GE Energy
Nuclear

3901
Castle Hayne Rd
Wilmington, NC 28401

NEDO-33219
Class I
DRF#0000-0050-2837

January 2006

LICENSING TOPICAL REPORT

ESBWR SYSTEM FUNCTIONAL REQUIREMENTS ANALYSIS IMPLEMENTATION PLAN

INFORMATION NOTICE

This document NEDO-33219, Revision 0, 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 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**, 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

Appendices

List of Tables

List of Figures

1 Introduction

The ESBWR Man-Machine Interface System And Human Factors Engineering Implementation Plan [2.1(2)] establishes three specific steps that support an overall system/operations analysis:

- System functional requirements analysis (section 4.3 ref. 2)
- Allocation of functions (section 4.4 ref. 2)
- Task analysis (section 4.5 ref. 2)

These steps support the design decisions to use manual, automatic or shared control in the design. Using the allocation as a basis the design is developed and modified. A functional verification is applied with feedback to address changes in the design and the impact on the functional requirements and allocation.

This Plan focuses on the first of these steps, system functional requirements analysis.

1.1 Background

The overall System/operations analysis integrates the three elements of functional requirements, function allocation, and task analysis to establish design requirements in a Human System Interface (HSI) design. The system/operations analysis addresses operational aspects of the plant by systematically defining equipment, software, personnel and procedural data requirements that meet all functional objectives of the operation centers such as the control room and its operating crew, including safe operation of the plant. It assists in determining the design of the plant and the design of the plant HSIs, particularly the control room HSI and the HSI for safe plant shutdown outside the control room. The analysis collects parameters concerning the plant (and its various systems) and identifies those required for the operating crew monitoring, cues for action, and feedback on actions taken. The analysis identifies the main control and operating options available to operators for safe and economic plant operation. The plant processes which should be placed under operator control, and their relationship to each other, are also revealed.

Some benefits resulting from the integrated system/operations analysis are:

- Systematic bases for determining the HSI design requirements.
- A control room design based on functions instead of physical systems. The compartmentalization of the instrumentation and control design to match the boundaries of individual physical system tends to ignore the natural and essential sharing of functions between systems. Ignoring these interrelations distorts the design toward detail tasks and ignores the overall functions which need to be accomplished.

- A sound basis from which future modifications to the HSI may be assessed.

Several terms are defined below to provide a common basis for subsequent paragraphs. The prefix "sub", as in sub function, subsystem, etc., refers only to a lower level category of the non-prefixed term and the definition remains essentially applicable.

System/operations 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.

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).

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

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

1.2 Purpose

The purpose of the functional requirements analysis is to:

(1) determine the objectives, performance requirements, and constraints of the design,

(2) define the high-level functions that have to be accomplished to meet the objectives and desired performance including safety functions,

(3) define the relationships between high-level functions and plant systems (e.g., plant configurations or success paths) responsible for performing the function including any functional interrelationship that safety functions may have with non-safety systems,

(4) identify critical safety functions defined as those functions required to achieve major system performance requirements or functions which, if failed, could

degrade system performance or pose a safety hazard to plant personnel or the general public, and

(5) provide a framework for understanding and assigning the role of controllers (whether personnel or system) for controlling the plant.

The purpose of this implementation plan is to prescribe and guide the conduct of functional requirements analysis for the ESBWR plant design.

This Plan meets the requirements of the ESBWR M-MIS Design Implementation Plan [2.1(2)].

1.3 Scope

The general approach to the implementation of the ESBWR MMIS for the System Functional Requirements Analysis (SFRA) will be to, (a) create plans in accordance with NRC guidelines, (b) establish baseline design inputs from previous ABWR system control room designs, (c) prepare ESBWR specific gap analysis to ABWRs, including an Operating Experience Review, (d) execute the HFE plans through to turnover to the COL Applicant, (e) follow standard human factors engineering and I&C practices and processes, (f) follow the activities for HSI design and system hardware/software design, and (g) meet the commitments of ESBWR DCD Chapter 18.

The inputs to System Functional Requirements Analysis are the M-MIS functions for the ESBWR as defined in DCD and ABWR reference summary reports and supporting documentation. The functional requirements analysis will use ABWR reference design documentation as the technical basis for identifying changed functions in the ESBWR design. From the Baseline Review Record and Gap Analysis as established during the ESBWR design process Summary descriptions of plant processes and detailed narrative descriptions of changed functions will form the detailed scope of SFRA and subsequent HFE activities.

This System Functional Requirements Analysis Implementation Plan establishes the following scope elements for the gap analysis:

1. Methods and criteria for conducting the System Functional Requirements Analysis in accordance with accepted human factors principles and practices;

2. System requirements that define the system functions and those system functions that provide the basis for determining the associated HSI performance requirements;

3. Functions critical to safety that are identified using both PRA/HRA techniques and deterministic evaluations; and

4. Descriptions developed for each of the identified functions and for overall system configuration design.

To accomplish these objectives, plant-level and system-level goals and functions are systematically analyzed according to a nine level hierarchical structure to obtain component level performance requirements. During this process, control and instrumentation requirements are identified and the functional relationships between plant functions and system functions are defined. Key steps of the analysis process, and their order of presentation in this plan document, are as follows:

Section 3: Methods and criteria for identification of Plant Performance Requirements

Section 4: Methods and criteria to perform system level functional analysis based on Plant Performance Requirements

Section 5: Identification of functions critical to safety

Section 6: Method for developing graphic functions descriptions

Section 7: Method for developing detailed functions narrative descriptions

Section 8: Analysis methods, which define the integration of closely, related sub-functions or the division of identified sub-functions

2 Reference Documents

2.1 Supporting Documents

1. ESBWR Design Control Document Tier 2 Chapter 18 Human Factors Engineering

2. ESBWR Man-Machine Interface System And Human Factors Engineering Implementation Plan, NEDO-33217

3. ESBWR System Design Specifications (SDSs), (design description documents)

4. GE Advanced Boiling Water Reactor Standard Safety Analysis Report (SSAR),

5. Task Analysis Implementation Plan,

6. Human Factors Verification and Validation Implementation Plan,

2.2 Codes and Standards

1. IEEE-1023, IEEE Guide to the Application of Human Factors Engineering to Systems, Equipments and Facilities of Nuclear Power Generating Stations, 1988, (IEEE)

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

2.3 Regulatory Requirements and Guidelines

1. NUREG-0700, Human-System Interface Design Review Guideline, 1986, (U.S. Nuclear Regulatory Commission)

2. NUREG/CR-3331, A Methodology For Allocating Nuclear Power Plant Control Functions to Human and Automated Control, 1983, (U.S. Nuclear Regulatory Commission)

3. Regulatory Guide 1.70, Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants, Rev. 3, November 1978, (U.S. Nuclear Regulatory Commission)

4. NUREG-0711r2, Human Factors Engineering Program Review Model, 2004, (U.S. Nuclear Regulatory Commission)

2.4 Electric Power Research Institute (EPRI)

1. EPRI NP-3659, Human Factors Guide for Nuclear Power Plant Control Room Development, 1984

2. Advanced Light Water Reactor Utility Requirements Document, Volume II ALWR Evolutionary Plant, Chapter 10 Man-Machine Interface Systems

3. EPRI TR-101814 Human Factors Guidelines for Fossil Power Plant Control Rooms and Remote-Control Stations

2.5 Department of Defense and Energy

1. AD/A233 168, System Engineering Management Guide, (Dept. of Defense, Defense System Management College, Kockler, F., et al)

2. AR602-1, Human Factors Engineering Program, (Dept. of Defense)

3. MIL-H-46855B, Human Engineering Requirements for Military Systems, Equipment and Facilities, (Dept. of Defense)

4. DOD-HDBK-763, Human Engineering Procedures Guide, Chapters 5-7 and Appendix A and B

2.6 Industry and Other Documents

1. IEC 964, Design for Control Rooms of Nuclear Power Plants, 1989, (Bureau Central de la Commission Electrotechnique Internacionale)

2. Handbook of Human Factors, edited by Gavriel Salvendy, John Wiley and Sons, 1987.

3 Methods and Criteria for Identification of Plant Performance Requirements

The objectives of functional analysis are to (a) determine performance requirements and constraints of the design, (b) define functions that must be accomplished to meet the requirements, (c) define relationships between functions and plant processes, and (d) provide a framework for understanding and assigning the role of humans and machines for controlling plant processes.

The functional analysis starts with the development of a hierarchical structure which shows all the relationships between the plant functions. The hierarchical structure has nine levels as listed in Table 3. These nine levels are divided into two groups. The first group called "Plant Level" covers the first four levels (PFL-1 through PFL-4) and the second group called "System Level" covers the remaining five levels (SFL-1 through SFL-5). The Plant Level Functional Analysis studies the plant as a whole while the System Level Functional Analysis is focused on the functions assigned to the physical systems in the plant.

The complete functional analysis (nine levels) should be performed for new designs of plants. The ABWR is not a new design, but an evolutionary design, based on BWR operating and design experience. Because of this, the ESBWR functional analysis begins at the System Level. The system functions are defined in each system design description (SDD). The bases for the design of each system is identified in the system specific SDD. An operational experience review (OER) has been performed and is documented by the system engineer. A methodology for this System Level Functional Analysis is provided in Section 4.2.

This section presents a methodology for conducting the Plant Level Functional Analysis. The Plant Level Functional Analysis methodology is included herein to provide guidelines for performing Functional Analysis. The top level hierarchical structure created in this section is only an example. The top-level structure is included implicitly in the design basis of the ESBWR plant systems.

The starting point in the development of the plant-level portion of the hierarchical structure is to define the plant primary goals. Since the ultimate purposes of the plant are controlled generation of electricity (availability goal) and prevention of radioactive release to the environment (safety goal), these are the goals to be placed at the top of the hierarchy [see Reference document 2.6(1), pages 21 and 71].

These goals should be developed further as plant primary subgoals and used in the design process. The second step should be the identification of all plant Critical Functions which are essential for the performance of each subgoal identified. The

third step is the identification of sub-functions of these functions needed to accomplish each one of them. The process will culminate in a collection of sub-functions that constitute the HSI performance requirements.

NUREG-0711 [2.3(4)] allows the System Functional Requirements Analysis (SFRA) and Allocation of Functions (AOF) to focus on those functions that have been allocated differently than their predecessor designs. However, for ESBWR, the SFRA and AOF is also being performed through screening for unchanged allocated functions to verify that the documentation for the Task Analysis is consistent in format and to verify that allocated functions of predecessor designs are consistent with the requirements of the ESBWR Project. The Operating Experience Review (OER) data collected during the design of the U.S. ABWR will be reviewed during the performance of the functional requirements analysis and allocation of functions activities for both modified and unmodified systems. The OER issues will be reviewed for their affect on the system functions and the assigned control function allocation for each system.

The steps to create the top level functional structure starting from the primary goals are:

1. Plant Primary Subgoals identification (PFL-2)
2. Plant Critical Functions identification (PFL-3)
3. Plant Performance Requirements identification (PFL-4)

These steps are explained in greater detail in Sections 3.1 to 3.3.

3.1 Method for Plant Primary Subgoals Identification (PFL-2)

This is the second level in the hierarchical structure. It is a "plant-status level" where the "defense-in-depth" concept and electricity production process optimization should be addressed. Subgoals are divided into two groups per the two top level (primary) goals dealing with generating electricity (the Availability Goal or A.G.) and preventing releases (the Safety Goal or S.G.). The two groups are:

1. Safety related subgoals
2. Availability-related subgoals

For the ESBWR Project, safety related and non-safety related system functions and design information are defined in the ESBWR System Design Description (SDD). The SDDs are the initial source of input for the SFRA work. In addition to system functions, the SDD defines mandatory allocations of functions prescribed by regulatory requirements or design goals. Using SDDs as input for the SFRA is consistent with guidelines for conducting HFE analyses [e.g., Reference 2.3(4)].

3.1.1 Safety Related Subgoals Identification [S.G. at PFL-2]

The following inputs are required for the analysis of specific safety related subgoals:

- Definition of ABWR barriers against radioactive release
- ABWR Emergency Procedure Guidelines (EPGs)

In an ABWR plant there are generally four physical barriers implemented to prevent activity release. Barriers in the context of Functional Analysis apply to the assignment of systems to plant Safety Goal requirements and they are:

- Fuel clad
- Boundary of reactor coolant system
- Primary containment
- Secondary containment

These physical barriers are the key to defining the second level of safety goals (PFL-2).

The EPGs provide a functional structure focused to avoid any damage to plant areas and to prevent the activity release to the environment for any postulated accident. This functional structure could be used to generate the second level of goals because the ultimate purpose is the same.

To accomplish these objectives, the EPGs are intended to maintain the integrity of the barriers against fission products release. Top level objectives of EPGs will constitute the PFL-2 safety subgoals for the functional structure.

These subgoals are:

- Reactor Protection (fuel, coolant boundary, etc.)
- Primary Containment Integrity
- Secondary Containment Integrity
- Activity Release Control

Figure 1 shows second level functional structure for the safety goal. The AND gate means that it is necessary to accomplish all the subgoals to get the fulfillment of the primary goal. Accomplishing all these subgoals assures the fulfillment of the safety goal.

3.1.2 Availability Subgoals Identification [A.G. at PFL-2]

The following inputs are required for the analysis of specific availability subgoals:

- Definition of ABWR normal operations
- Analysis of energetic transformations that happen in a BWR Nuclear Power Plant (NPP)

Normal operations in the cycle of production can be divided into planned operations, considered as a chronological sequence as follows:

The points or limits at which some of the planned operations end and others begin cannot be precisely determined. As an example, for BWR plants these limits are defined in Table 1. As noted in Table 1, planned operations 1 and 2 (Achieving Criticality and Heatup) are characterized by "Startup" operational mode. Planned operation 3 (Power Operation) is characterized by "Power Operation" operational mode. Planned operation 4 (Achieving Shutdown) is characterized by "Hot Shutdown" operational mode. Planned operation 5 (Cooldown) is characterized by "Cold Shutdown" operational mode. Planned operation 6 (Refueling outage) is characterized by "Refuel" operational mode. Additional modes 7A, 7B and 8 are provided to address specific train configurations when not at full power as shown in Table 2.

The key to defining the second level of availability goals (subgoals) is the transformations of mass and/or energy that happens in a BWR NPP. These transformations are shown in Table 4, BWR NPP Energetic Transformations.

These transformations are associated with:

- Physical plant systems where the transformation takes place
- Normal operation into NPP cycle of production

Physical systems associated with each transformation are:

- T1: Nuclear fuel and moderator
- T2: Reactor
- T3: Turbine set
- T4: Electrical generator

From this analysis four availability subgoals (PFL-2) will be defined:

- Bring the Plant to Operational State of Power

This subgoal covers Startup Mode 2, the energetic transformation T1, and planned operations 1 and 2.

- Control Nuclear Steam Supply (NSS)

  This subgoal covers Power Operation Mode 1, the energetic transformation T2, and planned operation 3.

- Electrical Conversion with the Highest Efficiency

  This subgoal covers Power Operation Mode 1, the energetic transformation T3 and T4, and planned operation 3.

- Shutdown and Refueling

  This subgoal covers Refuel Mode 5. There is no energetic transformation covered by this subgoal, but refueling could be considered as a mass transformation.

Planned Operation 4 (Achieving Shutdown) and Planned Operation 5 (Cooldown) are not availability-related because the PFL-2 availability subgoals are focused on maximizing the plant capacity factor to assure a satisfactory return on the financial investment. The availability-related subgoals shall not violate the safety subgoals.

Figure 2 shows the second level functional structure for the availability goal. As in Figure 1, the AND gate means that it is necessary to accomplish all the subgoals to fulfill the primary goal.

Table 1 identifies the operational plant modes of a typical BWR which will be used in the examples. The specific modes of the ESBWR NPP are defined in the ESBWR DCD. Figure 12 defines the change Mode Block Diagrams that are used for each system SFRA to define its specific system modes.

3.2 Method for Critical Functions Identification (PFL-3)

The identification of Critical Functions for each subgoal defined above is the third level in the hierarchical structure. A Critical Function is defined as an activity or role performed by human, structure or automated system essential to fulfilling its associated subgoal(s). As for subgoals, Critical Functions are divided into two groups: safety related Critical Functions and availability-related Critical Functions.

There are three parts to the definition of a Critical Function:

- **Boundary**: a conceptual surface which contains the physical systems of the plant where the function applies.

- **Parameter**: a physical measure which characterizes the function. This parameter doesn't need to be a directly "measurable" parameter of the plant.
- **Action**: the operation (or operations) which is (are) necessary to perform with the parameter in order to fulfill part of the associated subgoal(s) or the complete subgoal if there is only one dependence relation.

Making a mathematical identification:

If $G(x_1,\ldots,x_p)$ is the subgoal and $x_1,\ldots,x_p$ are the physical parameters upon which the subgoal depends, and f_i (i=1,...,n) are the Critical Functions for the subgoal. The relationship among them could be expressed by:

$$G\left(x_1,\ldots,x_p\right)=\sum_{1}^{n}\alpha_i f_i\left(x_1,\ldots,x_p\right) \tag{1}$$

With the constraint:

$$\sum_{1}^{n}\alpha_i f_i=0\Leftrightarrow\alpha_i=0;(\forall i) \tag{2}$$

which is the well known relationship of linear independence.

These relationships require that, for each subgoal, it is necessary to find a set of Critical Functions for which:

The set is big enough to cover the whole subgoal.

Functions included in the set must be independent from the other functions within the set. A Critical Function should not be accomplished by other Critical Functions.

In order to explain this proposed method, some Critical Functions associated with safety related and availability-related subgoals for a BWR-6 with Mark-III containment are identified in the following examples.

Example 1. Subgoal S.G.-2 (Primary Containment Integrity)

The first step in the definition process is to define all the boundaries associated with the subgoal. This is a process for matching the processes of the function with the subgoal associated with the function. The question will be:

Which boundaries are necessary to meet the subgoal?

For this safety subgoal, the barrier to protect is primary containment, which includes the drywell and the suppression pool, so the boundaries are:

- Drywell
- Suppression pool
- Primary containment envelope

The second step is to ask about the parameters related to these boundaries. The question will be:

What are the necessary parameters to be controlled in order to meet the subgoal, taking into account the boundaries?

All the parameters related to primary containment integrity must be considered. In this example, temperature, level and pressure are direct candidates because they are parameters addressed in the EPGs. Another parameter to analyze is hydrogen concentration because it constitutes a threat to containment integrity by hydrogen combustion.

The third step consists in identifying all the processes related to these parameters in order to fulfill the subgoal. The question will be:

Which actions are necessary to perform with these parameters in order to meet the subgoal?

The answer to this question will be written by the designer in Table 6 using action verbs such as "to maintain", "to control", etc., or state verbs such as "to have capability", "to be available", etc. In this example, a safety related subgoal is being analyzed, so the required actions should be focused on avoiding the defined parameters which exceed safety limits (systems design parameters). The appropriate action to perform is to control the parameter.

With these data compiled, the Critical Functions can be obtained for the subgoal S.G.-2. Each Critical Function is generated through the construction of Table 6. The candidate functions should be the drywell, suppression pool and primary containment temperature, pressure level and hydrogen concentration control because these are possible combinations. The question, however, is: Do these functions constitute a minimal set?

While the ESBWR design will be used in the HFE program, the examples of how we treat the information for SFRA is a BWR Mark-III containment design, where some

parameters are dependent among the functions. As an example, drywell pressure is transmitted to primary containment (vacuum breakers, horizontal vents) by design, so the better parameter to analyze is primary containment pressure rather than drywell pressure. In this way, primary containment level coincides with suppression pool level, etc. These parameters which depend upon each other will implicate dependent functions which should be eliminated. These eliminated functions are marked with N/A in Table 6.

The final PFL-3 Critical Functions for a BWR Mark-III containment are:

- Control suppression pool temperature
- Control drywell temperature
- Control primary containment temperature
- Control primary containment pressure
- Control suppression pool level
- Control hydrogen concentration in primary containment envelope

The ESBWR PFL-3 Critical Functions for the primary containment have been identified and they are the bases for EPGs. These Critical Functions are identified in the EPGs and in the ESBWR DCD.

Example 2. Subgoal A.G.-3 (Electrical Conversion with the Highest Efficiency)

As another example, if Critical Functions associated with the Availability-related subgoal A.G.-3 are going to be defined, the questions and their answers are:

Which boundaries are necessary to meet the subgoal?

This subgoal will be satisfied when the production reaches maximum established in the design basis.

As was done with safety related Critical Functions, boundaries are chosen taking into account the place where the process associated with the intended subgoal is performed in the plant. Boundaries proposed are:

- The design basis takes into account the material properties in the fuel, cladding, heat removal rate, steam cycle (Clausius-Rankine Cycle 4 transitions), turbine and generator to define critical function boundaries. The steam cycle side is addressed in the example 2 and the reactor heat up cycle (e.g., Reactor heating and power control (2→3)) is addressed in example 3. Turbine and MSR set (process 3→4)

  - Condenser (process 4→1)
  - Heaters chain (process 1→2)
- By systems involved in electrical efficiency
  - Electrical Generator

Parameters have been chosen taking into account the thermodynamic parameters involved in Clausius-Rankine cycle efficiency, and generator thermodynamic and electrical characteristics. Parameters should also be chosen in such a way that they characterize the process performed (i.e., steam expansion in the turbine could be characterized by inlet pressure) and by their influence in the global Rankine cycle efficiency (high temperature in the electrical generator caused by a loss of cooling or loss of pressure in turbine caused by loss of sealing steam involve a challenge to production).

These are the parameters that need to be controlled in order to fulfill the subgoal, taking into account the boundaries:

- Reactor Water Level
- Rector Pressure
- Steam Flow
- Water Flow (to reactor)
- Temperature
- Efficiency
- Electrical Parameters

This treatment is similar to that of a safety related subgoal, meaning that decreasing efficiency is a challenge against the production goal.

Which actions are necessary to perform with these parameters in order to meet the subgoal?

The final PFL-3 Critical Functions to accomplish this PFL-2, A.G.-3 subgoal will be the following (see Table 7):

- Maintain reactor water level
- Control MSR level
- Maximize generator efficiency
- Control electrical parameters

- Control turbine & MSR pressure
- Control turbine steam flow
- Control turbine & MSR temperature
- Maximize turbine efficiency
- Prevent generator water level increase (PWR only)
- Control generator H2 pressure
- Control generator temperature
- Control condenser water level
- Control condenser pressure
- Maximize condenser efficiency
- Control heaters level
- Control heaters steam flow
- Monitor heaters temperature
- Maximize heaters efficiency

Example 3. Subgoal A.G.-2 (Control NSS under all operational modes)

As another example of defining Critical Functions associated with the availability-related subgoal, A.G.-2 can be performed using the following methodology. For this subgoal, process 2→3 in the Clausius-Rankine cycle is considered. Using the same method and analysis criteria as the other examples, the questions and their answers are:

Which boundaries are necessary to meet the subgoal?

- Reactor core
- Reactor vessel
- Condenser

What are the necessary parameters to be controlled in order to meet the subgoal, taking into account the boundaries?

- Thermal limits
- Neutron flux distribution
- Nuclear power
- Pressure
- Water level

Considering these boundaries and parameters, the steam production from nuclear fission is addressed.

Which actions are necessary to perform with these parameters in order to meet the subgoal?

The final PFL-3 Critical Functions to accomplish this PFL-2, A.G.-2 subgoal will be the following (see Table 7):

- Maintain reactor core within thermal limits
- Control neutron flux distribution
- Control reactor power
- Control reactor pressure
- Maintain reactor water level
- Control condenser pressure

All Critical Functions can be identified through the application of this method to the whole set of subgoals. At the end of the process a set of Critical Functions would be obtained. This set could not be a minimal set because different subgoals could have associated closely-related Critical Functions which could be treated as a whole. These functions should be identified and integrated. The integration, however, must not cause unique requirements (and traceability) associated with a particular subgoal to be missed altogether. In order to purge this set of functions, the following questions should be asked for each function:

- Is this function necessary? Can it be eliminated?
- Can this function be combined with another? Should it be divided?
- Can this function be improved?

Critical Functions identified for a BWR-6 are shown in Figures 4 and 5. The safety related subgoals and related Critical Functions have been identified for the ABWR. Those Critical Functions will be the bases for the identification of performance requirements described in Subsection 3.3.

3.3 Method for Performance Requirements Identification (PFL-4)

The identification of performance requirements (or sub-functions) for each Critical Function defined in Subsection 3.2 is the fourth level in the hierarchical structure. These performance requirements are the interface between plant systems functions and design basis, and top-level plant functional structure (see Table 3).

If the performance requirements are well defined they will constitute the set of functions to which the System should provide control and/or monitoring capability by the operator, by the machine, or by both.

The method for specifying performance requirements is similar to that used for specifying Critical Functions identification.

The following difference should be noticed. For these sub-functions, the boundary is imposed by the Critical Function from which the sub-function (requirement) derives. If a Critical Function is well constructed, it should have a well defined boundary, parameter and action.

The question for each Critical Function is "How could the action required by the Critical Function be accomplished?" To answer this question, the design team should prepare a list with all feasible methods to perform the Critical Function. These methods could include a physical process (i.e., steam condensation to control pressure), or engineered features needed (as need of turbine lubrication or generator's stator or rotor cooling to improve the efficiency). All possibilities should be considered in a first approach in order to avoid an early restriction that may produce a less than complete analysis.

When all possibilities are listed, they should be reviewed in order to eliminate those that are not technically feasible. The ESBWR DCD, industry standards, and operating experience should be consulted for this purpose. The questions to ask for this purpose could be:

- Is this proposed method technically feasible?
- Has this method a precedent in previous designs?
- Is this method necessary? Can it be eliminated?
- Is this method imposed by mandatory regulations?

As for Critical Functions, elimination of possibilities that are not technically feasible, combined with expressing functions with conciseness and brevity, should result in requirements that specify:

- Boundary: where the requirement applies.
- Parameter: what is managed with the method.
- Action: what it is necessary to do with the parameter.
- Plant condition: safety related or non-safety related requirement (this is implicit and comes from the function from which the requirement derives).

An example of such a performance requirement (at PFL-4) is:

The system shall provide control and/or monitor capability for reactor water flow in (non-accident condition).

In this example, "reactor" is the boundary, "water" is the parameter (an alternative could be "coolant") and "flow in" is the action, and it is a non-safety requirement because it derives from a non-safety related function.

As an example, sub-functions for PFL-3 availability-related Critical Function A.C.F-5 (Maintain Reactor Water Level & Purity) will be defined. However, for simplicity, only water level will be addressed in this example.

Function:	Maintain reactor water level and purity
Question:	How could the action required by the Critical Function be accomplished?

Joining the question and the function, the next question results: How (which methods could be used) could the level of water in the reactor be maintained?

The methods proposed are:

- Reactor water flow in
- Reactor water flow out
- Steam condensation
- Steam relief
- Coolant temperature variation
- Vessel geometry variation

All these methods could be used to maintain reactor vessel water level (inventory). They should be reviewed in order to eliminate those which do not apply, so it is necessary to answer the following questions:

- Is this proposed method technically feasible?
- Has this method a precedent in previous designs?
- Is this method necessary? Can it be eliminated?
- Is this method imposed by mandatory regulations?

Answering these questions it can be seen that to modify vessel geometry is not a feasible technical solution, because vessel geometry cannot be changed during plant operation, so this method can be deleted. The remaining methods have been used in the nuclear industry for years and are feasible possibilities.

The final set emerging from this process will constitute the performance requirements for this function. In other words, the HSI should provide the operator with the capability to accomplish and monitor these requirements. Taking this into account, the final answer will be:

In order to maintain the level of water in the reactor under non-accident conditions, the operator should have the capability to monitor and/or control the following:

- *Reactor water flow in*
- *Reactor water flow out*
- *Steam condensation*
- *Steam relief*
- *Coolant temperature variation*

Figure 6 shows a block diagram including the performance requirements for the following Critical Functions:

- Reactor Power Control
- Reactor Pressure Control
- Reactor Water Level and Purity

Figure A-1 in Appendix A shows the HSI functional structure through the fourth level.

4 Methods and Criteria to Perform System Level Functional Analysis Based on Plant Performance Requirements

4.1 Interface Between Plant Performance Requirements and System Functions

The objective of this step in the analysis is to identify the systems (including specific system modes of operation), as defined in the ESBWR Project SDDs, whose functions are relied upon to meet the plant performance requirements defined in the plant-level functional analysis. The safety related and non-safety related functions of a system are identified in Sections 3.1.1 and 3.1.2 of the systems' SDD. The basis for the functions are also defined in the SDD. The functions are based upon design and operating experience, regulatory requirements, industry requirements (i.e., IEEE, etc.) and utility specification requirements. The utility specification may provide

requirements that are specific to the plant site or implements customer requirements for implementation of specific regulatory or industry requirements. The performance requirements of the system to meet its design functions are described in Section 3.3.2 of the SDD. This SDD format is applicable to all ESBWR SDDs.

The plant performance requirements used to conduct these identifications are *final requirements* in the sense that the plant performance requirements which are closely related (and can therefore be treated as a unified group) should have been integrated previously. Integration is described in Section 8.

Each plant performance requirement (sub-function) is performed by using one or more subsystems or components of the plant (as specified in the ESBWR Project SDDs for example). For instance, "steam relief" could be performed by more than one system and with very different purposes. Steam relief could be (a) a safety action taken to avoid a high pressure condition in the reactor pressure vessel, (b) a control action taken in response to an anticipated operating transient such as a load rejection, or (c) a normal operational action taken as part of an adjustment to main generator electrical output.

A system could be assigned to more than one requirement for two reasons. First, the system could have been designed to perform different functions (i.e., RHR in a BWR-6 may inject water into the RPV in order to maintain water level and condense steam in order to maintain RPV pressure). Secondly, an action performed by a system can cover two or more requirements (feedwater injection is necessary to produce steam and to cool the core). This is a top-level assignment because only the system considered as a whole is assigned to the requirements. More detailed analysis will be conducted for each system.

Systems may provide or receive performance requirements from other systems. As an example, reactor water level may cause an initiation signal to safety related system functions of the RCIC or HPCF systems. These interfaces are defined in Section 3.5, System Interface, of the SDD. Each of the interfacing systems and its applicable functions are defined in Section 3.5. For detailed functions and performance requirements, the applicable SDDs must be reviewed. Detailed interfaces may only be defined in the system P&IDs and logic diagrams.

For complex systems, it may be necessary to develop a matrix that identifies the relationship between functions identified in Section 3.1 of the SDD and performance requirements of interfacing systems. Table 8 and 9 are provided as examples of formats that may be used as necessary.

Requirement: is the first format input. The plant performance requirement to be analyzed must be written in this field.

Function: the plant performance requirement derives from the Critical Function. The Critical Function must be written in this field.

A.G.-1,... or S.G.-1,...: PFL-2 subgoals related to the function must be identified in this field by crossing the proper box (Y if it is related and N if it is not related).

Normal Operations and Barriers: This field shows normal operations covered for each availability-related subgoal, and barriers preserved by each safety related subgoal.

System Function: is the function(s) of system(s) related to the requirement?

To use this format, the designer should list all system functions which are related to the requirement under study and to specify, by crossing the proper box, which normal operation is covered or which barrier is defended by the system function. The starting point for the ESBWR will be the latest database file from previous ABWR designs. However, to illustrate the format and process for allocation of functions a BWR-6, safety related, PFL-4 plant performance requirement for control rod insertion is shown below.

	Requirement: Rods Insertion control and/or monitoring capability				**PFL-4**
	Function:				**PFL-3**
Barriers Against Radioactive Release:	**S.G.-1**	**S.G.-2**	**S.G.-3**	**S.G.-4**	**PFL-2**
1. Fuel Clad	Reactor Protection	Primary Containment	Secondary Containment	Activity Release Control	
2. Boundary of RCS					
3. Primary Containment	**Y**	**N**	**N**	**N**	
4. Secondary Containment	**Barriers**	**Barriers**	**Barriers**	**Barriers**	
5. Normal operation activity release control	**1** **2**	**3**	**4**	**5**	
System Functions					
Reactor Protection System	X X				**SFL-1**
Alternative Rod Insertion	X X				

This is a type of output that can be obtained from a database program. The database program also provides the means to maintain the lessons learned from past designs

and provides a way for linking component names, numbers, systems, functions, barriers, etc. with other project databases.

4.2 System Functional Analysis Methodology

System functional analysis is performed following completion of the plant-level functional analysis with the plant performance requirements having been obtained. Systems (as a group of functions) are analyzed instead of individual functions for the following reasons:

1. The information available is that provided by the designer of the systems, and these constitute a logical unit for study.

2. All the functions of a system will be performed within the components (human, hardware, software, etc.) constituting the system.

3. The low level control is designed on the basis of systems rather than functions.

This methodology does not conflict with function and objective compliance-based plant operation because the process described in Section 4.1 identifies the system functions which partially or totally satisfy the plant performance requirements. The end result will be a tree structure covering everything from general plant objectives down to the functions of each individual component (pump, valve, etc.), regardless of how the functional study has been performed at the system level.

Furthermore, functional analysis for the ESBWR Project can take advantage of predecessor system ABWR designs. Depending on the schedule for completing certain ESBWR Project engineering activities, systems analysis could also be based on functions defined in the ABWRs that followed US NUREGs and implemented NUREG 0700 and 0711, thus confirming the top-level functional structure of the plant.

The method to be applied will be analogous to that developed to determine the plant performance requirements, working from the system goals (functions) and moving towards determination of the system performance requirements and associated information and control requirements. These results will provide input for the human-machine function allocation plan, which will determine the functions assigned to the operator, those assigned to the software, those assigned to the machine, and those functions to be shared. Functions assigned to the operator will be studied during Task Analysis in order to determine the features to be implemented in the control room.

This section will explain the steps to be taken for performance of system functional analysis. The examples used to illustrate this methodology will be the functional

breakdown of the RWCU (Reactor Water Cleanup) (G33) system from a generic BWR-6 plant Since the process is generic, it can be applied to the ESBWR, ABWR and even PWRs.

As in the case of identification of the Plant Performance Requirements, the analysis tool used will be a Functional Diagram including logic gates to express the different combinations of processes, sub-systems, equipment and components required for compliance with the function being analyzed.

4.2.1 System Functions Identification (SFL-1)

Given that the aim of a system is to satisfy the functions for which it has been designed, these functions will constitute the system goals. These goals will be obtained from those listed in the corresponding section of the applicable ESBWR Project SDD. The result will be a list of functions to be accomplished by the system.

In the example used here, the functions to be accomplished by the BWR-6 RWCU system are as follows:

1. To reduce the amount of impurities in the reactor water in order to avoid their being deposited on the fuel elements, and to maintain the quality of the water.
2. To discharge excess water from the vessel during reactor STARTUP, SHUTDOWN, REFUELING and HOT STANDBY conditions.
3. To reduce the secondary sources of gamma and beta radiation by removing corrosion products, impurities and possible fission products from the reactor water.
4. To provide a reactor vessel drainage path.
5. To minimize temperature stratification in the lower part of the reactor vessel.

In this example, only the hierarchical structure of function 1 "Purify RPV water" will be dealt with.

4.2.2 System Process Identification (SFL-2)

Once these functions have been obtained, they will be broken down into the individual processes performed by the system in order to accomplish them. These processes should be such that compliance implies the capability of the system to perform the function (capability level). Breaking down a function into simple processes may be accomplished in many ways. Its is advisable that the same breakdown criteria be used by all analysts, as follows:

- The processes should be only those required to accomplish the function.

- The processes chosen should be as "basic" as possible, without division becoming excessive.
- They should be independent from one another.
- Each process should be located in the part of the system that is being analyzed.
- That part of the system associated with each process will be defined by the functions of the component (i.e., the individual function assigned to each system component by design).

The following example will show how the breakdown criteria defined above is applied, using the BWR-6 plant RWCU system function "Purify RPV water".

- Step 1 - Initial process identification

  The first step will be to identify the processes carried out by the system in order to perform the selected function. In this respect, the analyst should answer the following question:

  WHAT basic processes will the system carry out in order to perform the function?

  The answer to this question will provide an initial number of processes, which will not necessarily be definitive.

  Thus, in the case of the BWR/6 RWCU system, the question will be as follows:

  WHAT basic actions does the RWCU system perform in order to purify the reactor water?

  This question leads us to deduce a series of processes, as shown in Figure 7.

- Step 2 - Identified process review

  The next step consists of a review in order to verify that the proposed processes are mutually independent. To accomplish this, the following question will have to be answered:

  Are the proposed processes independent?

  In the example, the RWCU system cleanup function has been broken down into 6 processes:

- Vessel water flow out
- Transport (pumping)
- Cooling
- Filtering/demineralization
- Heating
- Injection (return) to the vessel

More detailed analysis shows that the cooling process is required because the physical characteristics of the demineralizer resins used in design are not capable of withstanding temperatures in excess of 55°C. As a result, this cooling might be included as part of filtering/demineralization due to its being a dependent process.

The heating performed subsequent to the filtering/demineralization process is a result of the need to prevent thermal stresses in the RPV return lines. Consequently, it might be included as part of the makeup or flow in process, for the same reasons of dependence as pointed to above. The final result of this process of revision is shown in Figure 8.

- Step 3 - Identification of process boundaries into the physical system

This step consists of bounding the part of the system in which each process is analyzed. For this purpose the corresponding diagram must be used (P&ID, IED, etc.) to determine the components (valves, pumps, piping, etc.) associated with each process, taking into account the specification provided by the designer. In Appendix A, Figure A-3 shows the BWR-6 RWCU P&ID used in this example.

The following procedure must be followed in order to accomplish this bounding:

- Identification of the main components associated with each process. In the example used, the following will be obtained:

  Flow out: Letdown isolation valves (MOV G33-F001 and F004)

  Transport: Pumps (G33-C002A/B)

  Cleanup: Regenerating heat exchangers, non-regenerating heat exchangers and filters/demineralizers subsystem (G36-D001A/B)

  Flow in: Makeup isolation valves (MOV G33-F040 and F039)

- Identification of the auxiliary components associated with each of the main components:

  Flow out: Letdown valves (MOV G33-F100, F106 and F102)

  Transport: Pump isolation valves (HOV G33-F043A, F005A, F013A, F045A, F150, F151, F152, F159) and secondary containment isolation valves (MOV G33-F054 and F053)

  Cleanup: Heat exchanger isolation valves (HOV G33-F105) and filter/demineralizer bypass valve (MOV G33-F044)

  Flow in: Valves associated with the return line (HOV G33-F079A/B), heat exchanger bypass valve (MOV G33-F104) and heat exchanger isolation valve (MOV G33-F042)

In this way, the basic processes that determine the capability of the system to perform the function under analysis have been obtained. This level of analysis identifies the processes necessary to successfully achieve performance of a function.

The level of system capability to perform the function is represented in Figure 9, in which the AND gate expresses the need for the four processes to be accomplished in order for the function to be performed.

4.2.3 System Processing Elements Identification (SFL-3)

This analyses level includes analysis of what physical support (system element) must be available in order for the process to be carried out (i.e., availability of a train, chain, etc.) but without consideration being given to the conditions required for this to occur (which will be analyzed at the next level). The criteria to be used for this analysis are as follows:

- The system elements considered should only be those related to the function and process under consideration.

- The availability of a system element should depend on the requirements of the process, which will be determined by the design basis of the system itself. Thus, in order for a hydraulic circuit to be considered available it is not only necessary for the components to be correctly aligned, but also for the flow provided by the impelling element to be adequate for correct operation, in accordance with design. Thus, a 50% pump and correctly aligned components do not necessarily imply the availability of a system element.

- Consideration should be given to all the possible alternatives leading to accomplishment of the process in question. For example, if the return path of a hydraulic circuit may be established indistinctly via either of two parallel-

mounted valves, two process elements will be considered, one for each valve, related by means of a logic OR gate.

By way of an example, the processes RPV water flow out and transport, defined at the previous level, will be analyzed.

In the first case to be studied, it may be deduced from the P&ID shown in the Figure that the vessel water suction paths are as follows:

- From recirculation loop A. 100% capacity line
- From recirculation loop B. 100% capacity lines
- From the lower region of the vessel. 25% (approx.)

Consequently, the paths that should be available in order for the vessel suction capacity to be covered are as follows:

- From one single recirculation loop OR
- From both recirculation loops OR
- From the lower region of the vessel AND from one OR two recirculation loops

All these situations are shown in Figure 10; the logic gates express the possible combinations leading to performance of the process in question.

The following availability alternatives are deduced from the flow diagram, in relation to the transport process:

- Pumping train A available OR
- Pumping train B available OR
- Both trains available

Figure 11 shows the block diagram for these situations.

4.2.4 System Performance Requirements Identification (SFL-4)

This level includes an analysis of the components required (valves, pumps, etc.) to achieve availability of the process elements. This analysis results in identification of the system component alignments possible for performance of the function.

The following criteria should be used in carrying out this analysis:

- Consideration should be given to all the components, including locally operated components.

- The status of the components performing the function in question should be analyzed. Special operations such as equipment tests, conditioning and maintenance should be studied as a separate function. Thus, if the function under study in this case is reactor water purification by means of the RWCU system, changing of the filter element should not be analyzed, despite its being an operation performed during normal RWCU operation, since its objective is not purification.

- Local operations should be considered at a global level. Thus, heat exchanger vented and filled, or filter in service, will be entered to express the availability of these components, the understanding being that all the necessary maintenance operations have been performed (these operations will be analyzed at the next level as part of the requirements relating to component operability).

- Each component should be specified clearly. Thus, if reference is to a valve, it should be identified by type of drive, Master Parts List (MPL) or equivalent identifier, and component number.

This analysis will be carried out as follows:

- For each part of the system identified at the previous level, the flow path providing its availability will be established.

- The required status of each component (valve open or closed, pump started, controller in auto or manual, etc.) should be identified for the flow path considered.

These steps should be accomplished by filling in the following format (an example of this format is shown in Appendix A, Figure A-2).

System: **MPL:** **Function:** **Critical Function to Safety: Yes ☐ No ☐** **Process:** **Process Element:**		
Component	**Required Status**	**Support Requirements**

This format shall be filled in according to the following criteria:

- **FUNCTION** field: The function under analysis will be included in this field.

- **CRITICAL FUNCTION (Y/N)** field: This field will be filled with the information obtained in Section 5 about the character of the function (safety or not-safety).
- **PROCESS** field: The process under analysis will be included in this field.
- **PROCESS ELEMENT** field: The process element under analysis will be included in this field.
- **COMPONENT** field: This field will include all the components identified as being necessary for correct compliance by the process element.
- **STATUS** field: The information included here will be the required status required by each of the components for the process element in question to be satisfied.
- **SUPPORT REQUIREMENTS** field: The results of the analysis described in *System Support Requirements Identification* (SFL-5) will be inserted in this field.

For the process element train A available in the example considered, the following will be obtained:

System: Reactor water cleanup	**MPL: G33**	
Function: Purify RPV water	**Critical Function to Safety: Yes ☐ No ☒**	
Process: Transport capability		
Process Element: Train A available		
Component	**Status**	**Support Requirements**
HOV G33-F043	OPEN	
HOV G33-F005A	OPEN	
HOV G33-F013	OPEN	
G33 PUMP C002	ON	
MOV G33-F001	OPEN	
MOV G33-F004	OPEN	
MOV G33-F054	OPEN	
MOV G33-F053	OPEN	

4.2.5 System Support Requirements Identification (SFL-5)

This level identifies all the conditions required for each of the components to remain in the operability status determined by the system performance requirements. This level is determined by the system design specifications. It consists basically of

reflecting the conditions of operability described for each component in the system design specification.

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

System: Reactor water cleanup		**MPL: G33**
Function: Purify RPV water	**Critical Function to Safety: Yes ☐**	**No ☒**
Process: Transport capability		
Process Element: Train A available		
Component	**Status**	**Support Requirements**
HOV G33-F043	OPEN	
HOV G33-F005A	OPEN	
HOV G33-F013	OPEN	
G33 PUMP C001	ON	—Power supply available (BUS---) —Lubrication available (MPL---) —RUN order —NO pump trip signal: MOV G33-F001 not fully open MOV G33-F004 not fully open Suction low flow Inlet F/D High temperature Electrical protection actuated
MOV G33-F001	OPEN	
MOV G33-F004	OPEN	
MOV G33-F054	OPEN	
MOV G33-F053	OPEN	

System Operation Modes and Change Modes Identification

As a result of the analysis performed in the previous sections, a block diagram (Figures A-4 and A-5 in Appendix A) will be obtained, reflecting all the relationships of dependence between the different levels studied (SFLs). One of the results that might be derived from level SFL-4 is acquisition of all the system component alignments possible for performance of the function considered to be achieved.

Correct interpretation of the logic gates used in the functional flow diagram makes it possible to identify all the possible component alignments capable of ensuring the function.

This analysis makes it possible to define the different system operating modes that allow the function to be performed. Operating mode is the name we shall give to those alignments which are capable of performing the function. Each mode will be identified by a number followed by an indication of the function in question. Each possible alignment within this mode will be known as a sub-mode, and will be identified by the mode number followed by a letter. Thus, for the example used here we would have the following:

Mode 1 - RPV water purification - With respect to this mode, it is necessary to identify all the possible paths for function performance. In this way the operating sub-modes of each mode are obtained.

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

- The "ready to start" alignment (standby mode)
- 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 will be taken into account. All the modes of operation obtained will be listed.

For each system function defined in *System Functions Identification (SFL-1)*, there will be an associated operating mode (each possibly with different sub-modes) meeting the corresponding requirements for performance. Thus, for the functions defined for the RWCU system, we would have the following operating modes:

Mode	Description
0	System out of service
1	RPV water purification
2	RPV water overboarding
3	RPV drain
4	RPV thermal stratification reduction

In this case the mode zero has been defined as the out of service alignment because it does not have a "ready to start mode". The relationship between system functions and operating modes is not a one-to-one relationship. Indeed, for the five SFL-1 functions defined in Sec. 4.2.1 only four operating modes different from the zero mode of operation are considered since the gamma and beta radiation secondary source reduction function is satisfied by operating modes 1 and 2.

The status for all the components of the system for each mode, in relation with the mode zero, will be addressed in a table like the next one:

	Mode					
Component	0	1A	1B	2	3	...
MOV G33-F001	C	O	...	...	...	...
...	...	...	...	...	...	...
...	...	...	...	...	...	...
Pump C001	S	ON	...	...	...	...
Heater B001	OS	A	...	...	...	...
...	...	...	...	...	...	...

O: Open	F: Fail position	OS: Out of service
C: Closed	T: Throttling	S: Stop
A: Available	TO: Throttling or open	
ON: Run	TC: Throttling or closed	

All the components of the system will be listed in the component column. The Mode 0 ("zero") column will reflect status of the system components for that mode, and the rest of the columns will show the differences between the respective mode for that column and the Mode 0.

Once all the system operating modes and sub-modes have been identified, identification of the change modes will begin. The change modes will reflect those changes to component status which must occur for system operation to switch from

one mode or sub-mode to another. Change modes will be defined as shown in Figure 12.

The following criteria are used to identify all the feasible change modes:

- All changes starting from or ending at Mode 0 will not be considered change modes because they are reflected in the mode of operation table.
- If a system has two or more 100% independent loops, the change modes between loops will not be considered as change modes.
- The change modes must be technically feasible and coherent with design basis and functions established by the designer.

In order to document change modes, 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 mode, from an initial mode. In addition, a table such as Table 2 showing the feasible change modes will be created.

5 Identification of Functions Critical to Safety

5.1 General

The methodology of analysis proposed in Section 3 identifies the safety related plant Critical Functions as those functions needed to accomplish the plant's safety functional requirements. These functions, based on EPGs and Design Basis Accidents (DBA), are identified for a BWR-6 and shown in Figure 4. The design team should identify the safety related Critical Functions for the ESBWR plant systems as described in the ESBWR Project SDDs.

These functions cover the accident conditions because if one of these functions was not achieved, the respective subgoal (and consequently the primary safety subgoal) will be not satisfied. For the System Level Functional Analysis proposed in Section 4, all the events analyzed in the ESBWR DCD Chapter 15 Accident Analysis should be considered to satisfy the design basis conditions.

5.2 Accident Analysis

A Nuclear Safety Operational Analysis (NSOA) is conducted on the ESBWR DCD Chapter 15 accident scenarios to define unacceptable safety results and any required safety actions necessary to achieve acceptable safety results are identified. In addition, an evaluation of the entire spectrum of events in Chapter 19 is systematically carried out to demonstrate that an acceptable level of safety has been attained using measures of risk.

The scope of situations analyzed includes anticipated (expected) operational occurrences (AOOs) (e.g., loss of electrical load), abnormal (unexpected) transients that induce system operations condition disturbances, postulated accident of low probability (e.g., the sudden loss of integrity of a major component), and finally hypothetical events of extremely low probability (e.g., anticipated transient without the operation of the entire control rod drive system).

The starting point for NSOA is the establishment of unacceptable safety results. This concept enables the results of any safety analysis to be compared to applicable criteria. Unacceptable safety results represent an extension of the nuclear design criteria for plant system and components which are used as the basis for system design. The unacceptable safety results have been selected so that they are consistent with applicable regulations and industry codes and standards.

The full spectrum of initial conditions limited by constraints placed on planned operation for AOOs, accidents, and plant capability demonstrations are evaluated. All events are analyzed until a stable condition is obtained. This assures that the event being evaluated has no important long-term implications.

In the event analysis, all essential systems, operator actions, and limits to satisfy the required safety actions are identified. Limits are derived only for those parameters continuously available to the operator.

In the NSOA, a complete and consistent set of safety actions has been developed. These safety actions are those required to prevent unacceptable results. For transients and accidents a single failure proof path to plant shutdown must be shown. The application of a single failure criterion to these events is imposed as an additional measure of conservatism in the nuclear safety operational analysis process.

The spectrum of postulated initiating events developed from the NSOA is divided into categories based upon the type of disturbance and the expected frequency of the initiating events occurrence. Each event analyzed is assigned to one of eight categories listed in Chapter 15 of Regulatory Guide 1.70 [2.3(3)].

The methodology, and results, of accident analysis for design basis events will be included in the ESBWR DCD (Chapter 15). Additional reviews of operating experience addresses potential losses of availability and reduction of the safety margin. Future reviews of the important PRA sequences addresses beyond design basis events from the ESBWR DCD (Chapter 19) can challenge the operators to interact through the HSI in different ways with the plant.

5.3 Interface Between ESBWR DCD Chapter 15 and System Functional Requirements Analysis

A system function will be considered critical to safety if that function is required to achieve safety system performance requirements or this function which, if failed, could pose a safety hazard to plant personnel or to the general public. The design team should follow these steps in order to decide if a system function can be considered as a safety related Critical Function:

- Identify (from the ESBWR DCD Chapter 15 for example) all the design basis events in which the function is involved
- Analyze if that function is required to achieve safety system performance requirements (described in the ESBWR DCD for example).
- Judge, through study or analysis, whether or not there are potential consequences (e.g., from functional or performance deficiencies) that pose a safety hazard to plant personnel or to the general public.

If a system function is considered to be a Critical Function, it shall be documented in the function narrative description defined in Section 7.2 in order to ensure its inclusion in the analyses of Critical Functions during future stages. Critical functions can also include non-safety functions involving high asset value components, those that support plant availability, and capacity factor, and those requiring human resources that can become unavailable for other safety related tasks.

6 Method for Developing Graphic Function Description

Functional structure should be described initially in graphic form. Function diagramming shall be done starting at a "top level", where major functions are described, and continuing to decompose major functions to lower levels until specific requirements emerge.

The examples of functional structure shown in Sections 3 and 4 have been described in graphic form which accomplishes these requirements. The technique used to make these functional diagrams, called functional flow diagrams is the method proposed.

6.1 Method Description

A popular technique used for the determination of the system requirements is the Functional Flow Diagram (Ref. DOD-HDBK-763) [2.5(4)]. Functional flow diagrams can provide a detailed outline of all system requirements. They may be used as an extensive checklist of system functions that must be considered in assuring the ability of the system to perform the proposed goals. Functional flows are necessary to determine which system functional elements should be performed by operators, by software, by the machine or shared.

The Functional Flow Diagrams methodology starts with system goals, and then functional flows are developed interactively for more and more detailed system requirements. This process continues down to the level of specific system functions or, if necessary, the level of specific operator tasks. The designer judges what depth of analysis is appropriate. At this stage of functional analysis, a system function approach is recommended. During the construction of higher level flows, no distinction should be made between operator or machine implementation of system functions. This enables unbiased system trade studies to be performed in the succeeding functional allocation stage. A modification of this technique will be used.

Functional flows are constructed by arranging in tree-structure all of the various functions that are believed to pertain to a particular pre-defined goal (or sub-goal, depending on level of detail). Each function is a verb-noun combination. Occasionally nouns are assumed and adjectives are added. Each individual function is contained within a rectangular block. Each block is numbered for reference, more or less according to its sequence on the page. Each block is connected with all related blocks by arrows. Figure 13 shows a typical flowchart structure.

6.2 Flow Diagram Elements

In the next paragraphs, some concepts necessary to drawing functional flow diagrams are defined:

Reference block - If a function is repeated in other portions of the total series of functional flows, or if two defined functions are closely related and could be treated as a unit, the same number should be used and the block may be drawn as a reference block. Each functional flow diagram contains a reference to the next higher functional flow through the use of a reference block. Reference blocks may also be used to indicate functions occurring at the same level on different pages.

Symbols - The functional flow symbology used in Figure 13 is typical. The descending order between the function blocks indicates more levels of detail in the specification. Arrows should enter the block from the top to the bottom. Wherever arrows are joined or split out, they should be connected by AND, OR or AND/OR gates or junctions.

In success diagrams the significance of the AND junction is that all subordinate functions should be performed to accomplish a goal or a top-level function. The OR junction indicates a choice between two or more functions as to which one is performed. The AND and OR junctions may be combined if it will not cause confusion and page space is limited.

Functions - A function is that which must be accomplished by the system to perform a goal, a subgoal or a top-level function. So, all functions can be broken down or

divided into more detailed functions. Top-level and first level functions tend to be identical for similar goals. A specific operational requirement may call for modification to these higher functions; however, the changes generally occur at the lower level functions. This is a step approach to a complex problem dividing it into more and more specific functions, from abstract functions to system level specific functions. The global concept of functional level detail or definition must be based on the total size or scope of the particular system to be analyzed. For this stage of analysis, a four level approach is recommended.

Once the functional flows are constructed, the functions and sub-functions should be reviewed and analyzed in-depth for probable variations related to the system requirements.

An important point to take into account is that it is acceptable for the functional structure (format) to vary depending on the person who draws it—solutions can vary and still be correct. In view of this possible ambiguity, however, it is recommended that the parties concerned agree on the definition before considerable effort is expended on this technique. The definition of functional levels is not as important as the assurance that analysis is conducted to a sufficient degree of detail to determine significant HSI performance requirements.

Some of the essential features to take into account about the procedures for constructing functional flow diagrams are as follow:

- Functional flow blocks must contain a verb and a noun.
- It is essential to initiate the flows without any allocation to man or machine.
- Each expanded level of functional flow will contain more and more detailed information. The detail may be carried on to as many levels as appropriate. It is normally necessary to go to at least the third level.
- Functions are numbered in a manner which preserves continuity of function and logical breakout from function origin.
- The diagram should be organized so that one can easily find the input and follow the flow through the function blocks to the resulting output.
- It is generally good practice to limit the size of the diagrams. They should be divided up if too large for foldout pages in documents. Reference blocks may be used.

Functional flow diagrams have the following characteristics:

- The functional block numbering system provides a rationalized traceability from lower to higher level functions and between functions at the same level. Functional flows are flexible in that a change in one part of a total functional flow generally causes minimal effect on other parts. Because of this, they are easy to use to show the effects of preliminary functional allocation to man or machine. Functional flows are the ideal way to show relationships between functions.

- As more and more detailed functional flows are developed, specific system requirements begin to emerge. These requirements may then be documented by incorporation into system specifications.

7 Method for Developing Detailed Functions Narrative Description

7.1 Plant Performance Requirements Narrative Description

As discussed in Sections 3 and 4, requirements obtained from the functional analysis must be documented. This subsection describes a method for creating narrative descriptions for the plant performance requirements (PFL-4) identified in the fourth level of the hierarchical structure. The narrative descriptions are used as a basis for documenting lower level requirements obtained during system-level functional analysis (Section 7.2). Critical Functions (PFL-3) must also be documented in this way.

At this stage, the narrative descriptions should be general so as not to refer to specific solutions (implementations) or levels of automation and human involvement. The narrative description should eliminate all possible ambiguity for function interpretation. The descriptions should help the design team determine the basic operational information flow and processing required to accomplish the plant functions. Some table-oriented formats for collecting and recording the information used to assemble the narratives are offered as examples. However, the design team must decide what tool(s) to use to accomplish the formatting, recording, and assembly.

The plant performance requirements were defined by:

- **Boundary**. Where the requirement applies.

- **Parameter**. What is managed by the method.

- **Action**. What it is necessary to do with the parameter.

- **Plant condition**. Safety related or non-safety related requirement (this is implicit from the function from which the requirement derives).

The narrative describes these performance requirements, and it also answers the following four questions:

- Which observable parameters indicate system status? (The allocation process initially determines the functions that are to be monitored and alarmed by a machine and those to be monitored directly by an operator. For example, machines can monitor and alarm the turbine bearing temperature and vibration, where operators monitor the status of a redundant system out for service and the allowed outage time. Following the HFE evaluation process the initial allocations can be adjusted)
- What control process and data are required to achieve the function?
- How is successful completion of the function to be defined or measured?
- What alternatives are available if correct functioning is lost and how can alternatives be chosen? ("Alternatives" refers to requirements that can support a higher level function in place of the function being analyzed. For instance, boron injection is an alternative to control rod insertion in order to interrupt the nuclear power generation, or several redundant heat removal paths could be chosen depending on the plant conditions.)

Each item is now developed:

- Observable parameters that indicate system status

  These are observable parameters and the boundaries in which they apply. So, if a requirement is:

  The HSI shall provide control and/or monitor capability for reactor water flow in (non-accident condition)

  The parameter is the water flow into the reactor vessel.

- Control process and data required to achieve the function

  The control process to achieve the requirement (function) is the action to perform with the parameter. In the above example, the process to control would be to inject water into the reactor.

  "Data required to achieve the function" refers to plant data which are necessary to know in order to monitor the function. In the example above, feedwater flow could be among this data. Design basis, transient and accident analysis and operating experience should be used to determine these data.

- How successful completion of the function is defined or measured

  The definition or measure should be based on applicable normal operations, transient, and accident conditions. The designer should use information from several representative design basis events to identify performance measures that ensure the achievement of a function. Ideally, performance measures would be developed based upon a purely physical approach. For instance, one of the performance measures for core heat removal can be determined from the knowledge of the material used for the fuel cladding such as, for example, melting temperature. However, not all the performance measurements can be determined this way and information obtained from accident analyses could be used.

The following types of events should be included, consistent with analyses documented in Chapters 15 and 19 of the ESBWR DCD:

- Events requiring operations subjectively judged to be difficult in terms of complex data interpretation or control, control speed, etc.
- Events requiring the highest certainty of correct operator response (e.g., certain accident conditions)
- Events important in terms of the probabilistic risk assessment
- Events in which plant trip is highly probable unless corrective action is taken in time
- Events which occur frequently

The number of events to be included shall be large enough to adequately cover the functions associated with the hierarchical goal structure. For example, consider:

- Safety related events
  - Loss of coolant accidents
  - Main steamline breaks
  - Loss of all AC power
  - Anticipated transients without scram (ATWS)
- Availability-related events
  - Failure of control system sensors
  - Turbine/generator trip

The plant nuclear safety operational analysis (NSOA) described in the ESBWR DCD should be used to perform this analysis.

- **What alternatives are available if correct functioning is lost and how can alternatives be chosen?**

The requirements associated with a Critical Function should be analyzed in order to identify if one requirement is a redundant requirement, if the plant modes where the requirements apply are different, etc. A priorities scale should be made. This analysis should be based on:

  - Mandatory requirements (e.g., licensing and regulatory)
  - Operating experience
  - Industry standards
  - Plant operation mode
  - ESBWR systems design basis

7.2 System Level Function Narrative Description

All the general concepts dealt with in Section 7.1 in relation to Plant Performance Requirements should be applied to the system level functional analysis. The result will be identification of the parameters, limit values, etc., that complete the description of the system.

To perform this description, the following data collection format should be filled in (the full format is shown in Appendix A, Figure A-6):

System:	**MPL:**	
Function:	**Critical Function to Safety:**	**Yes** ☐ **No** ☐
Characteristic Parameter(s):	**Range:**	
Alternative Parameter(s):	**Range:**	
System Status Parameter & Limitations		
Parameter	**Limits**	**Comments**

The definition of the different fields of this format is as follows:

- **System field**: This field includes an identification of the system to which the function under analysis belongs.

- **Function field**: This field identifies the function being analyzed.
- **Critical Function (Y/N) field**: This field will be used to specify whether or not the function is considered to be critical for safety; i.e., whether or not it is part of the accident sequences analyzed in ESBWR DCD Chapter 15.
- **Characteristic Parameter and Range fields**: These fields will include a list of the physical parameters identifying function performance and the range of values considered acceptable for such performance. Choice of these parameters should be based on the design specifications, regulatory guides, accident analysis, etc.
- **Alternative Parameter and Range fields**: These fields will list those alternative physical parameters which, if the characteristic parameters are unavailable, might identify function performance. The range of acceptable values for these alternative parameters will also be specified. As in the previous field, the choice of these parameters should be based on the design specifications, regulatory guides, accident analysis, etc.
- **System Status Parameters and Limitations field**: This field specifies and documents the characteristic parameters which indicate the capability of the system to perform the function. It has been divided into three sub-fields:
  - **Parameter sub-field**: This sub-field will list the physical parameters characterizing each of the System Processing Elements. All those parameters required to characterize correct operation of the part of the system under consideration will be chosen. This choice of parameters should be based on operating experience, industry standards, mandatory requirements and recommendations by the system designer, as well as on analysis of events, transients, design basis accidents, etc. (Chapter 15 of ESBWR DCD). During the later stages, a check will be made of the need to incorporate all or part of these parameters in the HSI and the way in which they should be displayed.
  - **Limits sub-field**: This sub-field will indicate, for each parameter, the operating limits defining correct process performance. These limits shall be defined by design characteristics, mandatory requirements, etc.
  - **Comments sub-field**: This sub-field will be used to specify all comments considered necessary to justify choice of each particular parameter and its limits, such as the applicable regulatory guides, studies performed, etc.

The information included in the different formats for each system (i.e., all the functions) will provide a basis for selection of the system process instrumentation.

Along with the operating and change modes determined in Section 4, this will establish system information requirements.

An example of this data collection format is included in Figure 16 for the previous BWR-6 example RWCU system function Purify RPV Water (G33). This table includes only the parameters corresponding to the RPV Water Flow Out Capability and Transport Capability processes.

A short narrative description would be assembled using all of these parameters and the information provided by the functional structure described in Section 4. The content of the description would include the following:

1. System-related information
    a. System Functions (operational goals)
    b. System Processes
    c. System Process Elements, including such design features as:
        i) Automatic signals
        ii) Operational limits (normal, abnormal operating limits) and cautions
        iii) Set-points (for controls, alarms, etc.)
    d. Control features
    e. Relations with other systems
    f. Feasible Configurations (modes of operation) including:
        i) Alternatives
        ii) Redundancies
    g. Change modes
    h. Control Strategy
2. Component-related information
    a. Functions
    b. Redundancies
    c. Associated controls

d. Failure modes

e. Relations with other support systems

f. Set-points (for controls, alarms, etc.)

3. Integrity Data

a. Maintenance requirements (Maintenance personnel on the HFE team will verify the need for the HSI display to carry information on equipment status e.g., RTDs for motor windings, bearing vibration monitors, water quality, and etc. This will require interface with the suppliers to verify that automated information is correctly supplied and displayed).

b. Testing requirements (Testing personnel on the HFE team will verify the need for automated or manual testing of system and equipment either on line or during refueling periods. The HSI design must permit test signals to be entered and results displayed for shared and automated testing allocations. The testing group will interface with suppliers and verify that all automated and shared testing functions are adequately incorporated in the HSI and equipment designs.)

c. Surveillance requirements (Surveillance activities will be addressed through the HFE team. Proposed automated or shared technical specification surveillance activities will be verified for specific systems e.g., piping and vessel integrity monitoring, containment structural monitoring, system operability, etc. The HSI design must permit surveillance verification tests sequences to be entered and results displayed for shared and automated surveillance allocations. The surveillance group will interface with suppliers and verify that all automated and shared systems are adequately incorporated in the HSI and equipment designs.)

4. Applicable faults and accident analysis and results

Applicable events as analyzed in ESBWR DCD Chapter 15 should be used.

8 Analysis Methods Which Define the Integration of Closely Related Sub-functions or the Division of Identified Sub-functions

8.1 Integration/Division of Plant Performance Requirements

A comprehensive set of requirements must be determined because it will be the basis for further analysis. All requirements should be reviewed in order to obtain the best possible set. Thus, requirements that are too general should be divided into more

specific requirements. Redundant, or closely related, requirements should be integrated and treated as a unit.

A hierarchical structure of requirements should emerge from this process, so the fourth level in the global hierarchical structure could have some sublevels. Moving from top to bottom in the hierarchy, requirements become more and more specialized. The requirements at the bottom constitute the final set of performance requirements; they will be related to system level functions as stated in Section 4.

Figure 14 is a block diagram representation of this integration/division process.

Criteria

Two or more requirements could be considered closely-related if:

- They have the same boundary, parameter and action, and
- They have the same character: availability-related or safety related.

These conditions are necessary for requirements to be considered closely-related, but these conditions alone are insufficient. The designer must judge whether two requirements should be integrated.

One requirement could be divided into two or more requirements if:

- The boundary is too big and it can be divided into smaller boundaries.
- The parameter is complex and can be expressed by two or more simple parameters.

The designer must judge when a requirement should be divided.

The final set of requirements can be divided into two groups:

- Requirements whose common achievement is an essential condition for the accomplishment of a higher level function. These requirements will be called primary requirements.
- Requirements that are alternative supports to a higher level function or whose accomplishment is not an essential condition for a higher level function. These parameters will be called backup requirements.

Figure 15 shows a requirement which could be divided into two more specific requirements: one is a primary requirement "RPS scram" and the other is a backup requirement "Alternate Rod Insertion (ARI) scram".

8.2 Integration/Division of System Functions/Sub-functions

Once the final set of plant performance requirements is obtained and identified with system functions, these system functions should be analyzed in order to find the system level performance requirements shown in Section 4.2. The result of this analysis will be a hierarchical structure as shown in Figures A-4 and A-5 in Appendix A.

In that hierarchical structure the following identifications can be made:

System Function (SFL-1): Plant performance requirements which must be accomplished identified with some system function

System Process (SFL-2): Process which the system needs to perform in order to satisfy the system function

System Processing Element (SFL-3): Set of system components that are able to perform a system process by itself.

System processing elements make up the system sub-functions. These sub-functions could be grouped or divided as was shown in Section 8.1 with the plant performance requirements.

The functional block diagram created for each function should be used in the integration/division process. The criteria will be:

- Those sub-functions joined with OR gates can be integrated and treated as a unit. This logic defines that if some process elements are connected by an OR gate, it means that there the are alternative methods to perform the same process. In the RWCU example, the sub-functions train A available and train B available can be treated as a unit (pumping capability).
- Those sub-functions joined with AND gates can be divided into two groups:
  - Those sub-functions which are an essential condition for the accomplishment of a process. The sub-functions RHx (tubes) available and NRHx (tubes) available are an example of this. These functions are directly connected to the gate.
  - Those sub-functions which are an alternative supporting function to the process or those sub-functions for which accomplishment is not necessarily a requisite for the process. An example can be sub-function Filter/Demineralizer (F/D) bypass available. These functions are connected with a combination of OR and AND gates.

The information obtained from Sections 4.2 and 7.2 should be used to document these sub-functions. That is, each sub-function should be documented with:

- The reason why the sub-function is required (Section 4.2)
- The control action necessary for the accomplishment of the sub-function (Section 4.2)
- The parameters necessary for the sub-function control actions (Section 7.2)
- The criteria for evaluating the results of the sub-function control action (Section 7.2)
- The parameters necessary to verify the sub-function (Section 7.2)
- The criteria to be used to evaluate the sub-function (Section 7.2)

To summarize, starting from plant general goals the functional analysis provides a set of mutually related performance requirements (Plant level or System level) which let the HSI designer perform:

- An allocation of functions between human, machine or both
- A task analysis of activities necessary to accomplish these requirements

Table 1 Planned Operation

(Ref: Section 3.1.2, Availability Subgoals Identification)

1. **Achieving Criticality**: Includes all the plant actions normally accomplished in bringing the plant from a condition in which all control rods are fully inserted to a condition in which nuclear criticality is achieved and maintained.	
2. **Heatup**: Begins when achieving criticality ends and includes all plant actions normally accomplished in approaching nuclear system rated temperature and pressure by using nuclear power (reactor critical). Heatup extends through warm up and synchronization of the main turbine-generator.	**Startup** **Mode 2**
3. **Power Operation**: Begins when heatup ends and includes continued plant operation at power levels in excess of heatup power.	**Power Operation** **Mode 1**
4. **Achieving Shutdown**: Begins when the main generator is unloaded and includes all plant actions normally accomplished in achieving nuclear shutdown (more than one rod subcritical) following power operation.	**Hot Shutdown** **Mode 3**
5. **Cooldown**: Begins when nuclear shutdown is achieved and includes all plant actions normal including the continued removal of decay heat and reduction of RPV temperature and pressure.	**Cold Shutdown** **Mode 4**
6. **Refueling Outage**: Includes all the planned operations associated with a normal refueling outage.	**Refuel** **Mode 5**

Table 2 Typical Mode Change Matrix for a Hypothetical System

(Ref: System Operation Modes and Change Modes Identification at the end of Section 4.2)

To / From	1	2A	2B	3	4	5	6	7A	7B	8	...
1	n	1-2A	1-2B	X	1-4	1-5	X	X	X	X	...
2A	2A-1	n	2A-2B	X	2A-4	2A-5	X	X	X	X	...
2B	2B-1	2B-2A	n	X	2B-4	2B-5	X	X	X	X	...
3	X	X	X	n	X	X	X	X	X	X	...
4	X	X	X	X	n	X	X	X	X	X	...
5	5-1	5-2A	5-2B	X	X	n	X	X	X	X	...
6	X	X	X	X	X	X	n	6-7A	6-7B	X	...
7A	X	X	X	X	X	X	7A-6	n	X	X	...
7B	X	X	X	X	X	X	7B-6	X	n	X	...
8	8-1	8-2A	8-2B	X	X	X	X	X	X	n	...
...	...	...	...	...	...	...	...	...	...	...	n

Note:X indicates an excluded mode change

See Figure 12, Change Mode block Diagram

Table 3 Plant & System Functional Analysis Assignment

(Ref: Beginning of Section 3)

Level 1 Plant General Goals (PFL-1)	Plant Functional Analysis Level (Section 3)
Level 2 Plant Subgoals (PFL-2)	
Level 3 Plant Critical Functions (PFL-3)	
Level 4 Plant Performance Requirements (PFL-4) (the interface between the plant functional structure and the system functions and design basis)	
Level 5 Systems Goals (SFL-1)	System Functional Analysis Level (Section 4.2)
Level 6 Systems Subgoals (SFL-2)	
Level 7 Systems Critical Functions (SFL-3)	
Level 8 Systems Performance Requirements (SFL-4)	
Level 9 Systems Support Requirements (SFL-5)	

PFL: Plant Functional Level

SFL: System Functional Level

Table 4 BWR NPP Energetic Transformations

(Ref: Example of "Availability SubGoals Identification" in Section 3.1)

Energy	Nuclear Fission	Process		Electromagnetic Induction
		Steam Generation	Steam Expansion	
Nuclear	T1			
Thermal		T2		
Mechanical			T3	
Electrical				T4

Table 5 BWR Operational Modes

(Ref: Example of "Availability SubGoals Identification" in Section 3.1)

Mode	Reactor Mode Switch Position	Reactor Coolant T_{avg}
1: Power Operation	RUN	any
2: Startup	STARTUP/HOT STANDBY	any
3: Hot Shutdown	SHUTDOWN	>212°F
4: Cold Shutdown	SHUTDOWN	≥212°F
5: Refueling	SHUTDOWN OR REFUELING	≥140°F

Table 6 Primary Containment Integrity Selection Table

(Ref: Example 1 in Section 3.2)

	Boundary		
Parameter	**Suppression Pool**	**Drywell**	**Prim. Cont. Envelope**
Temperature	to control	to control	to control
Pressure	N/A	N/A	to control
Level	to control	N/A	N/A
H2 concentration	N/A	N/A	to control

Table 7 Electricity Production Selection Table

(Ref: Example 2 in Section 3.2)

	Boundary			
Parameter	**Turbine & MSR**	**Condenser**	**Heaters**	**Generator**
Level	to control	to control	to control	to prevent
Pressure	to control	to control	N/A	to control
Steam flow	to control	N/A	to control	N/A
Water flow	N/A	N/A	to control	N/A
Temperature	to control	N/A	to monitor	to control
Efficiency	to maximize	to maximize	to maximize	to maximize
Electrical Par.	N/A	N/A	N/A	to control

Table 7 NSS Selection Table

(Ref: Example 3 in Section 3.2)

	Boundary		
Parameter	**Reactor Core**	**Reactor Vessel**	**Condenser**
Thermal Limits	to maintain	N/A	N/A
Neutron Flux Distribution	to control	N/A	N/A
Nuclear Power	to control	N/A	N/A
Pressure	N/A	to control	to control
Water Level	N/A	to maintain	N/A

Table 8 Format for System Function/Availability-Related Requirements Identification

(Ref: Section 4.1)

	Requirement:				**PFL-4**
	Function:				**PFL-3**
Planned Operations:	A.G.-1	A.G.-2	A.G.-3	A.G.-4	PFL-2
1. Achieving Criticality 2. Heatup 3. Power Operation 4. Achieving Shutdown	Bring Plant to Oper. State of Power Y N	Control NSS Under All Oper. Modes Y N	Electrical Conversion with Highest Efficiency Y N	Shutdown & Refueling Y N	
5. Cooldown	Planned Op.	Planned Op.	Planned Op.	Planned Op.	
6. Refueling Outage	1 2	3	3	4 5 6	
System Functions					SFL-1

Table 9 Format for System Function/Safety Related Requirements Identification

(Ref: Section 4.1)

	Requirement:				**PFL-4**
	Function:				**PFL-3**
Barriers Against Radioactive Release: 1. Fuel Clad 2. Boundary of RCS 3. Primary Containment 4. Secondary Containment 5. Normal operation activity release control	S.G.-1 Reactor Protection Y N Barriers 1 2	S.G.-2 Primary Containment Y N Barriers 3	S.G.-3 Secondary Containment Y N Barriers 4	S.G.-4 Activity Release Control Y N Barriers 5	PFL-2
System Functions					SFL-1

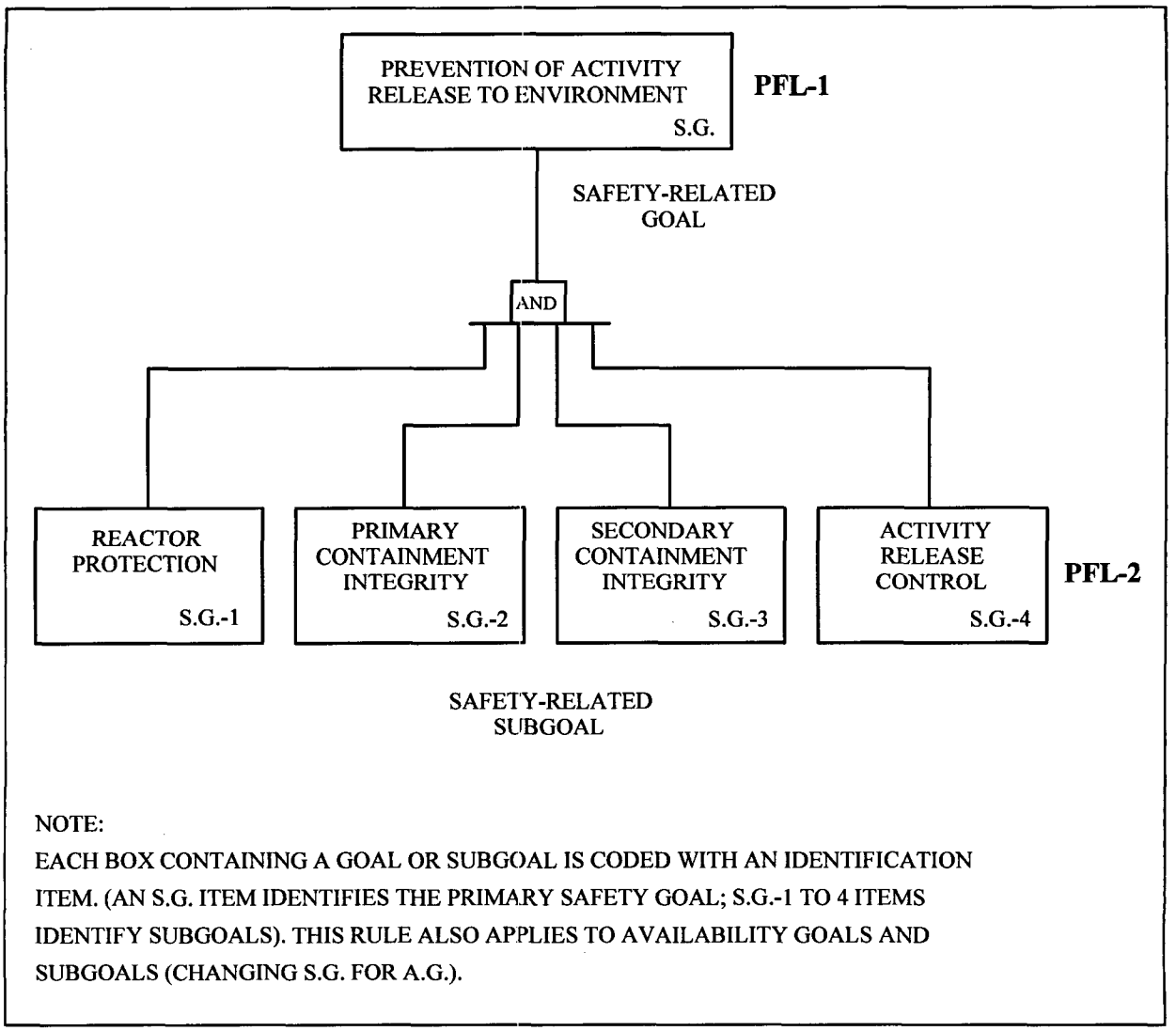

Figure 1 Block Diagram for Safety Subgoals

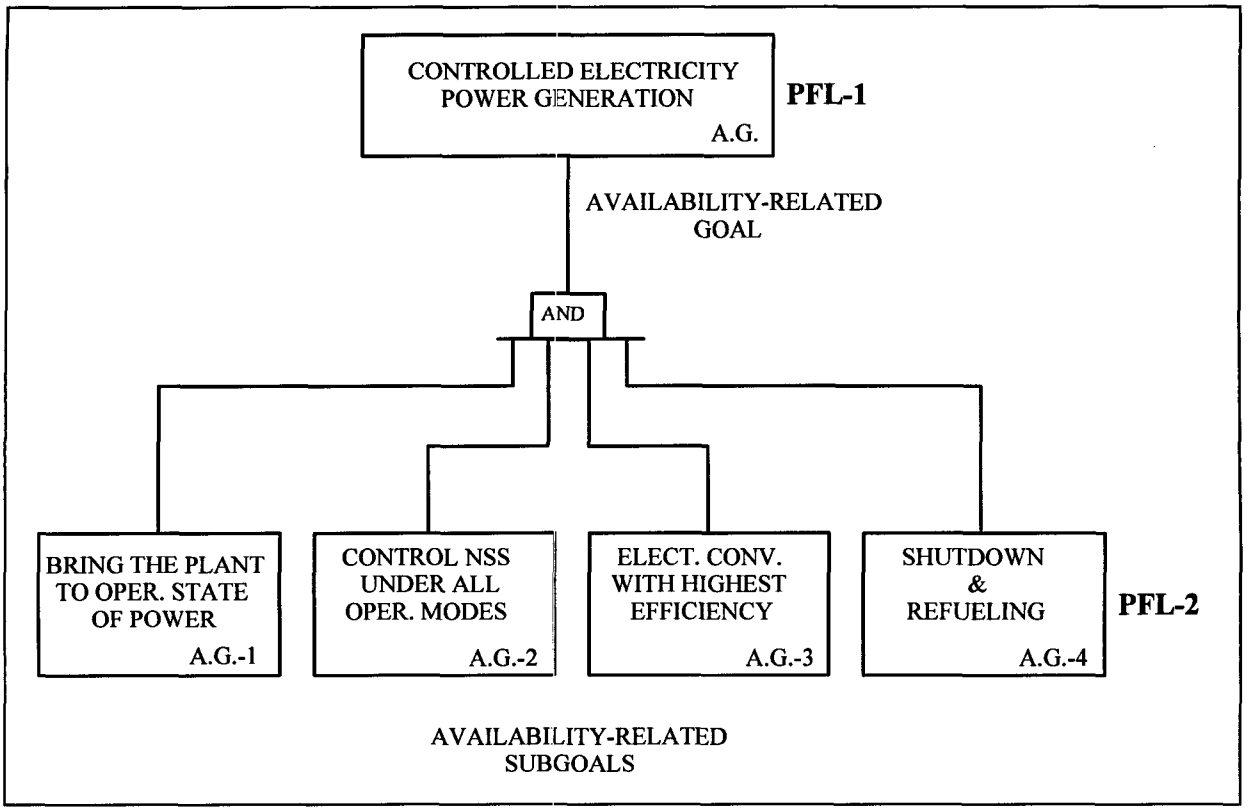

Figure 2 Block Diagram for Availability-Related Subgoals

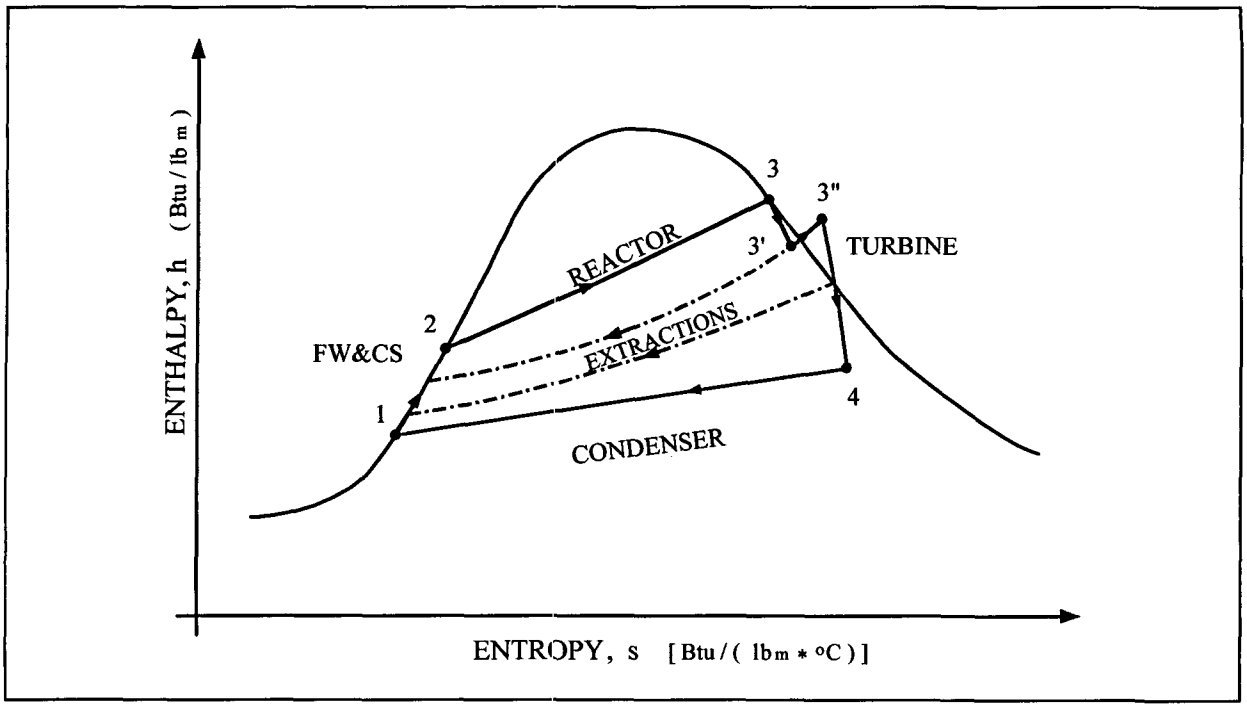

Figure 3 Clausius-Rankine Cycle

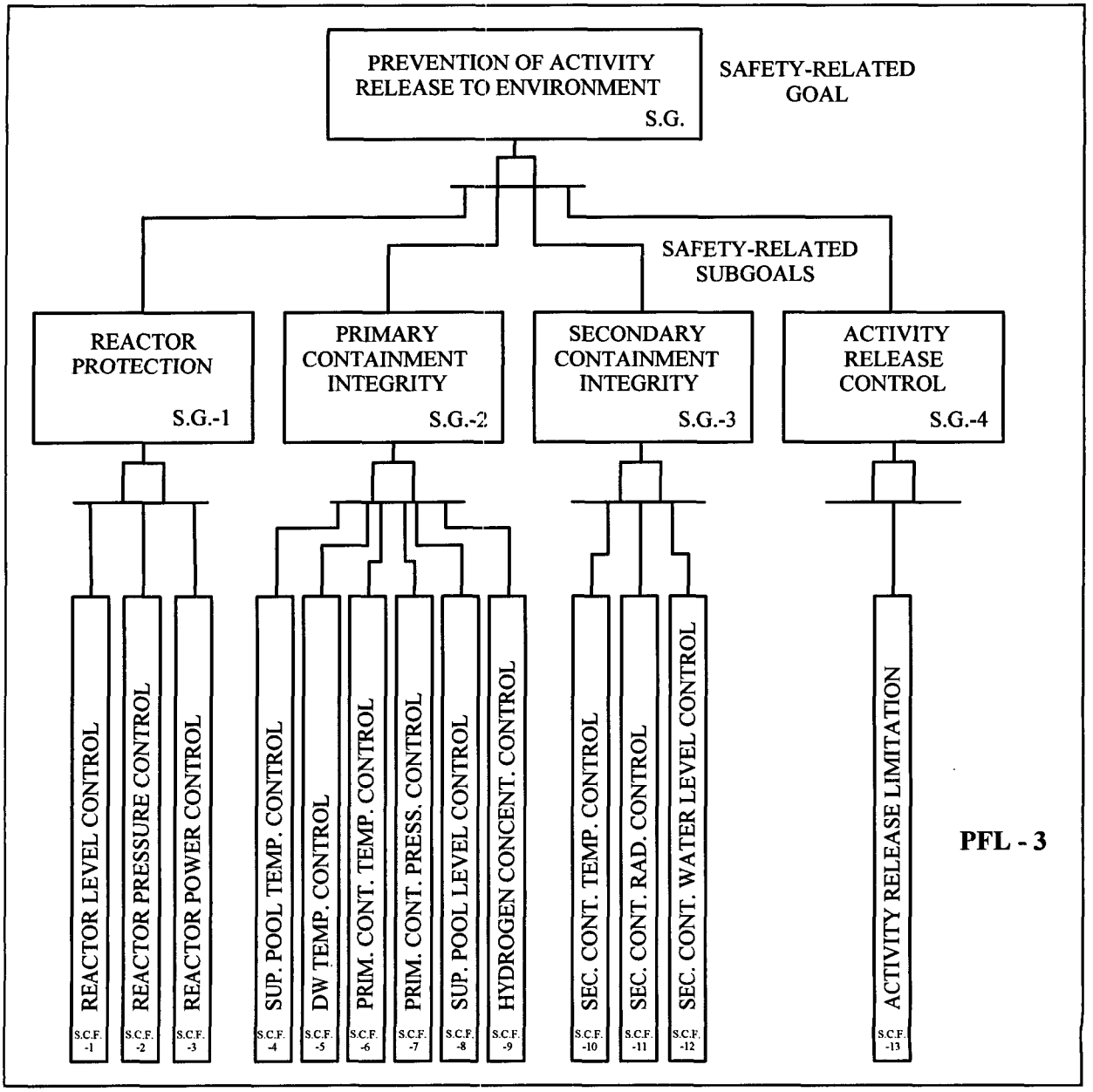

Figure 4 Block Diagram for Safety Related Critical Functions (PFL-3)

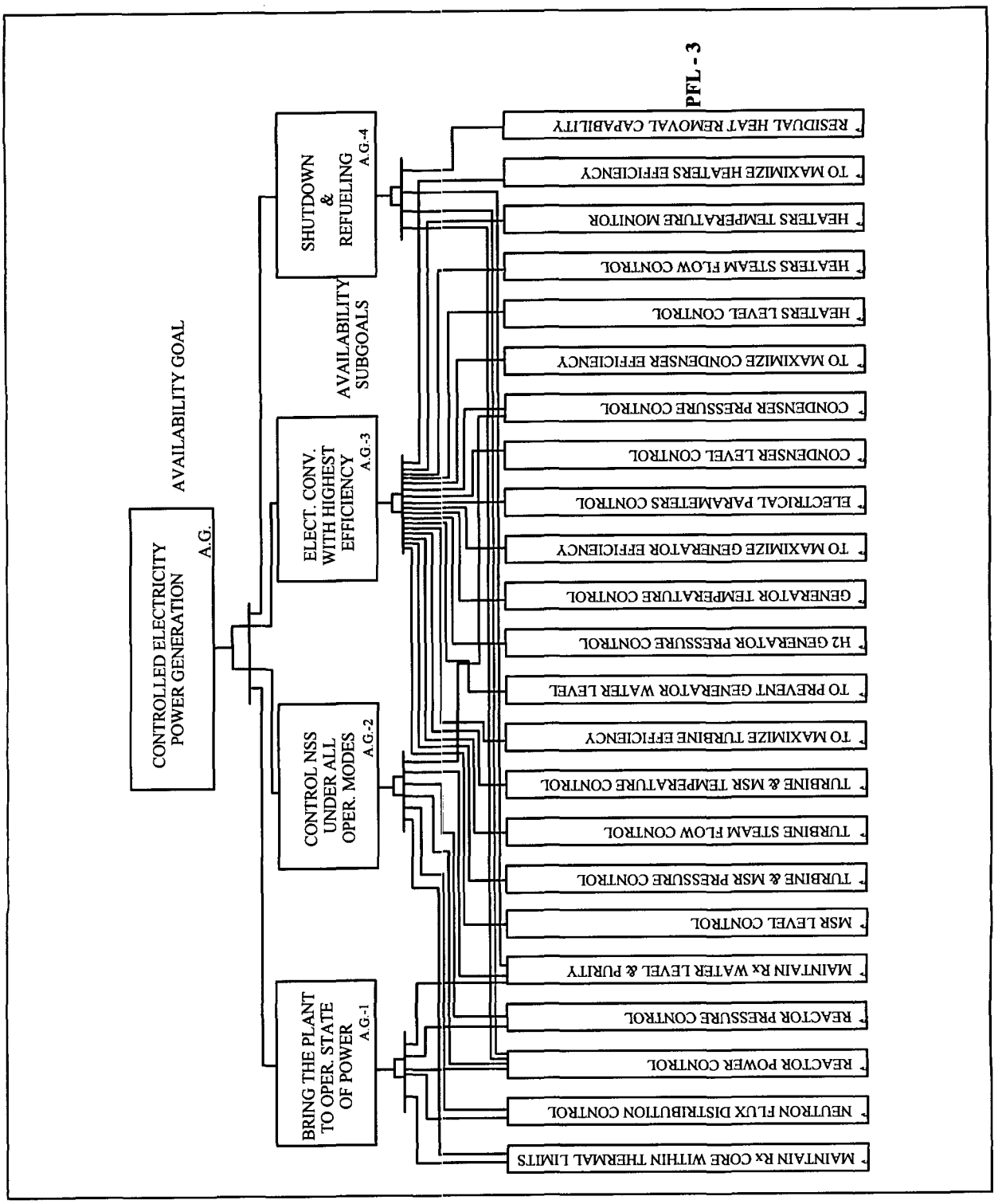

Figure 5 Block Diagram for Availability-Related Critical Functions (PFL-3)

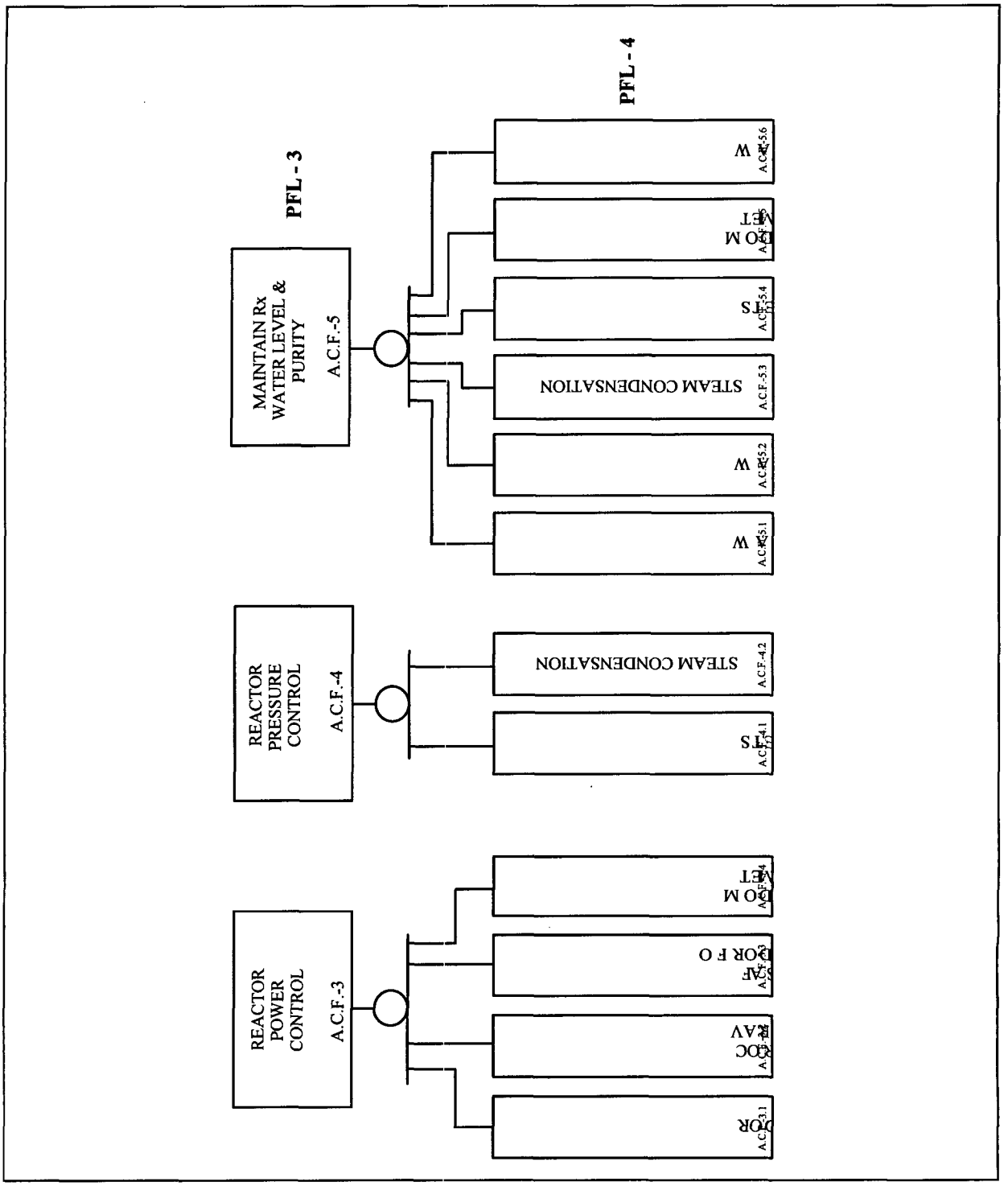

Figure 6 Block Diagrams for Some Performance Requirements (PFL-4)

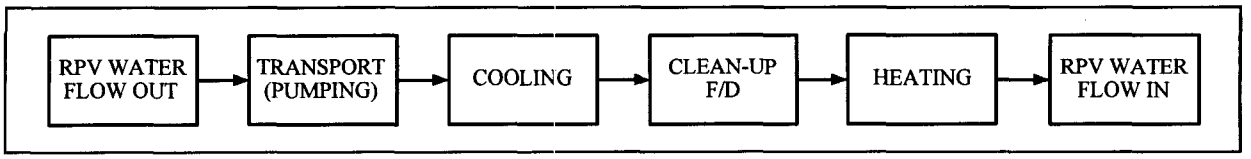

Figure 7 Block Diagram for Initial Process Selection

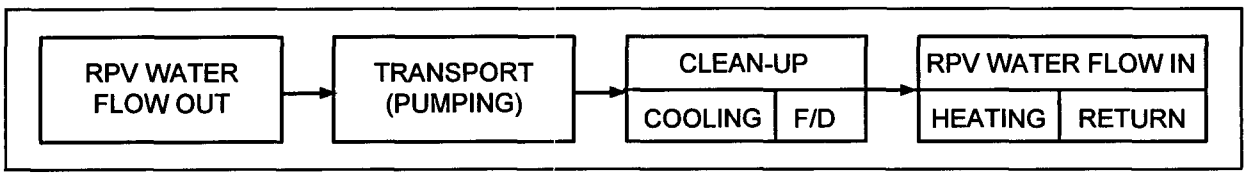

Figure 8 Process Block Diagram for the Purify RPV Water Function

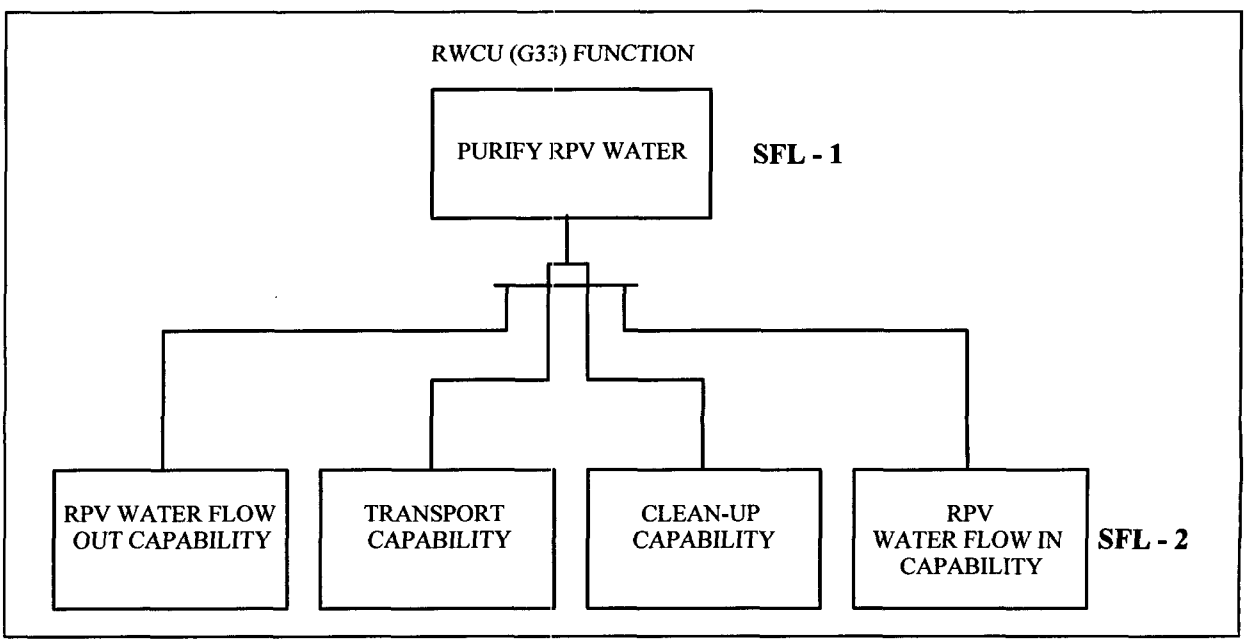

Figure 9 Block Diagram for SFL-2

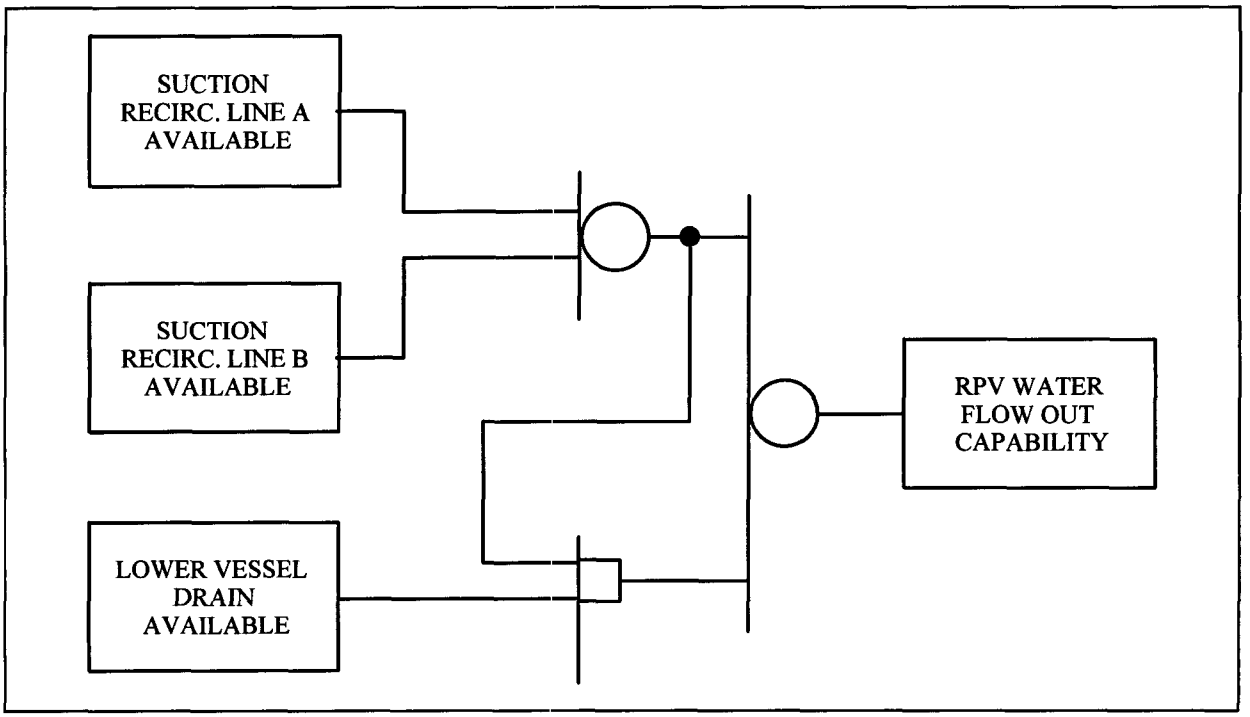

Figure 10 Block Diagram for Flow Out Process

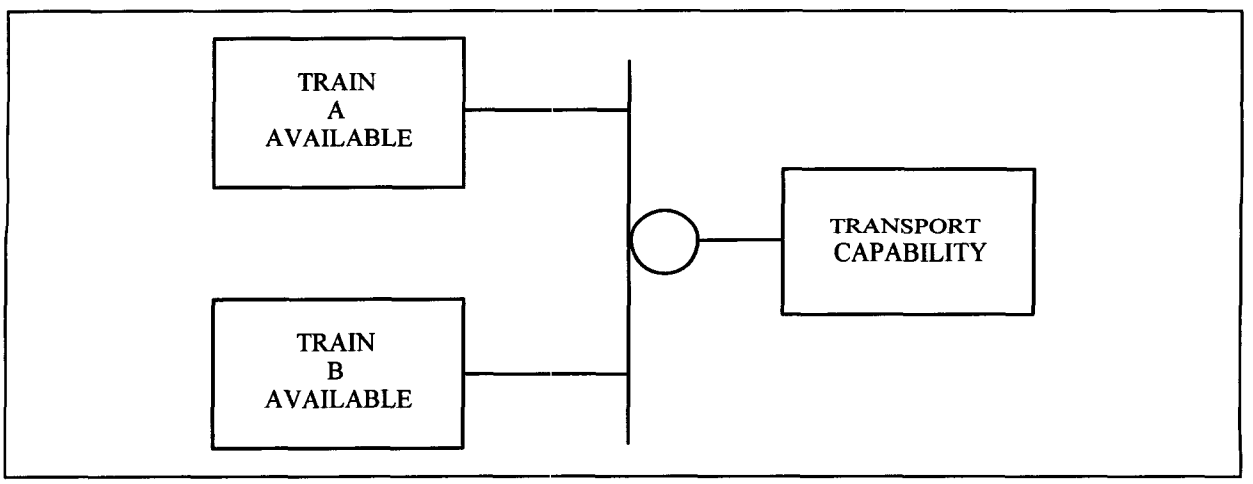

Figure 11 Block Diagram for Transport Process

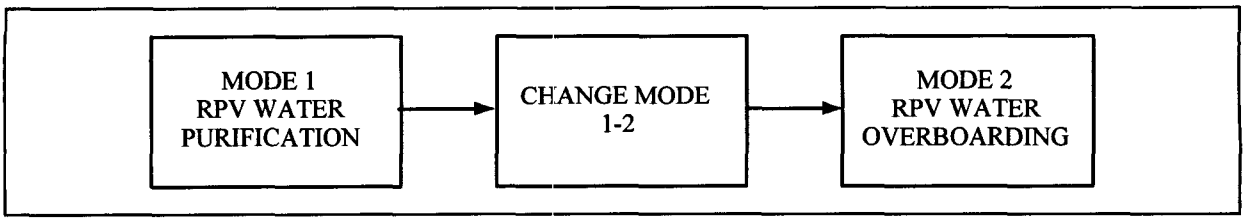

Figure 12 Change Mode Block Diagram

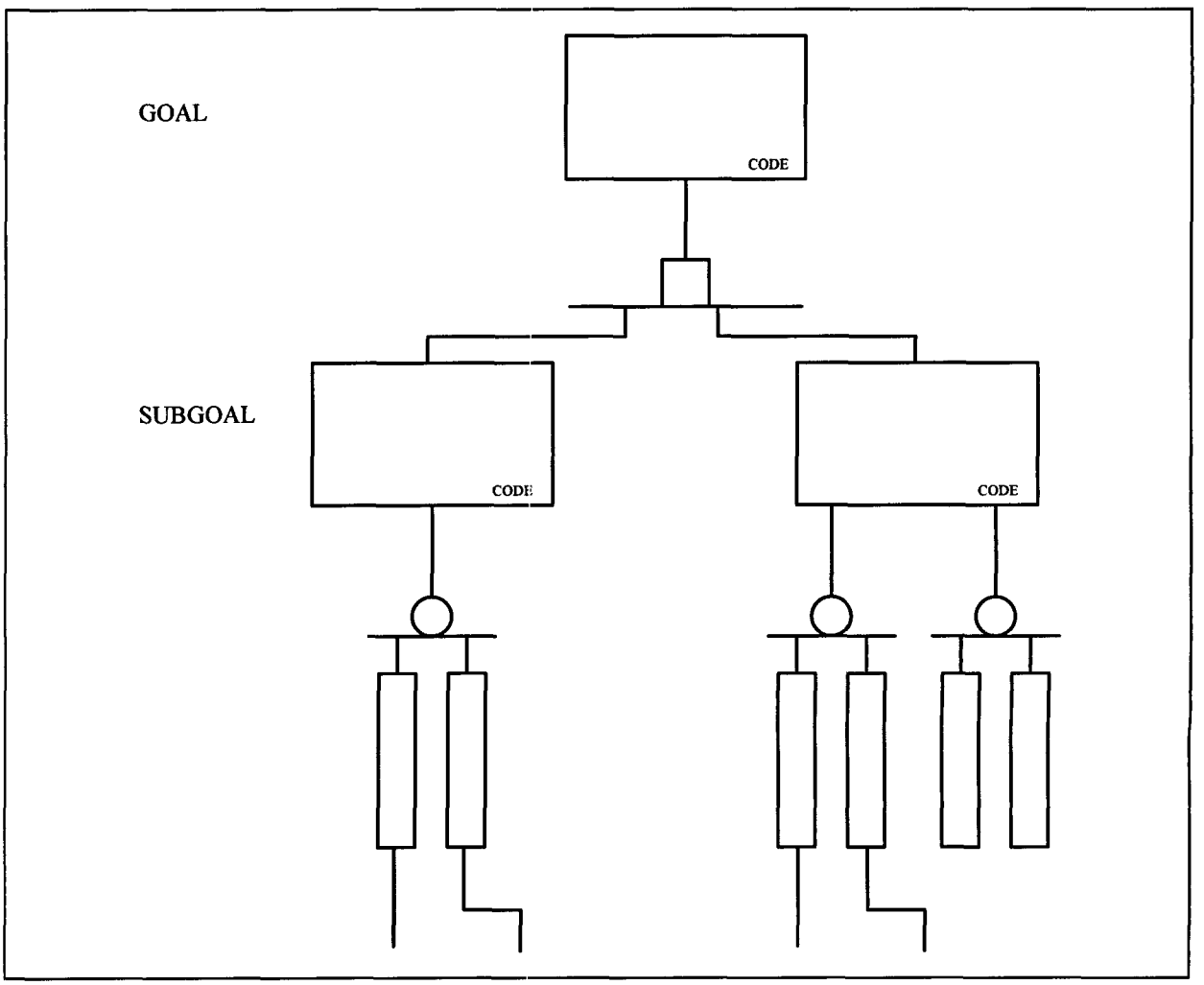

Figure 13 Typical Flowchart Structure

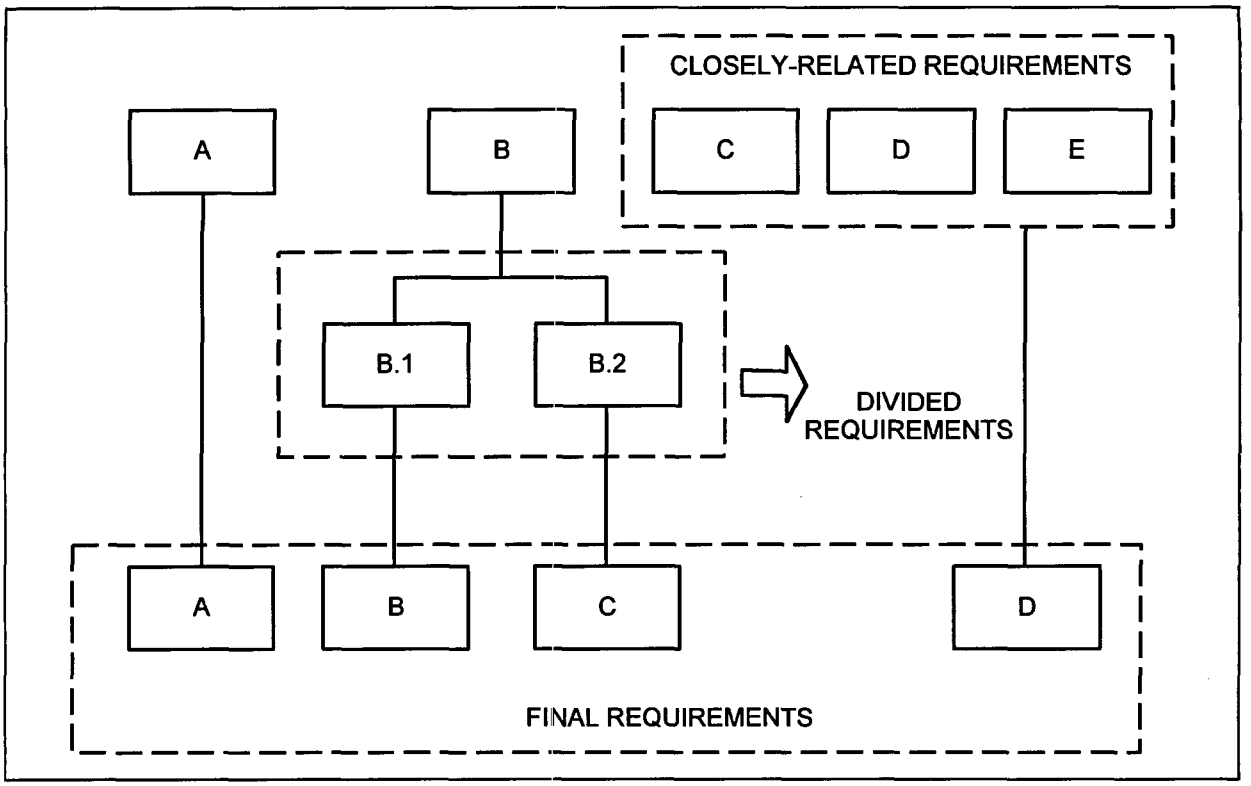

Figure 14 Block Diagram for Integration/Division of Requirements

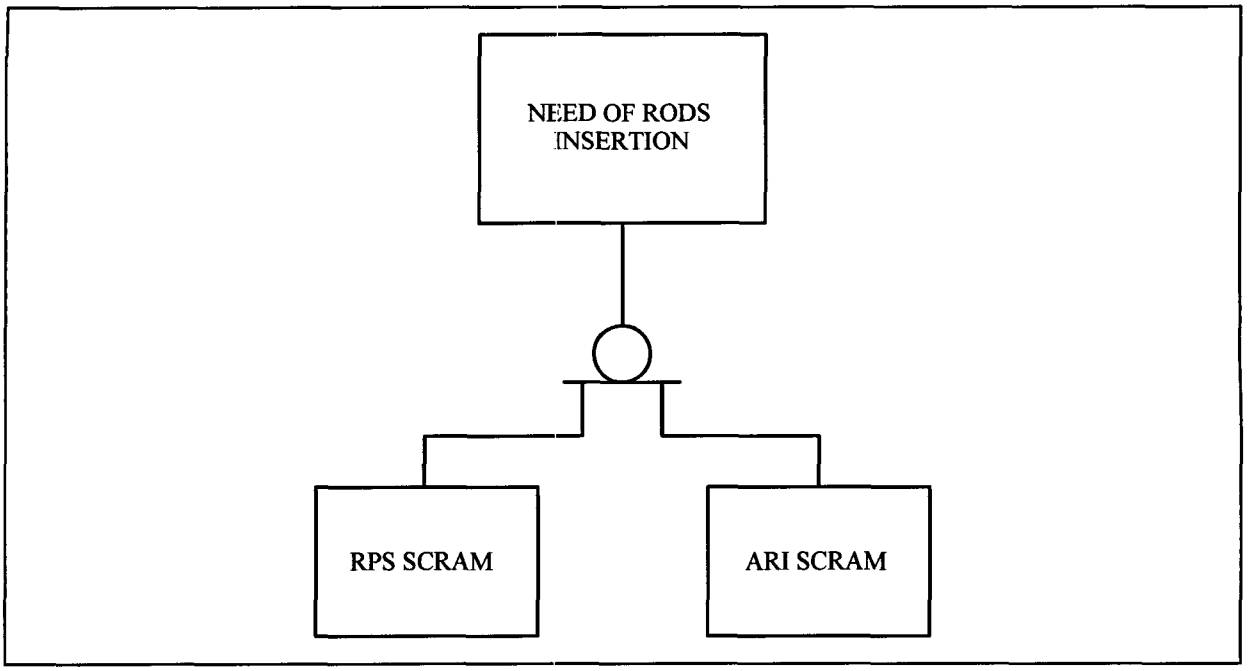

Figure 15 Pictorial Representation of Backup Requirements

System: RWCU	MPL: G33
Function: Purify RPV Water	Critical Function to safety: Yes No X
Characteristic Parameters(s): RPV water conductivity	Range: s ≤ 1 mmho/cm
Alternative Parameters(s): F/D flow & Return to RPV	Range: 28.4 m3/h & 67.2 m3/h

System Status Parameter & Limitations		
Parameter	Limits	Comments
System suction flow	67.2 m3/h	Nominal system flow
Pumps suction flow	A - 113.6 m3/h B - 113.6 m3/h	Design basis
Pumps discharge pressure	> 0.8 MPa	Design basis
Pumps discharge flow	> 7.9 MPa	Design basis
RHx tubes inlet temperature	≥ 279°C	Design basis
NRHx tubes inlet temperature	≥ 112°C	Design basis
F/D inlet temperature	≥ 55°C	Design basis
•	•	•
•	•	•
•	•	•

Figure 16 Data Collection Format for BWR-6 RWCU Purify RPV Water Function

Appendix A General Figures

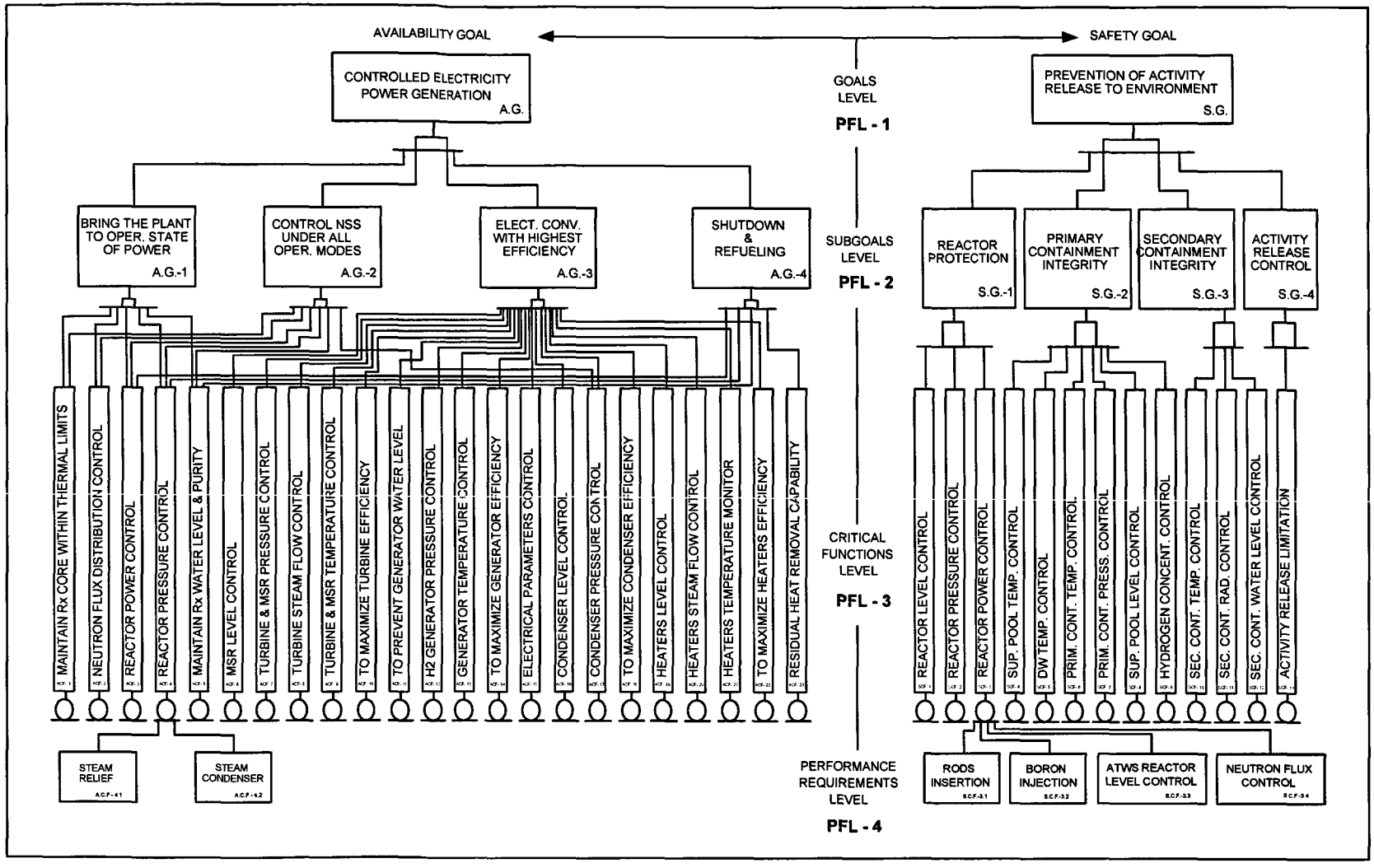

Figure A-1 HSI Functional Structure

SYSTEM	MPL	
FUNCTION:	CRITICAL FUNCTION TO SAFETY: YES ☐ NO ☐	
PROCESS:		
PROCESS ELEMENT:		
COMPONENT	STATUS	SUPPORT REQUIREMENTS

Figure A-2 Format for System Performance Requirements Identification

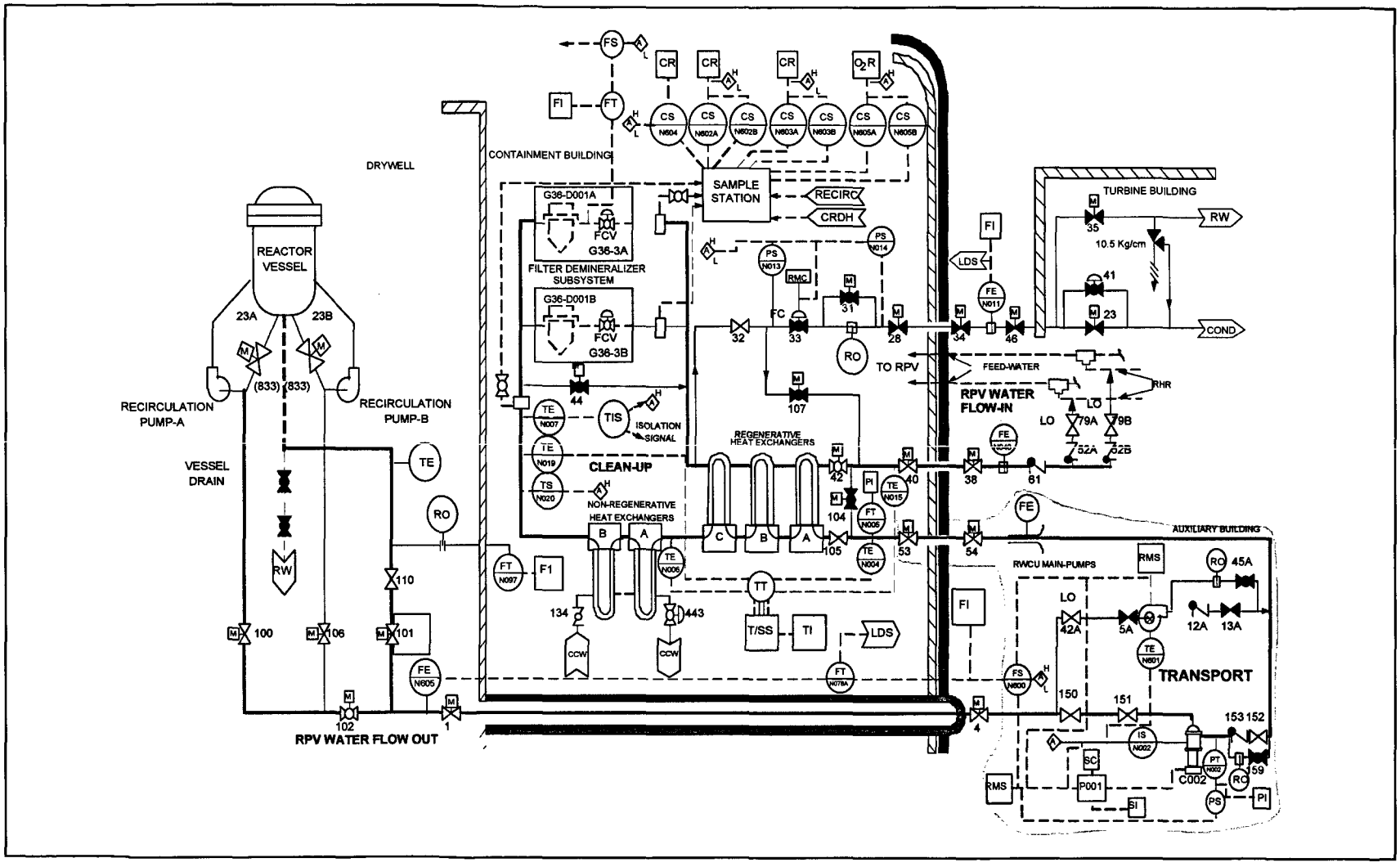

Figure A-3 BWR-6 RWCU P&ID (Simplified)

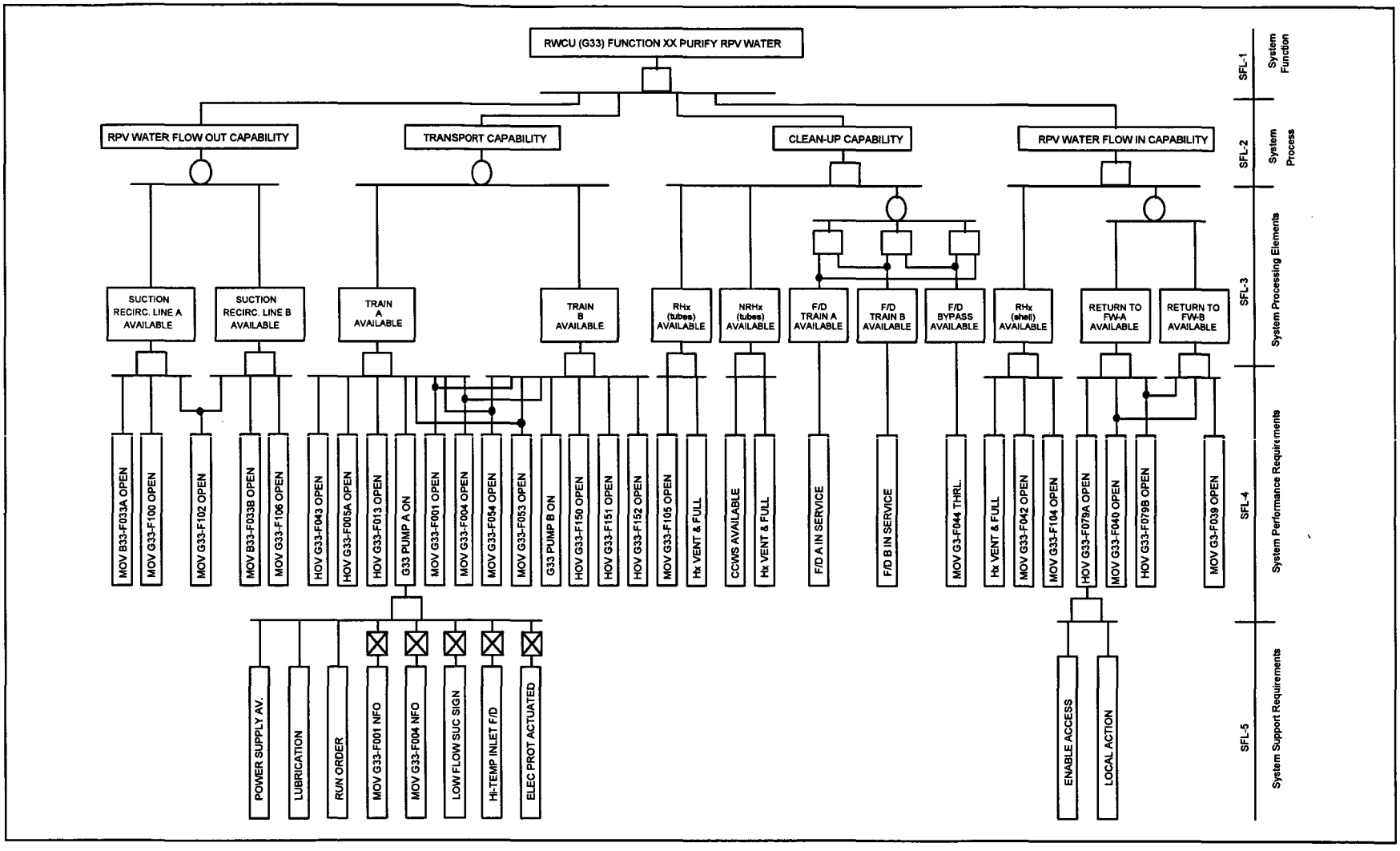

Figure A-4 Block Diagram for RWCU Functional Analysis Function: "Purity RPV Water"

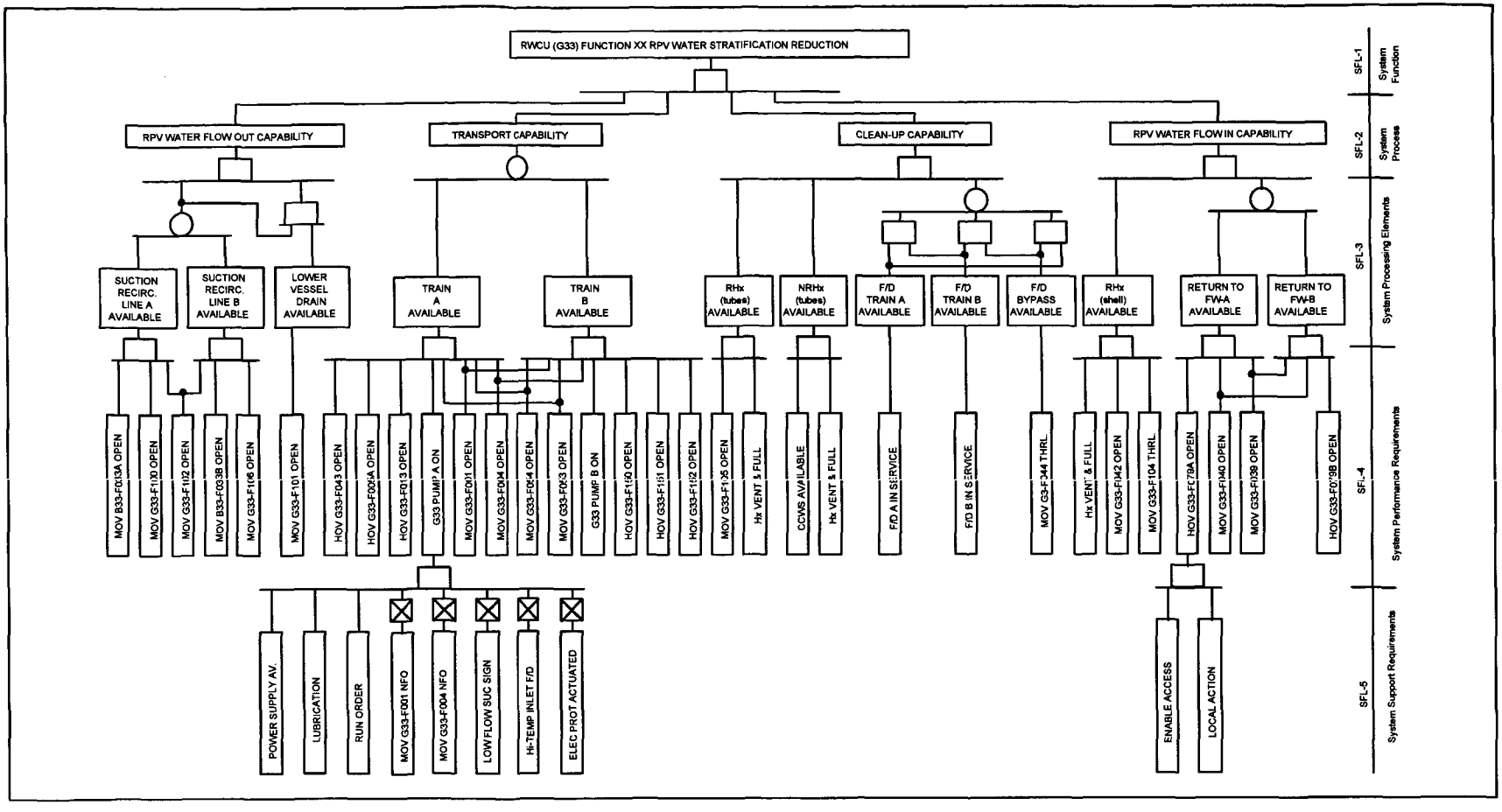

Figure A-5 Block Diagram for RWCU Functional Analysis Function: "RPV Water Stratification Reduction"

SYSTEM:	MPL	
FUNCTION:	CRITICAL FUNCTION TO SAFETY: YES ☐ NO ☐	
CHARACTERISTIC PARAMETER(S):	RANGE:	
ALERNATIVE PARAMETER(S):	RANGE:	
SYSTEM STATUS PARAMETERS & LIMITATIONS		
PARAMETERS	LIMITS	COMMENTS

Figure A-6 Data Collection Format for System Level Narrative Description