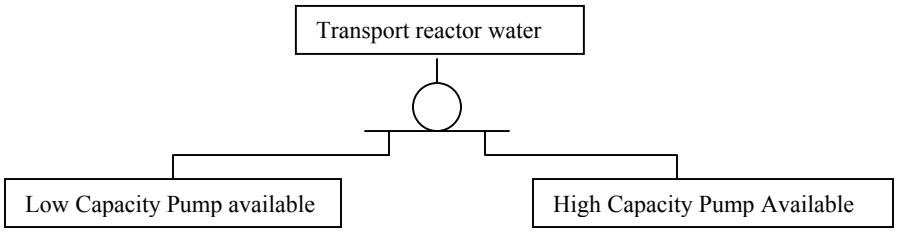
The reheating process is necessary to minimize thermal stresses in the RPV return lines. Therefore, it is included in the return reactor water process due to the same dependence reasoning stated above. The final result of this process is demonstrated in the following logic diagram:



Appendix C System Processing Elements Identification (SFL-4) Example

What physical support must be available to carry out this process?

In order to move the water through the system there must be a pump available that is capable of transporting the water. Since the RWCU system has a Low Capacity and a High Capacity pump, either one will transport water through the system. This is graphically displayed below using an OR logic gate.

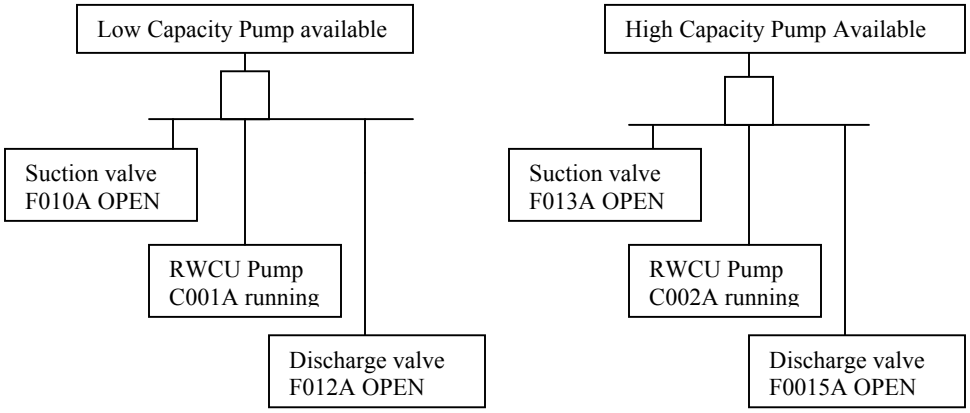


Appendix D System Component Requirements Identification (SFL-5) Example

Process Element– Low Capacity Pump OR High Capacity Pump available

The design of the system provides a low capacity and a high capacity pump. Either pump is capable of providing the transport capability requirements for the control of reactor water chemistry function. The following components are required to successfully complete the process element identified above:

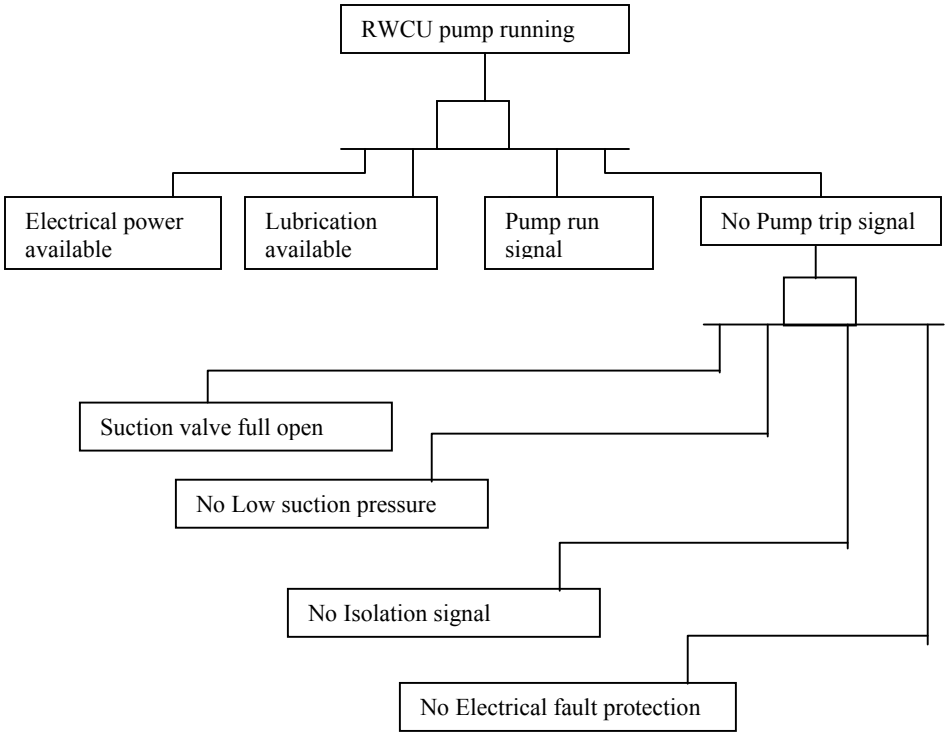
- Low Capacity Pump available with:
  - Suction valve F010A open
  - RWCU pump C001A running
  - Discharge valve F012A open
- High Capacity Pump available with:
  - Suction valve F013A open
  - RWCU pump C002A running
  - Discharge valve F015A open



Appendix E System Support Requirements Identification (SFL-6) Example

The following support requirements are necessary to maintain the RWCU pump availability status:

- Electrical power in service
- Motor and pump lubrication in service
- Pump run signal
- Suction valve full open
- No pump trip signal
- No low suction pressure
- No isolation signal
- No electrical fault protection actuated



Appendix F System Configurations and Configuration Change Identification Example (SFL-7 and SFL-8)

System Configuration A - RPV water purification - With respect to this system configuration, it is necessary to identify all the possible paths for function performance. In this way the operating configurations of each system function are obtained.

In accomplishing this division, the indications of the system designer and the technical characteristics of the equipment are taken into account. All of the operational configurations obtained will be listed.

For each system function defined in *System Function Identification (SFL-2)*, there is an associated system operating configuration (each possibly with different sub-configurations) meeting the corresponding requirements for performance. The System Operating configurations are not necessarily identified by the same name. Thus, for the functions defined for the RWCU system, we have the following system configurations:

System Configuration	Description
0	System out of service
A	RPV Water Purification
B	RPV Water Overboarding
C	RPV Cooldown
D	RPV Heatup

In this case, System Configuration 0 is defined as the out of service alignment. The relationship between system functions and operating configurations is not necessarily a one-to-one relationship. The status for all the components of the system for each configuration, in relation with the configuration zero, are addressed in a table like the following one:

Component	Description	System Configuration					
		0	A	B	C	D	E
Valve 001	Example Valve	Closed	Open	Throttled	Auto	Closed	---
Pump 001	Example Pump	Off	On	On	Standby	Off	---
Heat Exch 001	Example HX	OOS	In Service	In Service	Bypassed	OOS	---
Filter/Demin	Example Demin	OOS	In Service	In Service	Bypassed	OOS	---

Table 1, RWCU System configuration Example Table, is an example of this table completed for Train A of the RWCU system. All the components of the system are listed in the component column. The system configuration 0 ("zero") column reflects the status of the system

components for that configuration, and the rest of the columns show the differences between the respective configuration for that column and system configuration 0.

Once all the system operating configurations and sub-configurations have been identified, identification of the system configuration changes will begin. The system configuration change reflects those changes to component status, which must occur for system operation to switch from one system configuration or sub- configuration to another. System configuration changes are defined as shown in Table 2.

The following criteria are used to identify all the feasible system changes:

- All changes starting from or ending at system configuration 0 are considered system configuration changes because they are reflected in the configuration change table.
- If a system has two or more 100% independent trains, swapping trains in the same system configuration or sub-configuration is not considered a system configuration change.
- The configuration changes must be technically feasible and coherent with design basis and functions established by the designer. (See Table 2, ESBWR RWCU Configuration Change Table Example.)

In order to document alignment changes, a list will be drawn up showing the components which have to change and the status changes which must occur in order to reach the required final configuration, from an initial configuration. This will be accomplished by comparing the component lineups in the table listing the system configurations for the system configuration being changed from, to the system configuration being changed to. The components that change positions as a result of this comparison will populate this change list, which will be documented in a Table similar to Table 2, ESBWR RWCU Configuration Change Table Example.