

Enclosure 3

MFN 07-063

ESBWR Human Factors Engineering

Licensing Topical Report NEDO-33219

**ESBWR System Functional Requirements
Analysis Implementation Plan
Revision 1,**



**GE Energy
Nuclear**

3901 Castle Hayne Rd
Wilmington, NC 28401

NEDO-33219
Revision 1
Class I
DRF#0000-0050-0877
January 2007

LICENSING TOPICAL REPORT

**ESBWR FUNCTIONAL REQUIREMENTS ANALYSIS
IMPLEMENTATION PLAN**

Copyright 2007 General Electric Company

INFORMATION NOTICE

This document NEDO-33219 Revision 1, contains no proprietary information.

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT PLEASE READ CAREFULLY

The information contained in this document is furnished for the purpose of obtaining NRC approval of the ESBWR Certification and implementation. The only undertakings of General Electric Company with respect to information in this document are contained in contracts between General Electric Company and participating utilities, and nothing contained in this document are 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**, General Electric Company 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

1	OVERVIEW	1
1.1	Purpose.....	1
1.2	Scope.....	2
1.3	Definitions and Acronyms	3
1.3.1	Definitions.....	3
1.3.2	Acronyms.....	4
2	APPLICABLE DOCUMENTS	5
2.1	Supporting and Supplemental GE Documents	5
2.1.1	Supporting Documents.....	5
2.1.2	Supplemental Documents	5
2.2	Codes and Standards	6
2.3	Regulatory Guidelines	6
2.4	DOD and DOE Documents.....	6
2.5	Industry/other Documents.....	6
3	METHODS	7
3.1	Plant-Level Functional Requirements Analysis.....	7
3.1.1	Background.....	7
3.1.2	Goals	8
3.1.3	Bases and Requirements	8
3.1.4	General Approach	8
3.1.5	Application.....	8
3.2	System Functional Requirements Analysis Method	9
3.2.1	Background.....	9
3.2.2	Goals	9
3.2.3	Basis and Requirements.....	9
3.2.4	General Approach	9
3.2.5	Application.....	10
3.3	System Function Gap Analysis Method	10
3.3.1	Background.....	10
3.3.2	Goals	10
3.3.3	Basis and Requirements.....	11
3.3.4	General Approach	11
3.3.5	Application.....	11
4	IMPLEMENTATION	12
4.1	Plant-level Functional Requirements Analysis Implementation.....	12
4.1.1	Assumptions.....	12
4.1.2	Inputs.....	12
4.1.3	Process	12
4.1.4	Outputs.....	14
4.2	System Functional Requirements Analysis Implementation	14
4.2.1	Assumptions.....	14
4.2.2	Inputs.....	15
4.2.3	Process	15

4.2.4	Outputs.....	18
4.3	System Function Gap Analysis Implementation.....	18
4.3.1	Assumptions.....	18
4.3.2	Inputs.....	18
4.3.3	Process	19
4.3.4	Outputs.....	20
5	RESULTS	21
5.1	Results Summary Report	21
5.2	Periodic Reports.....	21
5.3	Technical Output Reports	21
	Figure 1. HFE Implementation Process.....	22
	Figure 2 Operational Analysis Iterations	23
	Figure 3 Functional Requirements Analyses.....	24
	Figure 4 Plant-level FRA Iterations	25
	Figure 5 System Functional Requirements Analyses	26
	Figure 6 Systems Gap Analyses	27
	Table 1 ESBWR RWCU System Configuration Table - Example.....	28
	Table 2 ESBWR RWCU Configuration Change Table Example	29
	Table 3 ESBWR RWCU Configuration Change Matrix Example	30
	Appendix A System Function Identification (SFL-2) Example.....	31
	Appendix B System Function Processes Identification Example (SFL-3).....	32
	Appendix C System Processing Elements Identification (SFL-4) Example	34
	Appendix D System Component Requirements Identification (SFL-5) Example	35
	Appendix E System Support Requirements Identification (SFL-6) Example	36

1 OVERVIEW

The ESBWR Man-Machine Interface System And Human Factors Engineering Implementation Plan (NEDO-33217), 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 operations 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 it's 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.

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 (NEDO-33217).

The FRA Plan establishes methods to:

- Conduct the FRA consistent with accepted 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
- Provide analysis method 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 systems HSI requirements,
- Critical safety functions resulting from PRA, HRA, and deterministic evaluations,
- Descriptions for each identified function, and
- 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 as a design input 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 the Probable Risk Assessment (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

Change Mode: An allowable realignment of system components from one mode 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).

Hierarchical goal structure: Relationship between a functional goal and sub-functional goal structured in hierarchical order.

Operations 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 Mode: 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:

AOF	Allocation of Function
AOP	Abnormal Operating Procedure
BRR	Baseline Review Record
EOP	Emergency Operating Procedures
FRA	Functional Requirement Analysis
HA	Human Actions
HFE	Human Factors Engineering
HFEITS	Human Factors Engineering Issues Tracking System
HRA	Human Reliability Analysis
HSI	Human System Interface
MPL	Master Parts List
OER	Operating Experience Review
OSHA	Occupational Safety & Health Administration
PFRA	Plant-level Functional Requirements Analysis
PRA	Probabilistic Risk Assessment
RSR	Results Summary Reports
RWCU	Reactor Water Cleanup
SDC	ShutDown Cooling
SDS	System Design Specifications
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 Design Control Document Chapter 18, Rev 2, (GE26A6642BX)
2. NEDO-33181, Rev 1, NP-2010 COL Demonstration Project Quality Assurance Plan
3. NEDO-33217, Rev 1, 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. EPI 20-15 , Rev 2, ESBWR Project Instruction, Engineering Change Control Process
2. ESBWR Design Specification, 26A6623 Rev. 0, ESBWR Plant Automation System
3. NEDO-33251, Rev 0, ESBWR Diversity and Defense in Depth Plan,
4. NEDO-33268, Rev 2, ESBWR Human-System Interface (HSI) Design Implementation Plan
5. NEDO-33274, Rev 1, ESBWR HFE Procedure Development Plan
6. NEDO-33275, Rev 1, ESBWR Training Program Development Plan,
7. NEDO-33276, Rev 1, ESBWR HFE Verification and Validation Plan

2.2 Codes and Standards

The following codes and standards are applicable to the HFE program to the extent specified herein. The applicable date/revision of the code or standard is specified in the Composite Specification [2.1.1.2].

1. IEEE-1023, Recommended practice for the application of human factors engineering to systems, equipment, and facilities of nuclear power generating stations and other nuclear facilities. New York: IEEE.

2.3 Regulatory Guidelines

1. NUREG-0700, Human System Interface Design Review Guidelines, 2002
2. NUREG-0711, Rev 2, Human factors engineering program review model, 2004a
3. NUREG-0800, Standard review plan, chapter 18 – human factors engineering, 2004

2.4 DOD and DOE Documents

N/A

2.5 Industry/other Documents

N/A

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 (applicant/holder) Owners’ Group (COLOG) and COL Applicants
6. Follows accepted human factors engineering 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 provides high-level Abnormal Operating Procedure (AOP) outlines. The Detailed PFRA, the third iteration of FRA, provides the basis for surveillance, operating, and maintenance procedures.

3.1.1 Background

The PFRA is the first step of the “top down” approaches to the HFE design illustrated in Figure 2, 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:

- Control release of radionuclides
- Economic operation
- Maintain economic operation
- Maintain emergency preparedness

3.1.2 Goals

The PFRA yields data structure that describes the plant function requirements. This data structure is rendered to provide inventories of required parameters, indications, controls, and outlines for EOPs and AOPs. These outputs are required as inputs to the AOF and TA.

3.1.3 Bases 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, function, 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 (see Figure 4, 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, and
- 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.

3.2.1 Background

The SFRA is the second step of the “top down” approaches 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 relationship among systems. The data structure provides system lineups, component manipulations, and process control requirements 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. Associated information and process control requirements are also identified.

The SFRA is performed concurrently with the PFRA. Systems (as a group of functions) are analyzed instead of 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 Plant Automation System (PAS), automatic control, or human action. Shared functions are also identified. 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 input (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 indication, controls, and 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” approaches to FRA. This is illustrated in Figure 4, System Function Gap Analyses. The process looks at each system 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 HFE and MMIS Implementation Plan (NEDO-33217) and shown in Figure 6.

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 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 PRA 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 requirements 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 input (Refer to Figure 6, System Requirements 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
- Minimized single failures leading to a plant scram, turbine trip, or unplanned power change
- 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 functions 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
- Protect economic operation

4.1.3.2 Plant state identification (PFL-2)

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

- Power operation
- Startup
- Shutdown
- Refueling

4.1.3.3 Plant function identification (PFL-3)

Identify the functions required to support the plant goals for each plant state. For example, the processes required for economic operation during power operation include:

- Release of energy
- Transfer of energy
- Conversion of energy
- Coordination and control of operation

4.1.3.4 Plant Redundancy Identification (PFL-4)

Identify trains, channels, and divisions required to support plant functions. The bases for redundancy include:

- General Design Criteria
- Diversity and defense in depth
- Desired reliability
- Redundancy for maintenance of subsystems and components

4.1.3.5 Critical Safety Function Identification (PFL-5)

Identify those functions that are required to limit radionuclide release within 10CFR-100 limits by identifying the functions that protect the fission product barriers. For example, these functions include:

- Protect reactor
- Maintain primary containment
- Maintain Reactor Building Integrity

List the critical safety sub-functions required to support the Critical Safety Functions. For example, the sub-functions of “protect reactor” include:

- Maintain fuel integrity and
- Maintain reactor coolant boundary.

Determine sub-functions; for example, the sub-functions of “maintain fuel integrity” include:

- Control fuel within power limits
- Control RPV water level
- Control heat removal

4.1.3.6 Plant Process Function Identification (PFL-6)

Identify those functions that are required to support plant processes (similar to the method used to identify the sub-functions that support critical safety 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 (EPG, IOP, and EAL) outlines
- Plant process and function redundancies
- Critical safety functions
- Plant functions and sub-functions
- Inventory of critical safety parameters
- Requirement for HIS design
- Outlines for simulator scenarios

4.2 System Functional Requirements Analysis Implementation

The SFRA is performed by the responsible system engineer and is facilitated by the HFE team. The system engineers ensure that the SFRA 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 SFRA

4.2.1 Assumptions

This analysis assumes:

- System design satisfies the plant performance requirements

- 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

4.2.2 *Inputs*

SFRA inputs include:

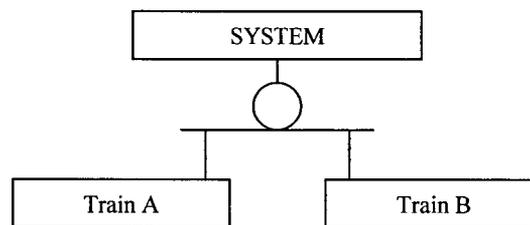
- OER and BRR
- PRA and HRA
- FRA, AOF and TA data structures from previous iterations
- ESBWR System Design Specification (SDS)
- Design changes

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 and 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.

Use 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 (FEG).

- 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 design 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 design 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.

This level matches with the low-level logic diagrams for components. In order to fill this level these logic diagrams are referenced (with code and page) in the SUPPORT REQUIREMENTS field and only the signals related with the component are listed in that field.

An example of support requirements are necessary to maintain the RWCU pump in an operability 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 letter, which in some cases is followed by a number. 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 Modes
- System Change Modes
- Component Lineups
- Component Operational Requirements (i.e. components required to be remotely operated)
- Component control requirements (i.e. automatic, manual, etc.)
- Component manipulations required to change modes (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 PFGA and employs a data structure to record and render the plant 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 step “System Function Identification.”

4.3.3 Process

4.3.3.1 System Function Comparison

Compare and match plant functions and system functions.

4.3.3.2 Link PFRA to SFRA

Tie the PFRA data structure to the SFRA data structure where system functions match one another.

4.3.3.3 Determine Differences

Identify plant 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 root of the 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 HFE and MMIS Implementation Plan
- Provide the Responsible System engineer with design inputs
- Re-perform the applicable portion of the FRA to confirm resolution
- Document out of process issues in HFEITS

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
- Requirements for HSI design

5 RESULTS

5.1 Results Summary Report

Following each iteration, FRA results are recorded in a data structure and rendered in a form that accommodates validation and verification. Once rendered and verified, results are attached to the SDS as Appendices. FRA Results Summary Reports (RSR) may be combined with the AOF and/or TA RSRs.

Results Summary Reports contain:

- Roster of team members and their roles in performing the FRA.
- Inputs and Outputs, and
- Issues carried forward in HFEITS.

5.2 Periodic Reports

FRA analysis produces a report following Operational Analysis iterations. The FRA does not produce periodic reports.

5.3 Technical Output Reports

The FRA produces technical reports include:

- High-level PFRA
- Inventory of critical safety parameters
- Design Input Reports (HFEITS)
- SDS Appendix updates:
- Critical safety functions
 - Plant functions and sub-functions
- Design input reports
- Process requirements
- I&C requirements
- Software requirements

Figure 1. HFE Implementation Process

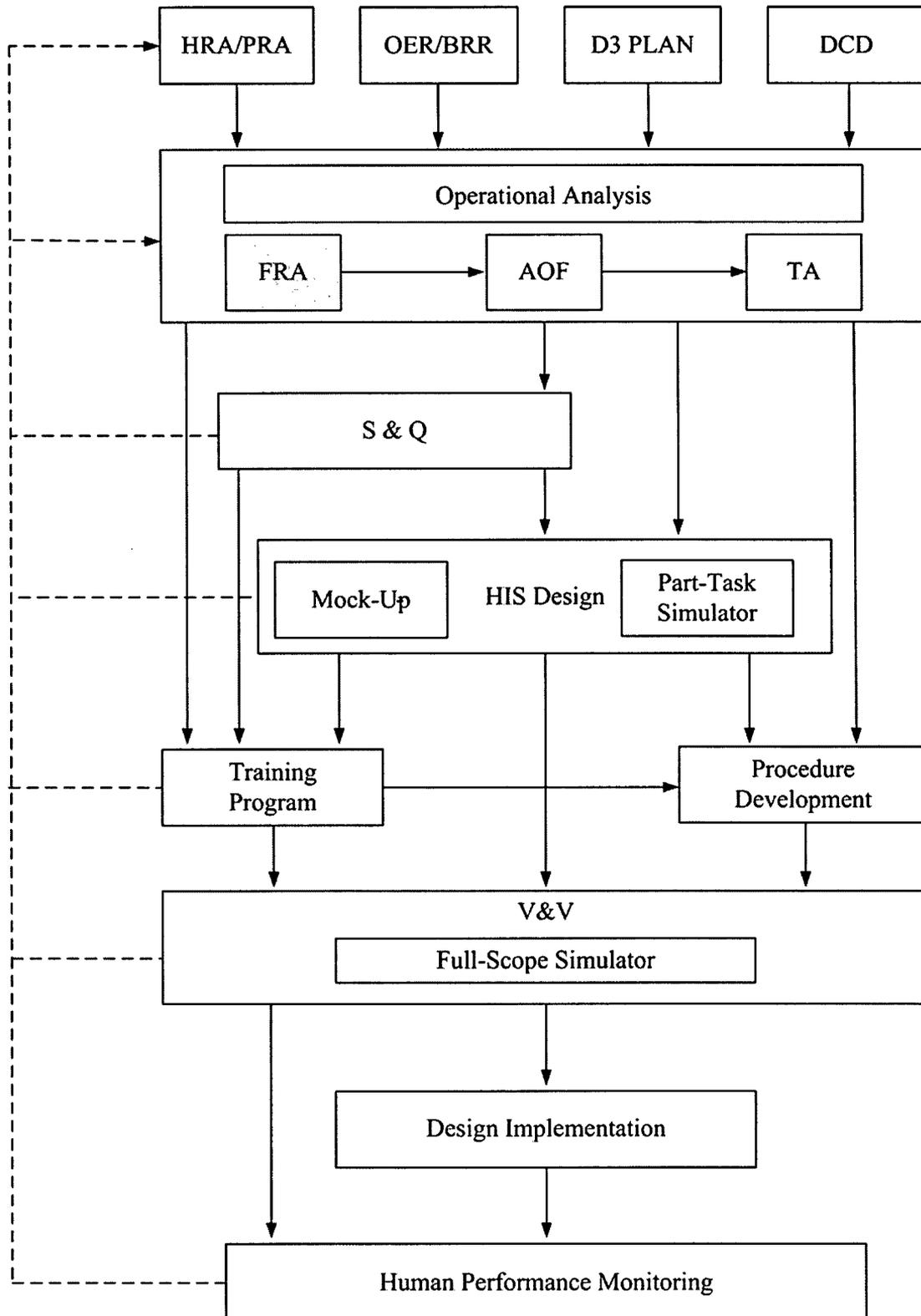


Figure 2 Operational Analysis Iterations

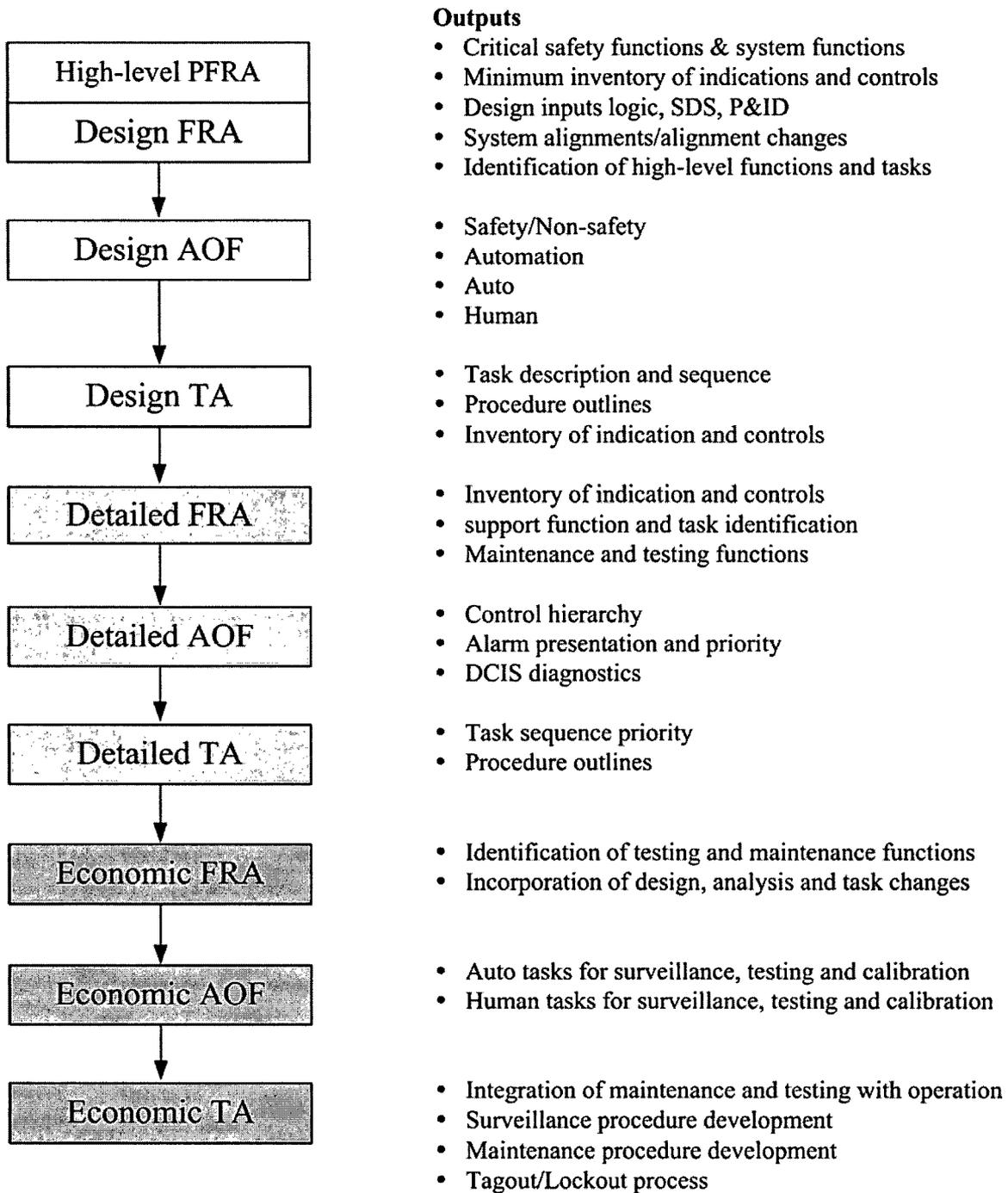


Figure 3 Functional Requirements Analyses

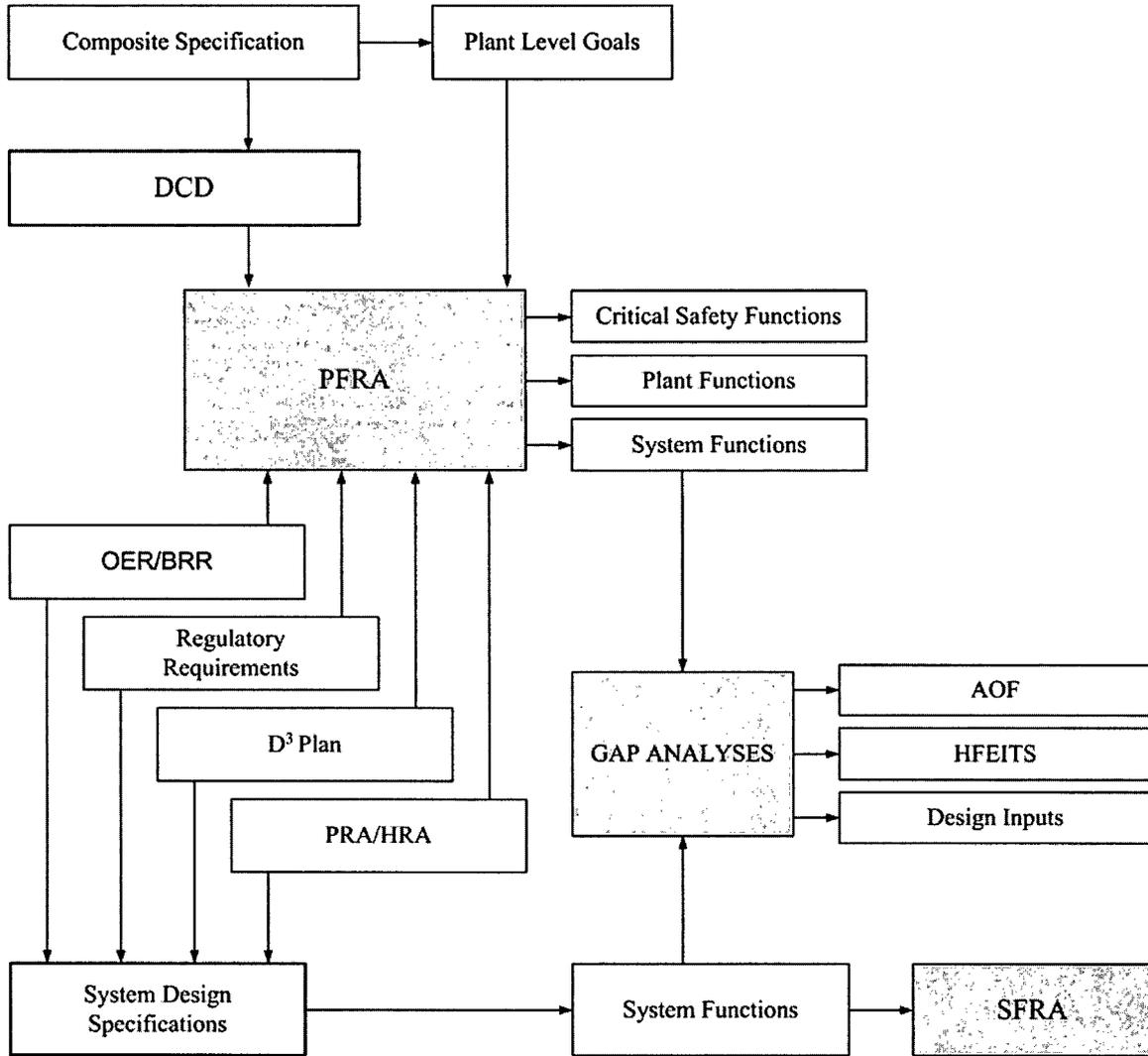


Figure 4 Plant-level FRA Iterations

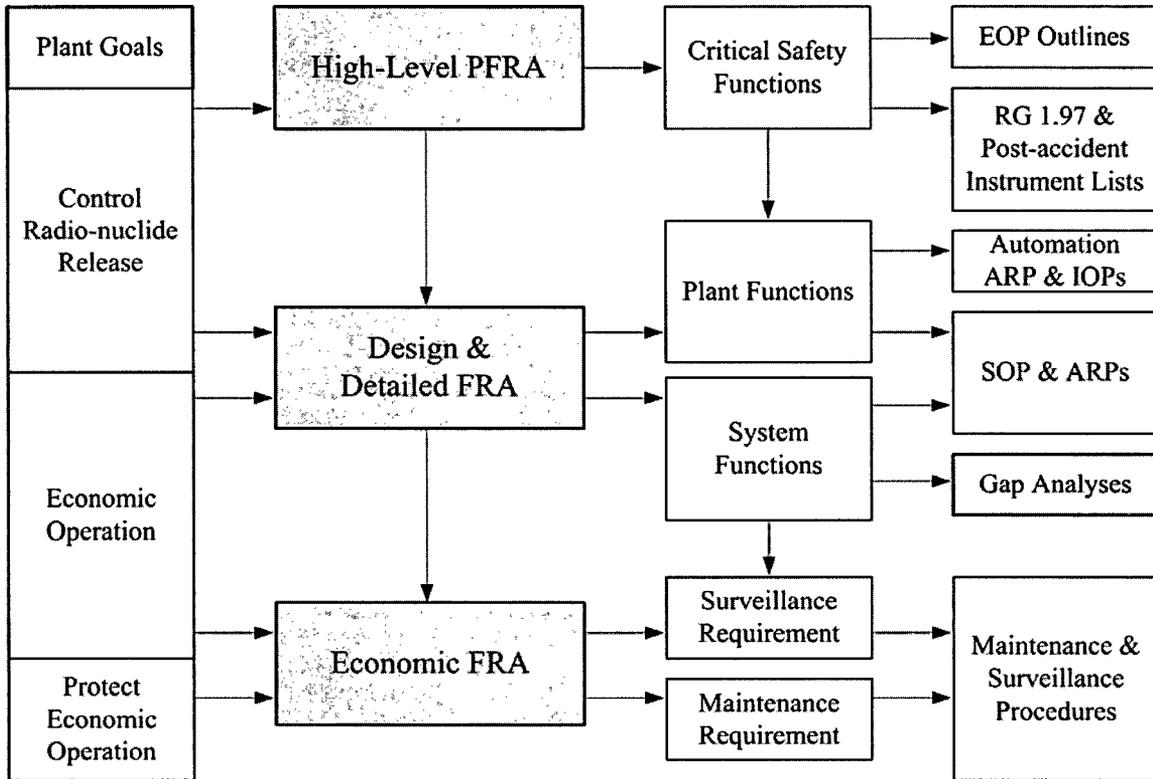


Figure 5 System Functional Requirements Analyses

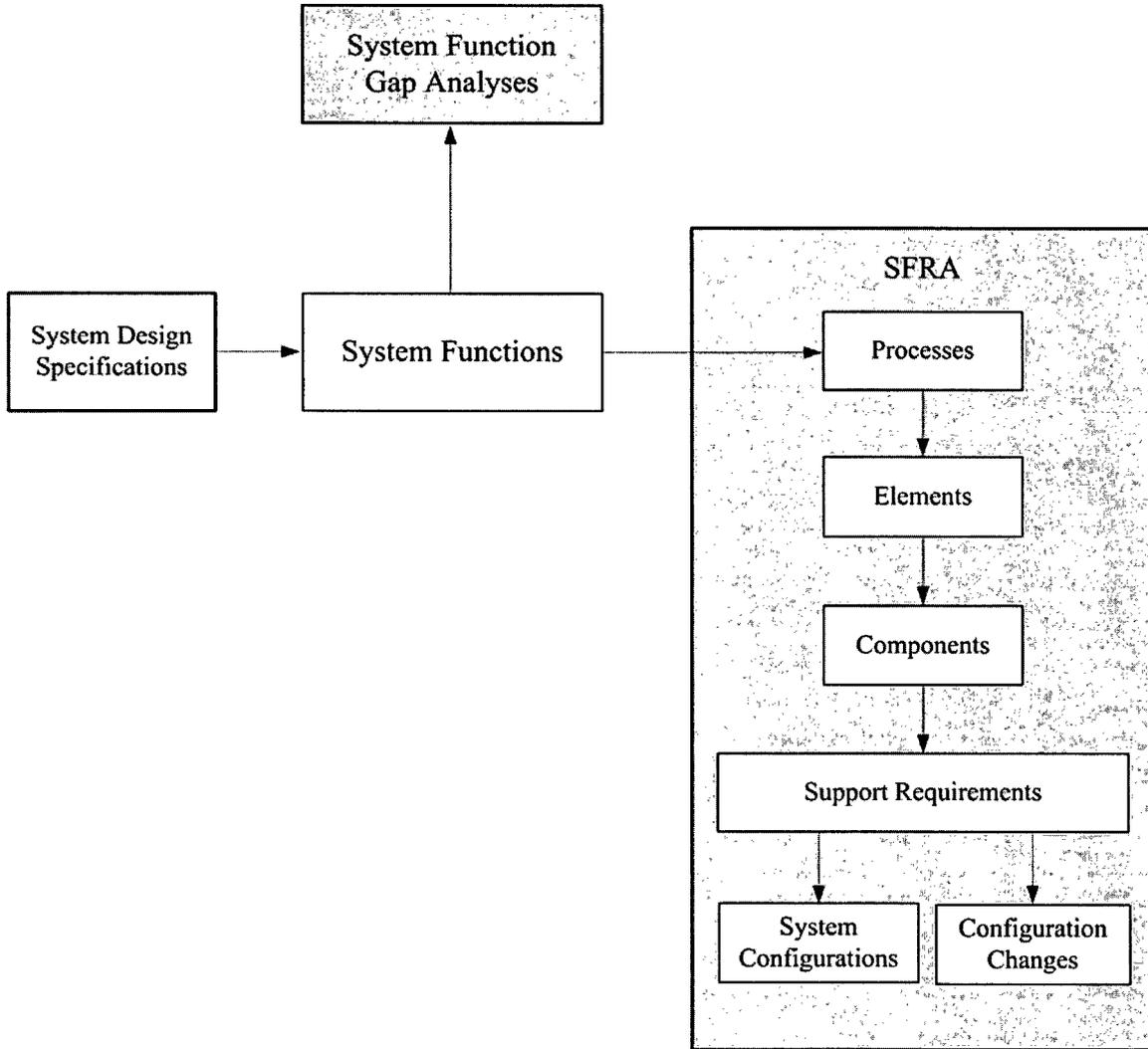


Figure 6 Systems Gap Analyses

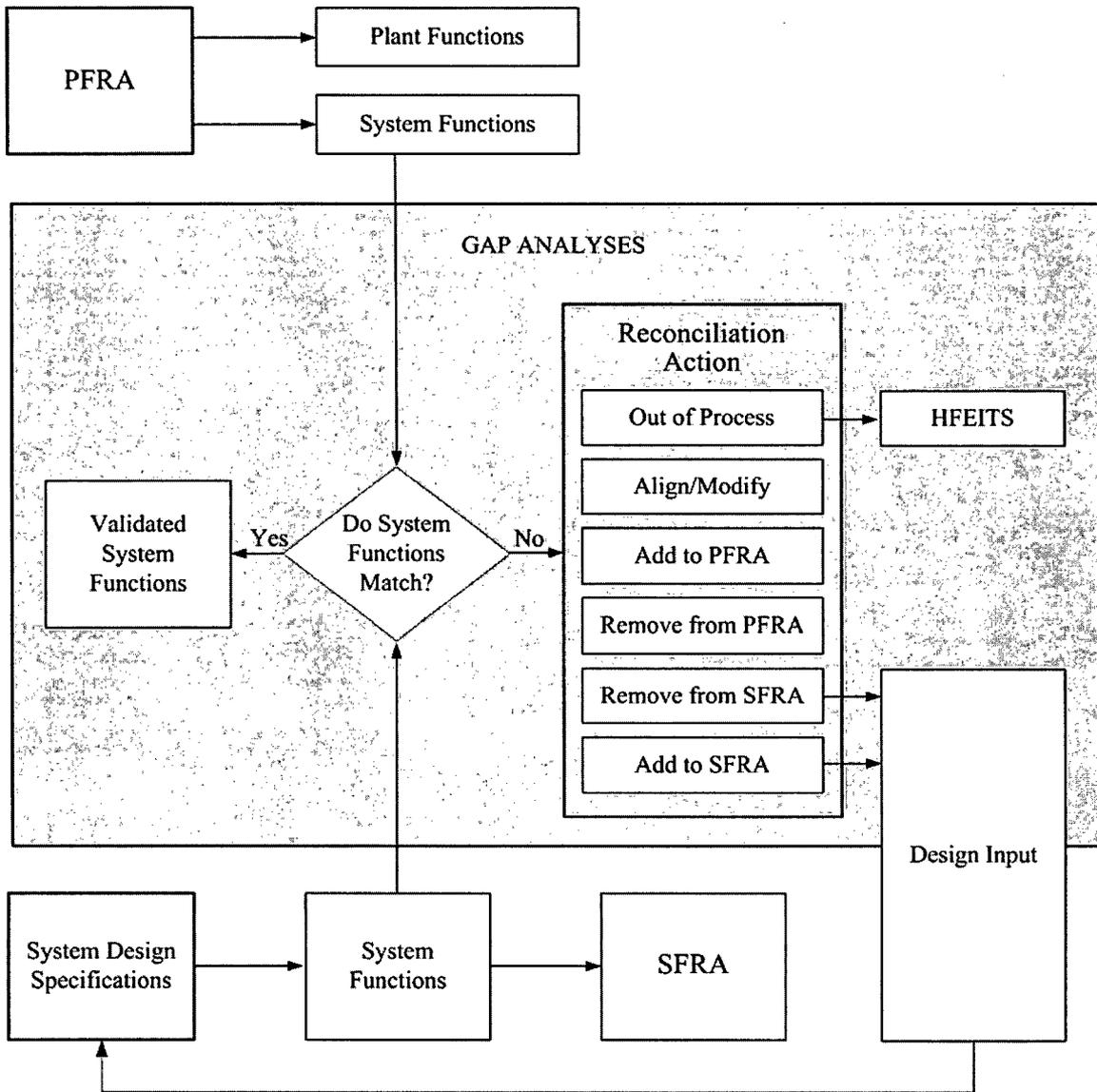


Table 1 ESBWR RWCU System Configuration Table - Example

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

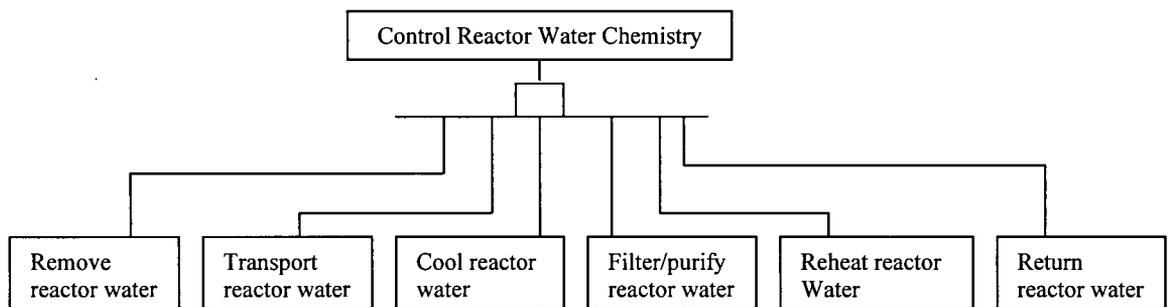
Function Processes Identification

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:

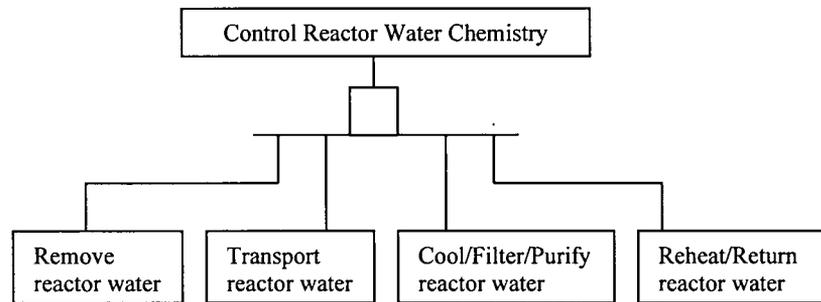
1. Remove the water from the Reactor Vessel.
2. Move the water through the system.
3. Cool the reactor water.
4. Filter/purify the reactor water.
5. Reheat the reactor water.
6. Return water to the Reactor Vessel.

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.

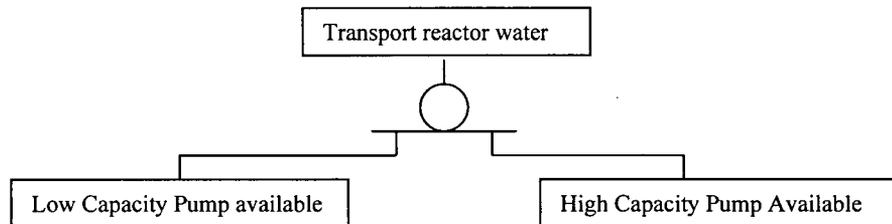
The reheating process is necessary to minimize thermal stresses in the RPV return lines. Therefore, it is included in the return reactor water process due to the same dependence reasoning stated above. The final result of this process is demonstrated in the following logic diagram:



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.



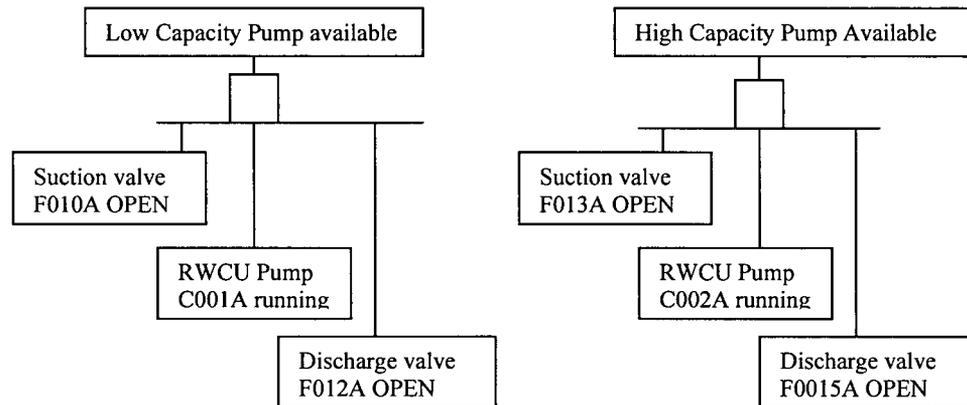
Appendix D System Component Requirements Identification (SFL-5) Example

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

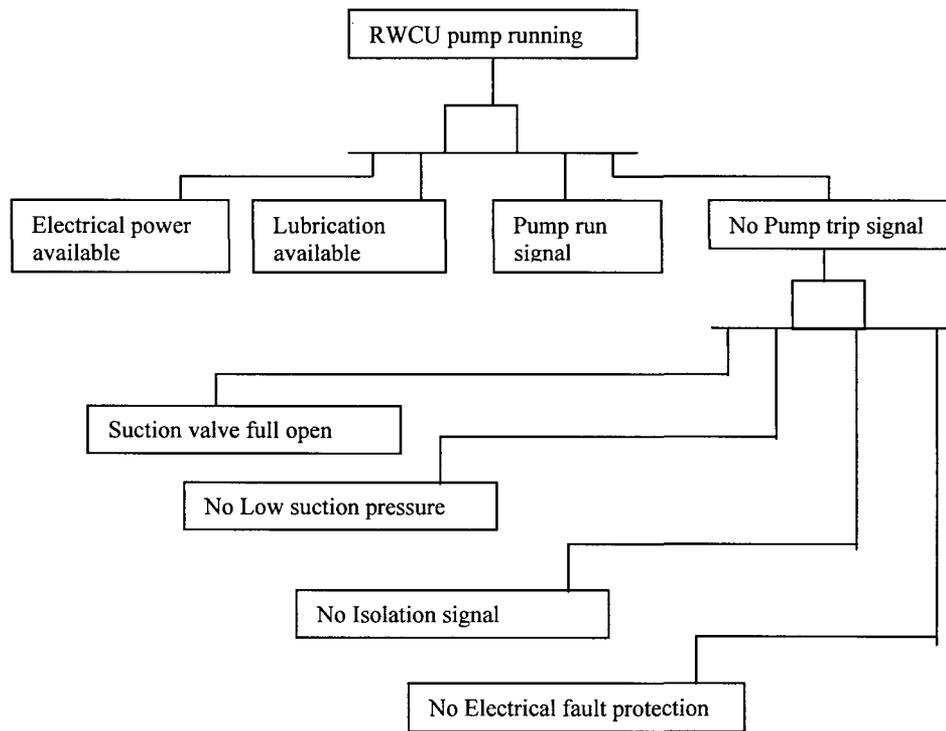
- High Capacity Pump available with:
 - Suction valve F013A open
 - RWCU pump C002A running
 - Discharge valve F015A open



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

As reference, a standard system configuration of operation (called system configuration zero) is defined. This system configuration zero is used as the initial configuration of operation, and all the rest of the configuration and sub-configurations will be referenced as changes over it. The analyst is free to define this configuration, but the following configurations can be used:

- The “ready to start” alignment
- The alignment shown at the P&ID (usually the system status during plant normal operation)
- The alignment defined by the failure mode of the system components
- The “out of service” alignment (all the components closed and/or off)

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 mode (each possibly with different sub-modes) 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 modes 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 reflect 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 change modes will begins. 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 Figure 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 mode of operation table.
- If a system has two or more 100% independent trains, swapping trains in the same system mode or sub-configuration are not considered as system configuration changes.
- The configuration changes must be technically feasible and coherent with design basis and functions established by the designer. (See Table 2, RWCU Configuration Change Matrix 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, RWCU Configuration Change Example.