

**MFN 10-030**

**Enclosure 2**

**Licensing Topical Report NEDO-33220  
ESBWR Human Factors Engineering Allocation of  
Function Implementation Plan  
Revision 4**

**Non-Proprietary Version**



**HITACHI**

GE Hitachi Nuclear Energy

NEDO-33220

Revision 4

Class I

DRF Section 0000-0049-8915 R5

February 2010

Licensing Topical Report

**ESBWR HUMAN FACTORS ENGINEERING  
ALLOCATION OF FUNCTION IMPLEMENTATION PLAN**

*Copyright 2006, 2010 GE-Hitachi Nuclear Energy Americas LLC  
All Rights Reserved*

## **NON-PROPRIETARY INFORMATION NOTICE**

This is a non-proprietary version of NEDE-33220P, which has the proprietary information removed. Portions of the document that have been removed are indicated by an open and closed bracket as shown here [[ ]].

## **IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT**

### **Please read carefully**

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

**Table of Contents**

**1. Overview.....1**

1.1 Purpose.....2

1.2 Scope.....3

1.3 Definitions and Acronyms .....3

    1.3.1 Definitions.....3

    1.3.2 Acronyms .....6

**2. Applicable Documents.....8**

2.1 Supporting Documents and Supplemental GEH Documents .....8

    2.1.1 Supporting Documents.....8

    2.1.2 Supplemental Documents .....8

2.2 Codes and Standards .....9

2.3 Regulatory Guidelines .....9

2.4 DOD and DOE Documents.....9

2.5 Industry and Other Documents .....9

**3. Methods .....10**

3.1 The Allocation of Function .....10

    3.1.1 Background.....10

    3.1.2 Goals .....11

    3.1.3 Basis and Requirements.....12

    3.1.4 General Approach .....12

    3.1.5 Application.....14

        3.1.5.1 Design Allocation of Functions .....14

        3.1.5.2 Detailed Allocation of Functions .....14

        3.1.5.3 Economic Allocation of functions .....14

**4. Implementation .....15**

4.1 Allocation of Function Implementation.....15

    4.1.1 Assumptions.....15

    4.1.2 Inputs.....15

        4.1.2.1 Direct Inputs.....15

        4.1.2.2 Feedback Inputs .....16

    4.1.3 Process .....17

        4.1.3.1 Allocation of Function Flow Chart Process.....18

        4.1.3.2 Shared Function Detailed Flowchart Process .....21

    4.1.4 Outputs.....27

**5. Results.....28**

5.1 Results Summary Reports.....28

**Appendix A Human Capabilities and Limitations .....33**

**Appendix B Allocation of Function Criteria.....35**

**List of Tables**

Table A.1 Criteria that Limit or Preclude Human Participation in a System Function..... 33  
Table A.2 Criteria that Define Unique Human Capabilities..... 34

**List of Figures**

Figure 1 HFE Implementation Process ..... 29  
Figure 2 Allocation of Function Phases..... 30  
Figure 3 Allocation of Function Flowchart ..... 31  
Figure 4 Shared Function Detailed Flowchart..... 32

## 1. OVERVIEW

The ESBWR Man-Machine Interface System and Human Factors Engineering Implementation Plan, Reference 2.1.1(2), illustrated in Figure 1, establishes three specific activities that support operational analysis:

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

These steps determine:

- Functions required to achieve plant goals and system functions;
- Distribution of functions among human, machine, and shared control; and
- The integrated Human Actions (HAs) and machine actions required at the task level.

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

The proper distribution of activities among automation options and human operators is an essential factor in ensuring safe and reliable operation of nuclear power plants. As shown in Figure 1 the ESBWR is designed using a systematic process for integrating Human Factors Engineering (HFE) principles into the system design using focused inputs and processes. The foundation for HFE is established in the Design Control Document (DCD), Chapter 18, and is supported by other DCD chapters.

One of the early pivotal processes in the HFE design implementation is operational analysis. Operational analysis is an iterative process that describes plant, system, or component state changes as a series of tasks including supporting information requirements. This is accomplished through performance of Functional Requirements Analyses (FRA), Allocations of Functions (AOF), and Task Analyses (TA). They determine what must be done, who does it (man, machine, or shared), and how it is to be done (controls, indications, supporting information, etc.). Results of the analyses are design requirements for the Human Systems Interface (HSI), procedures, and training. This document outlines how the allocation of function portion of operational analysis is performed.

Through the allocation of functions to the most efficient implementer (human, machine or shared) human factor improvements help prevent or mitigate potential human error. Allocation of functions ensures that only those activities and functions that need active human participation are brought to the attention of operators and other plant personnel. The allocated functions are then processed through task analysis where information, controls, and feedback required to complete the tasks that accomplish the overall function are determined. This detail enables HSI designers and procedure writers to streamline tasks. This approach to reducing human error

simplifies the information reaching the operating personnel and enables control room personnel to have a clear understanding of the plant status at any time.

Allocation of function analyzes functional requirements for plant operation and assigns control functions to:

- Human (e.g., manual control or operation)
- Machine (e.g., automation, automatic control, and passive, self-controlling phenomena)
- Shared (combinations of human and machine control)

Subsequent HFE tasks refine this initial assignment by strategically utilizing human and machine capabilities. Factors considered during allocation of functions include:

- Existing practices and operational experience,
- Regulatory requirements and the ESBWR mission and supporting goals,
- Reliability of the human, machine, and shared control schemes, and
- Capital cost, operating cost, and technical feasibility.

## 1.1 PURPOSE

This plan addresses methods, processes, and criteria for verifying that the allocation of function portion of operational analysis is consistent with accepted ESBWR HFE practices and principles. The HFE team uses the allocation of function process to ensure that overall operational analysis successfully generates allocated tasks to accomplish all needed system functions. This output forms the requirements for HSI design, training, procedures, and staffing and qualifications. Through this process, applicable requirements of NUREG/CR-3331 and NUREG-0711 R2 are met. Additionally, this implementation plan guides function allocation for the ESBWR plant design in accordance with the requirements of the ESBWR Man Machine Interface System (MMIS) and HFE Implementation Plan, Reference 2.1.1(2).

The AOF Plan establishes methods to:

- Conduct the AOF consistent with accepted HFE methods
- Promote the ESBWR mission, goals, and philosophy
- Allocate functions between human, machine, and shared control
- Coordinate human and machine tasks for shared functions during normal, abnormal, and emergency operation
- Coordinate human and machine tasks for shared surveillance functions
- Coordinate human and machine tasks for shared maintenance functions
- Provide analysis method to assess the impact of design, staffing, training, procedure, and HSI changes on the ability of operators to monitor and coordinate activities

## 1.2 SCOPE

This document establishes an allocation of function process that conforms to the ESBWR MMIS HFE design plan and applicable regulatory requirements. Every system-level and plant-level function from the FRA that requires monitoring or control is analyzed and allocated to human, machine, or shared ownership by the AOF process. AOF places emphasis on Human Actions (HAs) that have been found to affect plant risk by means of Human Reliability Analysis (HRA)/Probabilistic Risk Assessment (PRA). The probability of successful completion of these tasks is increased by proper allocation of supporting functions such as machine backup, machine limits on human actions, and supporting automations.

This plan establishes the following scope elements for the analysis:

- Objectives, performance requirements, and constraints.
- Methods and criteria for conducting the AOF in accordance with accepted human factors principles and practices.
- System and function requirements that define function allocation restraints.
- The results of the HRA/PRA, OER/BRR, and deterministic evaluations.
- Each function identified in the FRA that requires monitoring or control is allocated.
- AOF outputs are sets of logical, coherent, and meaningful tasks.
- The full range of plant conditions, including startup, low-power, normal operations, shutdown, abnormal, transient, and emergency operations.

## 1.3 DEFINITIONS AND ACRONYMS

### 1.3.1 Definitions

Several terms referred to in this plan are defined to provide a common basis for communications between this and other plans.

**Abnormal Operating Procedures (AOPs):** Procedures that specify steps that operators take to restore an operating variable to its normal controlled value when it departs from its normal range or to restore normal operating conditions following a transient.

**Emergency Operating Procedures (EOPs):** Emergency condition procedures that direct actions necessary for the operators to mitigate the consequences of transients and accidents that cause plant parameters to exceed the predetermined symptom based thresholds developed in either the Emergency Procedure Guidelines or related Plant Specific Technical Guidelines.

**Expert Judgment (as it relates to HFE):** Decisions made that typically require multivariate judgments based on complex evaluations of probable utility versus probable risk. [Adapted from NUREG/CR-3331]

**Feedback:** System or component response (e.g., visual or aural) that indicates the extent to which the user's desired effect was accomplished. Feedback can be either intrinsic or extrinsic. Intrinsic feedback is that which the individual senses directly from the operation of the control devices (e.g., clicks, resistance, control displacement). Extrinsic feedback is that which is sensed

from an external source that indicates the consequences of the control action (e.g., indicator lights, display changes, aural tones).

**Filtering:** An alarm display processing technique which may eliminate alarm messages that are irrelevant, less important, or otherwise unnecessary. These alarm messages are not available to the operators. (This is in contrast to suppression, which does not make the alarm messages immediately available but does allow the operator to retrieve them.)

**Full-Scope Simulator:** A high-fidelity simulation environment that includes the physical, environmental, and controls and displays for the environment to be simulated. This typically refers to the main control room simulator and meets the requirements of Regulatory Guide 1.149 and ANS-3.5.

**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 requirements analysis:** The examination of system goals to determine what functions are needed to achieve them.

**HFE Design Team:** The HFE design team (design team) is a team of engineers, as defined in Reference 2.1.1(2), Man-Machine Interface System And Human Factors Engineering Implementation Plan, responsible for the design of the HSI systems.

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

**Human Factors Engineering (HFE):** The application of knowledge about human capabilities and limitations to plant, system, and equipment design. HFE ensures that the plant, system, or equipment design, human tasks, and work environment are compatible with the sensory, perceptual, cognitive, and physical attributes of the personnel who operate, maintain, and support the system.

**Human Reliability Analysis (HRA):** A structured approach used to identify potential human failure events and to systematically estimate the probability of those errors using data, models, or expert judgment. [ASME PRA Std]

**Human System Interface (HSI):** HSI encompasses all instrumentation and control systems provided as part of the ESBWR for use in performing the monitoring, controlling, alarming, and protection functions associated with all modes of normal plant operation (that is, startup, shutdown, standby, power operation, and refueling) as well as off-normal, emergency, and accident conditions. Specifically, the HSI is the organization of inputs and outputs used by personnel to interact with the plant, including the using of alarms, displays, controls, and job performance aids.

**Local control station (LCS):** An operator interface related to process control that is not located in the main control room. This includes multifunction panels, as well as single-function LCSs, such as controls (e.g., valves, switches, and breakers) and displays (e.g., meters) that are operated or consulted during normal, abnormal, or emergency operations.

**Main Control Room (MCR):** Room that provides the location from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents.

**Normal Operating Procedures:** Plant operating procedures that provide instructions for energizing, filling, venting, draining, starting up, shutting down, changing modes of operation, preparing for maintenance or modification, performing maintenance, returning to service following maintenance and testing (if not contained in the applicable testing procedure), and other instructions appropriate for operation.

**Operational Analysis:** An iterative process that describes plant, system, and component state changes as a series of tasks including supporting information requirements. This is accomplished through performance of system functional requirements analyses, allocation of functions, and task analyses. The analysis process determines what must be done, who does it (man, machine, or shared), and how it is to be done (for example, controls, indications, supporting information). Results of the analyses are design requirements for the HSI, procedures, and training.

**Risk-Important Human Actions:** Actions that are performed by plant personnel to provide assurance of plant safety. Actions may be made up of one or more tasks. There are both absolute and relative criteria for defining risk-important actions.

From an absolute standpoint, a risk-important action is any action whose successful performance is needed to provide reasonable assurance that predefined risk criteria are met. From a relative standpoint, the risk-important actions may be defined as those with the greatest risk in comparison to all human actions. The identification can be done quantitatively from risk analysis and qualitatively from various criteria such as task performance concerns based on the consideration of performance shaping factors.

**Risk Significant Local Control Station:** A local control station at which risk-important human actions are performed or which controls safety-related equipment.

**Safety-related:** A term applied to those plant systems, structures, and components (SSCs) that prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public (see Appendix B to Part 50 of Title 10 of the U.S. Code of Federal Regulations). These are the SSCs on which the design-basis analyses of the safety analysis report are performed. They also must be part of a full quality assurance program.

**Task Analysis (TA):** A method for describing what plant personnel must do to achieve the purposes or goal of their tasks. The description is in terms of cognitive activities, actions, and supporting equipment.

**Validation:** The process of evaluating a system or component (including software and human interactions) during or at the end of the development process to determine whether it satisfies specified requirements.

**Verification:** The process of evaluating a system or component (including software and human interactions) to determine whether the products of a given development process satisfy the requirements imposed at the start of that process.

**Verification and Validation (V&V):** The process of determining whether the requirements for a system or component (including software and human interactions) are complete and correct.

The products of each development process fulfill the requirements or conditions imposed by the previous process, and the final system or component (including software) complies with specified requirements.

### 1.3.2 Acronyms

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

<b>Acronym</b>	<b>Description/Name</b>
AOF	Allocation of Function
ASME	American Society of Mechanical Engineers
BRR	Baseline Review Record
COL	Combined Operating License
D3	Defense-in-Depth and Diversity
DCD	Design Control Document
FRA	Functional Requirements Analysis
HA	Human Action
HFE	Human Factors Engineering
HFEITS	Human Factors Engineering Issue Tracking System
HPM	Human Performance Monitoring
HRA	Human Reliability Assessment
HSI	Human System Interface
IOP	Integrated Operating Procedure
LCS	Local Control Station
MCR	Main Control Room
MMIS	Man Machine Interface System
NRC	Nuclear Regulatory Commission
OER	Operating Experience Review
PAS	Plant Automation System
PFRA	Plant-level Functional Requirements Analysis
PRA	Probabilistic Risk Assessment
RSR	Results Summary Report
S&Q	Staffing and Qualifications
SDS	System Design Specifications
SFGA	System Function Gap Analysis
SFRA	System Functional Requirements Analysis

SSC	System, Structure, and Component
TA	Task Analysis
V&V	Verification and Validation

## 2. Applicable Documents

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

### 2.1 SUPPORTING DOCUMENTS AND SUPPLEMENTAL GEH DOCUMENTS

#### 2.1.1 Supporting Documents

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

- (1) ESBWR DCD, Tier 2, Chapter 18 (GEH 26A6642BX).
- (2) NEDE-33217P and NEDO-33217, ESBWR Man-Machine Interface System and Human Factors Engineering Implementation Plan.
- (3) NEDO-33201, ESBWR Probabilistic Risk Assessment.

#### 2.1.2 Supplemental Documents

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

- (1) NEDO-33219, ESBWR HFE Functional Requirements Analysis Implementation Plan.
- (2) NEDE-33221P and NEDO-33221, ESBWR HFE Task Analysis Implementation Plan.
- (3) NEDE-33226P and NEDO-33226, ESBWR – Software Management Program Manual.
- (4) NEDO-33251, ESBWR I&C Diversity and Defense-in-Depth Report.
- (5) NEDO-33262, ESBWR HFE Operating Experience Review Implementation Plan.
- (6) NEDO-33266, ESBWR HFE Staffing and Qualifications Implementation Plan.
- (7) NEDO-33267, ESBWR HFE Human Reliability Analysis Implementation Plan.
- (8) NEDE-33268P and NEDO-33268, ESBWR HFE Human System Interface Design Implementation Plan.
- (9) NEDO-33274, ESBWR HFE Procedures Development Implementation Plan.
- (10) NEDO-33275, ESBWR HFE Training Development Implementation Plan.
- (11) NEDE-33276P and NEDO-33276, ESBWR HFE Verification & Validation Implementation Plan.
- (12) NEDO-33277, ESBWR HFE Human Performance Monitoring Implementation Plan.

## **2.2 CODES AND STANDARDS**

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

- (1) IEEE Std 1023-2004, 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.

## **2.3 REGULATORY GUIDELINES**

- (1) NUREG/CR-3331, A Methodology for Allocating Nuclear Power Plant Control Functions to Human or Automatic Control, 1983.
- (2) NUREG/CR-2623, The Allocation of Functions in Man-Machine Systems: A Perspective and Literature Review, 1982.
- (3) NUREG-0711, Rev. 2, Human Factors Engineering Program Review Model, 2004.
- (4) NUREG-0800, Rev. 1, Standard Review Plan, Chapter 18 – Human Factors Engineering, 2004.

## **2.4 DOD AND DOE DOCUMENTS**

None.

## **2.5 INDUSTRY AND OTHER DOCUMENTS**

None.

### 3. METHODS

#### 3.1 THE ALLOCATION OF FUNCTION

##### 3.1.1 Background

The allocation of functions to humans and machines takes place as a part of the top-down HFE design process. The HFE team utilizes the System Design Specifications (SDS) and the output of functional requirements analysis to allocate those functions required by regulatory or system requirements. The AOF is performed in accordance with the ESBWR MMIS and HFE Design Implementation Plan.

The design allocation of function, shown in Figure 2, processes tasks at the plant and system level that support all aspects of normal operating modes. The detailed allocation of functions processes tasks that support all aspects of abnormal and emergency operations. The economic allocation of functions processes tasks that support all aspects of plant maintenance, calibration, inspection, and testing.

The AOF process is based on a number of underlying ergonomics principles as follows:

- (1) Human cognitive strengths are fully utilized by the designer. There are some things that humans do better than machines. The three disciplines of engineering, ergonomics, and psychology must work in harmony to utilize these strengths. Humans can successfully perform very complex tasks or processes that are difficult and costly to automate.
- (2) Automation starts with the most prescriptive procedural functions first. Those manual functions that are memorized or performed prescriptively by detailed procedures are automated whenever possible. This reduces the burden on operators when performing many routine control loop actions and shifts the human function to monitoring.
- (3) Automation is used to reduce human cognitive overload. Humans can suffer from information overload and consequent mental overload. This can occur from high information rates, multiple tasks competing for operator attention, or task complexity. An example is trying to manually control xenon oscillations and power level in a large reactor core at the same time. Whenever the designer can predict this problem, or whenever operating experience demonstrates this, automation is used to relieve the human of the function that causes the problem.

Tasks that have been assigned to automation should not be returned to a human when the automation fails. In general, humans do not act effectively as a back up for a machine, when the timing for a recovery action involving multiple control function actions is very short. For example, if automated systems for turbine speed control are lost, it is unlikely that the operator could control the power production for very long without a generator trip. Thus, this control circuit is a better choice for automation with no expectation of human backup.

- (4) Automation is used when system requirements exceed the capacity for human control. An example of this is that processors can evaluate multiple inputs simultaneously, make a comparison, and initiate a function. Consequently, human back up for the same control function is unlikely to be appropriate. In this case, human actions address a backup plan

such as power reduction or plant trip to achieve protection from safety barriers in a new defense-in-depth configuration, which is within human response capability.

- (5) Automation is considered for actions that occur infrequently if human performance of the task diminishes over time based on the level of planned training or actual experiences.
- (6) During a system failure automated systems are designed to clearly indicate the system status and minimize the need for operator intervention. This can be accomplished by achieving required functions by redundant or diverse active systems or passive systems. Operators can perform some simple valve alignments if sufficient cues, procedures, and time are available.
- (7) Automation and feedback information is used to protect the general public from the fallibility and variability of humans. This requires an analysis of the control function requirements for proposed human tasks to identify possible errors, the HSI cues for making corrections, and the consequences of an uncorrected error.
- (8) Particular attention is paid to risk-important functions. The tasks are automated if it is practical, feasible, and cost-effective.
- (9) The correct process for balancing human and machine actions is an institutionalized part of system design. The right balance does not emerge until there are common processes in use by designers, operators, and management, which reflect the correct principles and embody proven practices.
- (10) The evaluations include consideration of the professional motivation and psychological well being of the operator.
- (11) Ultimate control remains with humans, in that the human can set objectives for starting or stopping a process. In the ESBWR design, the control room operator maintains control.
- (12) Override capability is given to humans to correct automatic control if necessary. The ESBWR design allows the main control room operator to intervene in the automatic process.
- (13) Information is provided to humans concerning the actions of automatic controls and their objectives. Using break-point logic, the ESBWR operator monitors and controls automated processes, allowing them to continue at predefined steps.
- (14) Control logic of machines is designed for the intended manual operating strategies and associated manual control actions.
- (15) The information system presentation to the operator, such as computer generated displays and controls, are behaviorally suitable.
- (16) Adequate cognitive support is available to the operator, so that the operator has an adequate mental model when assuming control.

### **3.1.2 Goals**

The process begins with the ESBWR mission and analyzes plant functions for all operating modes to determine functions that must be completed to meet the plant goals. The following goals are met while taking advantage of human strengths and avoiding human weaknesses:

- Limit Radionuclide Release
- Operate Economically and Protect Economic Operations

Additional goals of the AOF process include:

- Minimize active errors
- Limit the impact of latent errors
- Limit the impact of active errors
- Coordinate and implement plans in accordance with NRC guidelines
- Perform analysis of normal, abnormal, and emergency functions
- Execute the HFE plans iteratively from the early design phase through turnover to the fleet-wide owner's group and COL applicants
- Follow accepted HFE and I&C practices and processes
- Meet the commitments of ESBWR DCD, Chapter 18

### **3.1.3 Basis and Requirements**

The AOF approach follows applicable guidance in NUREG-0800 Section 18, NUREG-0711 Section 4 and NUREG/CR-3331. Categories of allocated functions are in accordance with NUREG-0711 and a breakdown of the shared function category is shown in Figure 4. The AOF process is based upon a top-down iterative process as shown in Figures 2, 3, and 4 and is an integral part of the overall HFE design process, as shown in Figure 1.

### **3.1.4 General Approach**

Operational analysis is designed as a multi-step process, as illustrated in Figure 2. Subsequent iterations contain more detailed information about the system and further establish the roles of various personnel. The functional requirements analysis generates the following system level outputs:

- Plant goals
- Plant states
- Plant processes
- Procedure process outline for Emergency Procedure Guidelines, Integrated Operating Procedures, and Emergency Action Levels
- Plant process and function redundancies
- Critical safety functions
- Plant functions and sub-functions
- Inventory of critical safety parameters
- Requirements for HSI design
- Outlines for simulator scenarios

- System Operating Modes
- System Change Modes
- Component Lineups
- Component Operational Requirements (i.e. components required to be remotely operated)
- Component control requirements (i.e. automatic, manual, etc.)
- Component manipulations required to change modes, as defined for normal and abnormal system operating procedure development
- Functional logic diagrams

Each of these sets of functions are processed and presented by FRA as sequenced data structures. These data structures provide inventories of required parameters, indications and controls, and outline sequences to be processed by AOF. The general approach to AOF is shown in Figure 2, with specific actions required to implement this approach shown in Figures 3 and 4. Tables A1 and A2 in Appendix A provide additional insight into human capabilities and limitations to assist analysts in making allocation decisions. The function outline sequences are evaluated using the AOF process. Each function or sub-function in the sequence is evaluated and allocated to one of the following resources for execution:

- **Human Only** – the function is executed entirely by plant personnel. The HSI is used to carry out the actions and monitoring performed by humans. The machine has no direct control, backup, or limiting actions associated with the function(s) being allocated.
- **Machine Only** - the function is executed entirely by plant automation. Humans have no direct control, backup, or limiting actions associated with the function(s) being allocated.
- **Shared** – the function is executed using a combination of both human and machine resources. Figure 4 outlines the various combinations of human/machine sharing that can be allocated. Most functions are allocated as shared.

The allocated function data structures produced by AOF are provided as inputs to the task analysis process. Task analysis processes the allocated functions with respect to:

- (1) The detailed task sequences and associated logic determined by FRA to meet the goals and requirements; and
- (2) The resource to which the function was allocated in AOF.

The resulting task sequences provide IOP outlines and PAS logic used by HSI design, procedures, training, and S&Q. Procedures and machine logic generated by a common data structure minimize potential errors when transferring control from manual to automatic, as well as when human action is required.

The V&V, HSI design, procedures, S&Q, training, and HPM processes provide feedback that is evaluated to determine whether or not additional iterations of the operational analysis process are warranted in specific areas. When feedback is received, the HFE design team evaluates potential resolutions including changes to operational analysis determinations, HSI design, plant design, training, procedures, etc. If a solution is not identified through this normal feedback loop, the issue is entered into HFEITS for tracking and resolution. Once all issues are resolved and the

appropriate changes are made, the HPM process monitors performance over time. Future enhancements are identified as they become apparent.

### **3.1.5 Application**

When the allocation of function plan is implemented in the method shown in Figures 2, 3, and 4, the goals of the plan are fulfilled. Allocations are made using criterion that seeks to take advantage of human strengths and avoid human weaknesses [NUREG-0711, Rev 2]. Additionally, AOF is performed in a manner that seeks to eliminate human error and minimize the impact of latent and active errors should they occur. All FRA data structures will be allocated to the implementing resource that is best suited to meet AOF goals. Functions and sub-functions will be allocated to human, machine, or shared ownership for implementation.

#### **3.1.5.1 *Design Allocation of Functions***

The design allocation of functions, shown in Figure 2, processes tasks at the plant and system level that support aspects of all normal operating modes. Using the HRA/PRA, OER/BRR, D3 Plan, and DCD, normal operating inputs are processed and presented by FRA as sequenced data structures. These data structures provide inventories of required parameters, indications and controls, and outline sequences for normal operations to be processed by AOF. These normal operating function outline sequences are evaluated using the AOF process. Each function or sub-function in the sequence is evaluated and allocated to the most appropriate resource for execution.

#### **3.1.5.2 *Detailed Allocation of Functions***

The detailed allocation of functions processes tasks that support all aspects of abnormal and emergency operations. Using the HRA/PRA, OER/BRR, D3 Plan, and DCD, abnormal/emergency operating inputs are processed and presented by FRA as sequenced data structures. These data structures provide inventories of required parameters, indications and controls, and outline sequences for abnormal/emergency operations to be processed by AOF. These abnormal/emergency operating function outline sequences are evaluated using the AOF process. Each function or sub-function in the sequence is evaluated and allocated to the most appropriate resource for execution.

#### **3.1.5.3 *Economic Allocation of functions***

The economic allocation of functions processes tasks that support all aspects of plant maintenance, calibration, inspection, and testing. Using the HRA/PRA, OER/BRR, D3 Plan, and DCD, maintenance, calibration, inspection, and testing inputs are processed and presented by FRA as sequenced data structures. These data structures provide inventories of required parameters, indications and controls, and outline sequences for maintenance, calibration, inspection, and testing to be processed by AOF. These maintenance, calibration, inspection, and testing function outline sequences are evaluated using the AOF process. Each function or sub-function in the sequence is evaluated and allocated to the most appropriate resource for execution.

## 4. Implementation

### 4.1 ALLOCATION OF FUNCTION IMPLEMENTATION

The HFE design team applies the allocation of function criteria and logic presented in this plan to the data structures generated in the FRA process. The data structures, now allocated to the appropriate human and/or system resources, are processed through task analysis where the actions required to accomplish functions are broken down into task sequences. These task sequences establish requirements for HSI design, controls, displays, automations, procedures, training, and staffing and qualifications.

#### 4.1.1 Assumptions

This plan assumes:

- ESBWRs are operated as a standardized fleet of nuclear plants.
- The ESBWR mission is safe economical power generation.
- All plants in the ESBWR fleet use the same HFE processes, as defined in DCD, Tier 2, Chapter 18.
- All normal plant controls, indications, and procedures use the same names and numbering of plant equipment.
- All ESBWR plants meet the standards developed.
- The ESBWR is designed to operate with many passive systems.
- The control systems for the ESBWR have a high level of automation. All systems are automated unless regulation or HFE analysis results dictate otherwise.

#### 4.1.2 Inputs

AOF is the second step in the iterative operational analysis process and takes process input only from FRA. Inputs into the overall operational analysis process are summarized below in order to establish understanding of the basis for FRA output.

##### 4.1.2.1 *Direct Inputs*

Direct inputs to the overall operational analysis process include the following:

- **Regulatory Requirements** - Regulations set many of the minimum standards for the HFE process and guide the analysis of ESBWR control functions and tasks.
- **HRA/PRA** - Provide analysis results used to coordinate the roles of individuals to reduce the likelihood and/or consequences of human error associated with risk-important HAS needed to manage accident sequences, and the use of advanced technology in the ESBWR.
- **OER/BRR** - Provide lessons learned from pertinent events and deficiencies noted in previous plant designs and problems with their operation. This information is gathered and maintained in the OER/BRR database for generating lessons learned involving HFE issues. It is used to enhance operational analysis by applying lessons learned from past

experience. The OER should also be used to identify modifications to function allocations, if necessary. If issues are identified, then an analysis should be performed to:

- Justify the original analysis of the function
- Justify the original man-machine allocation
- Identify changes to processes such as training or procedures that will address the OER issue. [NUREG-0711, Rev 2]
- **Defense-in-Depth and Diversity** – Provides the basis for ensuring that the distributed control and information system is sufficiently fault tolerant, redundant, and diverse to meet probabilistic safety-related goals.
- **Design Control Document** – Provides the overall plant design and system information that, coupled with system design specifications, form the basis for plant-level goals, system functions, interdependencies, and redundancies.

#### 4.1.2.2 *Feedback Inputs*

Feedback inputs to the overall operational analysis process include:

- Issues or enhancement opportunities relating to the allocation of functions identified during:
  - Training development or implementation
  - Procedure development or use
  - Staffing and Qualification evaluation process or implementation
  - HSI design, testing, or use
  - Task analysis workload assessment
- Verification and Validation - V&V enhancements are a feedback input into the AOF process. The revised results are then put through the V&V process again to validate the adequacy of the changes.
- Human Performance Monitoring - Human Performance Monitoring enhancements are a feedback input into the procedure, training, and AOF processes. The revised results are then put through the V&V process again to validate the adequacy of the changes.

The operational analysis inputs outlined above are processed through functional analysis to generate the lists and sequences of manipulations, decisions, parameters, controls, and indications to be allocated to the appropriate human and/or system resources. FRA inputs into AOF include the following:

- (1) The Plant Functional Requirements Analysis (PFRA) provides an integrated top down approach to functional analyses by linking plant-level goals, function, interdependencies, and redundancies with system level functions.
- (2) The System Functional Requirements Analysis (SFRA) yields a data structure that describes the functional dependencies within systems and relationship among systems. The

data structure provides system lineups, component manipulations, and process control requirements as inputs to the AOF.

- (3) The System Functional Gap Analysis SFGA links the PFRA and SFRA data structures creating a data structure that describes the plant function requirements down to the component level. The SFGA generates design inputs to ensure that design fulfills the ESBWR mission and goals. This data structure provides inventories of required parameters, indications and controls, and outline sequences to be processed by AOF.

#### 4.1.3 Process

Plant safety and reliability are enhanced by exploiting the strengths of personnel and system elements, including improvements that can be achieved through assigning control to these elements with overlapping and redundant responsibilities. Allocations of functions are based upon HFE principles using a structured and well-documented methodology that provides personnel with logical, coherent, and meaningful tasks. It is not based solely on technology considerations that allocate to plant personnel everything the designers cannot automate. The technical basis for all allocations is documented, including the allocation criteria, rationale, and analysis method used. The technical basis for function allocation can be one factor, or a combination of factors. [compiled and adapted from NUREG-0711, Rev 2]

Allocation of function is a qualitative process relying heavily on the judgment of the expert teams and their analysis of available data. Multi-disciplined teams perform the allocation of function analyses and make the appropriate decisions. These teams contain the minimum skills and experience specified in the ESBWR Man-Machine Interface System And Human Factors Engineering Implementation Plan, Reference 2.1.1(2). The teams are comprised of members from operations, engineering, and HFE who present their expert opinions. The team utilizes the structured process shown in Figures 2, 3, and 4, the descriptions and criteria presented in this section, and Tables A.1 and A.2 in Appendix A when making allocation decisions. In addition, Appendix B provides additional contextual information and guidance for the technical bases being considered. This process ensures that:

- Conservatism is fundamental to the judgment process, and allocations:
  - Result in safe, reliable, and efficient operation of the ESBWR, in compliance with regulations
  - Place reasonable demands on and provide reasonable support of personnel
  - Meet HFE principles
  - Take advantage of human strengths and avoid human weaknesses
- All available information is gathered and made available, including:
  - Past performance of analogous systems including OER/BRR results
  - Quantified engineering predictions including PRA results
  - Human factors experimental data
  - Previous system cost data and future cost estimates

- Input/output data from connected subsystems of the design
- Previously completed allocations of identical or substantially similar functions
- Allocation decisions are broken into their logical elements.
- Allocations are the sum of expert professional judgments.
- Judgment is made by a consensus of qualified people.
- An expanding body of analysis and design data informs each judgment.
- All aspects are considered.
- Allocation is closely responsive to other design decisions and could change when the other design decisions change.
- Formal records are kept that capture the criteria, rationale, and analysis method for use during later cycles of redesigns or plant modifications. [Compiled and adapted from NUREG/CR-3331]

Figure 2 presents the phases in which allocations of function are performed and the expected outcomes. Figure 3 presents the methodology, logic, and sequence by which allocation decisions are made. Figure 4 presents the methodology, logic, and sequence by which the details of shared allocation decisions are made. Each of the decision points in the attached Figures is described below.

#### **4.1.3.1 Allocation of Function Flow Chart Process**

- (1) **Safety-Related Function** – Those plant Structures, Systems, and Components (SSCs) that prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public (see Appendix B to Part 50 of Title 10 of the U.S. Code of Federal Regulations). These are the SSCs on which the design-basis analyses of the safety analysis report are performed. ESBWR DCD and Technical Specifications further define which systems are safety-related or have functions that support the operability of safety-related systems.
- (2) **Automatic Actuation Required** – Functions that must be carried out by the machine due to regulatory requirement, design, or expert judgment. Later steps in the allocation of function logic will determine if human actions are also required to support successful completion of the function. Appendix A is referenced when making this determination. If any of the human limitations presented in Table A1 are part of the function being evaluated, automation is preferred unless otherwise precluded. If any of the uniquely human capabilities presented in Table A2 are part of the function being evaluated, human participation is required. Some technical bases considered when determining if automatic actuation is required include:
  - Regulatory requirement
  - Design requirement
  - PRA basis assumption
  - HRA/PRA risk significance

- OER/BRR significance
- Human cognitive limitations
- Human response time limitations
- Human physical limitations
- Hostile environment including atmosphere, temperature, and radiation

(3) **Human Backup Required** – Functions allocated to the machine that, due to their importance or nature, require either concurrent or supporting human action as specified by regulatory requirement, design, or expert judgment. Later steps in the allocation of function logic will determine the nature of human actions required to support successful completion of the function. Appendix A is referenced when making this determination. If any of the human limitations presented in Table A1 are part of the function being evaluated, automation is preferred unless otherwise precluded. If any of the uniquely human capabilities presented in Table A2 are part of the function being evaluated, human participation is required. Some technical bases considered when determining if human backup is required include:

- Regulatory requirement
- Design requirement
- PRA basis assumption
- Economic risk
- OER/BRR significance
- Consequence of automation failure
- Vesting ultimate control in the human
- Ensuring the human retains necessary emergency control
- Qualitative, discretionary, or deductive decision making required

(4) **Automatic Backup Required** – Functions allocated to the human that, due to their importance or nature, require either concurrent or supporting machine action as specified by regulatory requirement, design, or expert judgment. Later steps in the allocation of function logic will determine the nature of machine actions required to support successful completion of the function. Appendix A is referenced when making this determination. If any of the human limitations presented in Table A1 are part of the function being evaluated, automation is preferred unless otherwise precluded. If any of the uniquely human capabilities presented in Table A2 are part of the function being evaluated, human participation is required. Some technical bases considered when determining if automatic backup is required include:

- Regulatory requirement
- Design requirement
- PRA basis assumption

- HRA/PRA risk significance
  - Economic risk
  - OER/BRR significance
  - Consequence of human failure
  - Human limitations/machine capabilities
  - Cognitive overload
  - Human workload
- (5) **Configuration Change Required** – Functions which have been analyzed and found not to be safety-related and for which the affected component(s) changes state during normal, abnormal, or emergency operation. An example of such a component is a feed water manual isolation valve inside containment. The feed water isolation valve is only operated when the plant is shutdown, feed water is to be isolated, and personnel are inside containment. Such a valve does not need automation but may need remote operation capability due to its physical location inside containment.
- (6) **Remote Operation Required** – Functions that must be carried out from a location detached from the component(s) to be monitored, controlled, or manipulated due to regulatory requirement, design, or expert judgment. Later steps in the allocation of function logic will determine if machine actions are also required to support successful completion of the function. Some technical bases considered when determining if remote operation is required include:
- Regulatory requirement
  - Design requirement
  - PRA basis assumption
  - HRA/PRA risk significance
  - OER/BRR significance
  - Design layout – is the SSC accessible?
  - Human response time limitations
  - Human physical limitations
  - Broader plant control or monitoring requirements than is available locally
  - Hostile environment including atmosphere, temperature, and radiation
  - Human workload
  - Safety or economic risk associated with local operation
  - Economic benefit – centralized work location, fewer humans required, or other considerations

- (7) **Plant Automation System** – Functions that are carried out using the ESBWR’s HSI computers, their associated programming and logic, and linked remote control and indications capabilities. Later steps in the allocation of function logic will determine if human actions are also required to support successful completion of the function.
- (8) **Machine Only** – This output allocation assigns the function data sequences generated in FRA for the function being analyzed exclusively to the machine for implementation.
- (9) **Shared** - This output allocation assigns the function data sequences generated in FRA for the function being analyzed to a combination of both human and machine for implementation. Figure 4 outlines the process used to refine and define shared allocations to take advantage of human strengths and avoid human weaknesses. Figure 4 summarizes the possible shared function allocations.
- (10) **Human Only** - This output allocation assigns the function data sequences generated in FRA for the function being analyzed exclusively to the human for implementation.

#### 4.1.3.2 *Shared Function Detailed Flowchart Process*

- (1) **Machine Control Required** – Aspects of the shared functions that must be carried out by the machine due to regulatory requirement, design, or expert judgment. Later steps in the allocation of function logic will determine what human actions are also required to support successful completion of the function. Appendix A is referenced when making this determination. If any of the human limitations presented in Table A1 are part of the function being evaluated, automation is preferred unless otherwise precluded. If any of the uniquely human capabilities presented in Table A2 are part of the function being evaluated, human participation is required. Some technical bases considered when determining if machine control is required include:
  - Regulatory requirement
  - Design requirement
  - PRA basis assumption
  - HRA/PRA risk significance
  - OER/BRR significance
  - Human cognitive limitations
  - Human response time limitations
  - Human physical limitations
  - Hostile environment including atmosphere, temperature, and radiation
- (2) **Machine Control Practical** – Aspects of the shared functions to be carried out by the machine due to regulatory requirement, design, or expert judgment. This decision point evaluates whether or not functions allocated to the machine can be realistically carried out. Later steps in the allocation of function logic will determine if design changes to the ESBWR are required and what human actions are also required to support successful completion of the function. Appendix A is referenced when making this determination. If any of the human limitations presented in Table A1 are part of the function being

evaluated, automation is preferred unless otherwise precluded. If any of the uniquely human capabilities presented in Table A2 are part of the function being evaluated, human participation is required. Some technical bases considered when determining if machine control is practical include:

- OER/BRR significance
- Technical feasibility
- Economic feasibility
- Reliability
- Predictability
- Development time
- Component availability
- Cost

(3) **Human Backup Desired** – Aspects of the shared functions allocated to the machine that, due to their importance or nature require either concurrent or supporting human action as specified by regulatory requirement, design, or expert judgment. These supporting human actions take the form of either limitations requiring human action for automation to proceed or human backup in the form of human execution of functions allocated to the machine but which were not completed. This logic block is used when deciding between human backup and human limitations to machine functions. Appendix A is referenced when making this determination. If any of the human limitations presented in Table A1 are part of the function being evaluated, automation is preferred unless otherwise precluded. If any of the uniquely human capabilities presented in Table A2 are part of the function being evaluated, human participation is required. Some technical bases considered when determining whether to allocate human backup or human limitation include:

- Regulatory requirement
- Design requirement
- PRA basis assumption
- Economic risk
- OER/BRR significance
- Consequence of automation failure
- Vesting ultimate control in the human
- Ensuring the human retains necessary emergency control
- Qualitative, discretionary, or deductive decision making required
- Human workload
- Human limitations/machine capabilities
- Cognitive overload

(4) **Machine Control Desired** – Aspects of the shared functions that can be carried out by either human or machine assigned the machine due to design or expert judgment. Later steps in the allocation of function logic will determine what human actions are also required to support successful completion of the function. Appendix A is referenced when making this determination. If any of the human limitations presented in Table A1 are part of the function being evaluated, automation is preferred unless otherwise precluded. If any of the uniquely human capabilities presented in Table A2 are part of the function being evaluated, human participation is required. Some technical bases considered when determining if machine control is desired include:

- PRA basis assumption
- HRA/PRA risk significance
- OER/BRR significance
- Human cognitive limitations
- Human response time limitations
- Human physical limitations
- Hostile environment including atmosphere, temperature, and radiation
- Risk to the operator
- Degree to which function is predictable or repeatable
- Impact on vigilance and situational awareness
- Human limitations for:
  - Functions which are lengthy
  - Functions which require high consistency
  - Functions which require high accuracy
  - Functions which involve boredom or monotony for the operator

(5) **Error Consequence Acceptable** – Aspects of the shared functions for which machine control is neither required nor desired that are to be carried out by the human due to design or expert judgment. This logic block is used when deciding whether the consequences of potential human errors of omission or commission are acceptable. Later steps in the allocation of function logic will determine what machine actions are also required to support successful completion of the function. Some technical bases considered when determining if potential human error consequences are acceptable include:

- Can the error be corrected to eliminate adverse consequences?
- Could the error cause a scram, turbine trip, or initiate a transient?
- Could the error prevent the performance of a safety-related function?
- Could the error result in a release of radionuclides?
- Could the error result in unplanned radiation exposure?

- Could the error result in exceeding environmental or other regulatory limits?
- Cognitive overload
- Human workload
- Economic risk
- Regulatory margin
- HRA/PRA risk significance

(6) **Human Control Practical** – Aspects of the shared functions for which machine control is neither required nor desired that are to be carried out by the human due to design or expert judgment. The consequences of potential human errors of omission or commission have been evaluated and found acceptable. This decision point evaluates whether or not functions allocated to the human can be realistically carried out. Later steps in the allocation of function logic will determine what machine actions are also required to support successful completion of the function. Appendix A is referenced when making this determination. If any of the human limitations presented in Table A1 are part of the function being evaluated, automation is preferred unless otherwise precluded. If any of the uniquely human capabilities presented in Table A2 are part of the function being evaluated, human participation is required. Some technical bases considered when determining if human control is practical include:

- Human cognitive limitations
- Human physical limitations
- Human response time limitations
- Economic feasibility
- Human workload
- Hostile environment including atmosphere, temperature, and radiation
- Risk to the operator
- Economic risk
- Degree to which function is predictable or repeatable
- Impact on vigilance and situational awareness
- Human limitations for:
  - Functions which are lengthy
  - Functions which require high consistency
  - Functions which require high accuracy
  - Functions which involve boredom or monotony for the operator

(7) **Error Mitigated by Human** – Aspects of the shared functions for which machine control is neither required nor desired that are to be carried out by the human due to design or

expert judgment. The consequences of potential human errors of omission or commission have been evaluated and found acceptable. Human control of the function has been evaluated and found to be practical. This decision point evaluates whether or not the human can mitigate the consequences of potential errors of omission or commission. Some technical bases considered when determining if the human provides error mitigation include:

- Information and controls available to the operator
- Time period between the error and unacceptable consequence
- Speed with which error consequences manifest themselves
- Methods by which error can be identified
- Error type: active or latent
- Is error reversible prior to the occurrence of an undesired result?
- Human cognitive limitations
- Human response time limitations
- Impact on vigilance and situational awareness
- Qualitative, discretionary, or deductive decision making required
- Human ability to properly diagnose and respond to the error

(8) **Error Mitigated by Machine** – Aspects of the shared functions for which machine control is neither required nor desired that are to be carried out by the human due to design or expert judgment. The consequences of potential human errors of omission or commission have been evaluated and found to be unacceptable. This decision point evaluates whether or not the machine can mitigate the consequences of potential errors of omission or commission. Some technical bases considered when determining if the machine provides error mitigation include:

- Speed with which error consequences manifest themselves
- Ability of the machine to detect the error
- Error type: active or latent
- Is error reversible prior to the occurrence of an undesired result?
- HRA/PRA risk significance
- OER/BRR significance
- Technical feasibility
- Economical feasibility
- Impact on vigilance and situational awareness
- Vesting ultimate control in the human
- Ensuring the human retains necessary emergency control

- (9) **Machine, Human Limited** – This output allocates the aspect of shared function to plant equipment and automation for performance. This performance is limited in one or more steps in the function data structure sequence by required human action of some kind. The required action can be an acknowledgement of a HSI queue alerting the operator to impending action or it can be more detailed. One example of when this allocation is selected is where economic impacts may result if the machine sequence continues.
- (10) **Machine, Human Backup** – This output allocates the aspect of shared function to plant equipment and automation for performance. Plant personnel monitor the machine and perform or complete performance of the function in the event that the machine does not complete its execution. Analysis has shown that while the machine is best suited to perform the function sequence, plant personnel are capable of performing the sequence if called upon. Additionally, analysis has determined that the consequences of partial or incorrect performance are such that operator performance of the functions following machine failure is warranted.
- (11) **Human, Machine Assist** – This output allocates the aspect of shared function to plant personnel for performance. Equipment and automation assist plant personnel in performance of the function. Analysis has shown that the human is capable of mitigating error consequences. One or more forms of machine assistance are provided to aid in the performance of the function.
- (12) **Human, Machine Backup** – This output allocates the aspect of shared function to plant personnel for performance. The machine monitors human performance of the function and performs or completes performance of the function in the event that the human does not complete its execution. Analysis has shown that while the human is best suited to perform the function sequence, potential error consequences are unacceptable and the machine is capable of mitigating the consequences of potential human errors.
- (13) **Design Input** – This output is attained, as shown in Figure 4, when allocation analysis reaches an unacceptable conclusion with the design and allocation options presented. The aspect of the shared functions or sub-functions that cause this output conclusion are feedback inputs to the ESBWR design process for the development of design changes that correct the issue. If a design solution cannot be identified using the normal iterative HFE design process, then the issue is entered into HFEITS for resolution.

#### 4.1.4 Outputs

The function outline sequences generated in FRA and processed through AOF are evaluated using the logic and sequence shown in Figures 2 and 3. There are criteria that have been established for each of these decision points. Each function or sub-function in the sequence is evaluated and allocated to one of the following resources for execution:

- **Human Only** – the function is executed entirely by plant personnel. The HSI is used to carry out the actions and monitoring performed by humans. The machine has no direct control, backup, or limiting actions associated with the function(s) being allocated.
- **Machine Only** - the function is executed entirely by plant automation. Humans have no direct control, backup, or limiting actions associated with the function(s) being allocated.
- **Shared** - the function is executed using a combination of both human and machine resources. Figure 4 outlines the various combinations of human/machine sharing that can be allocated.

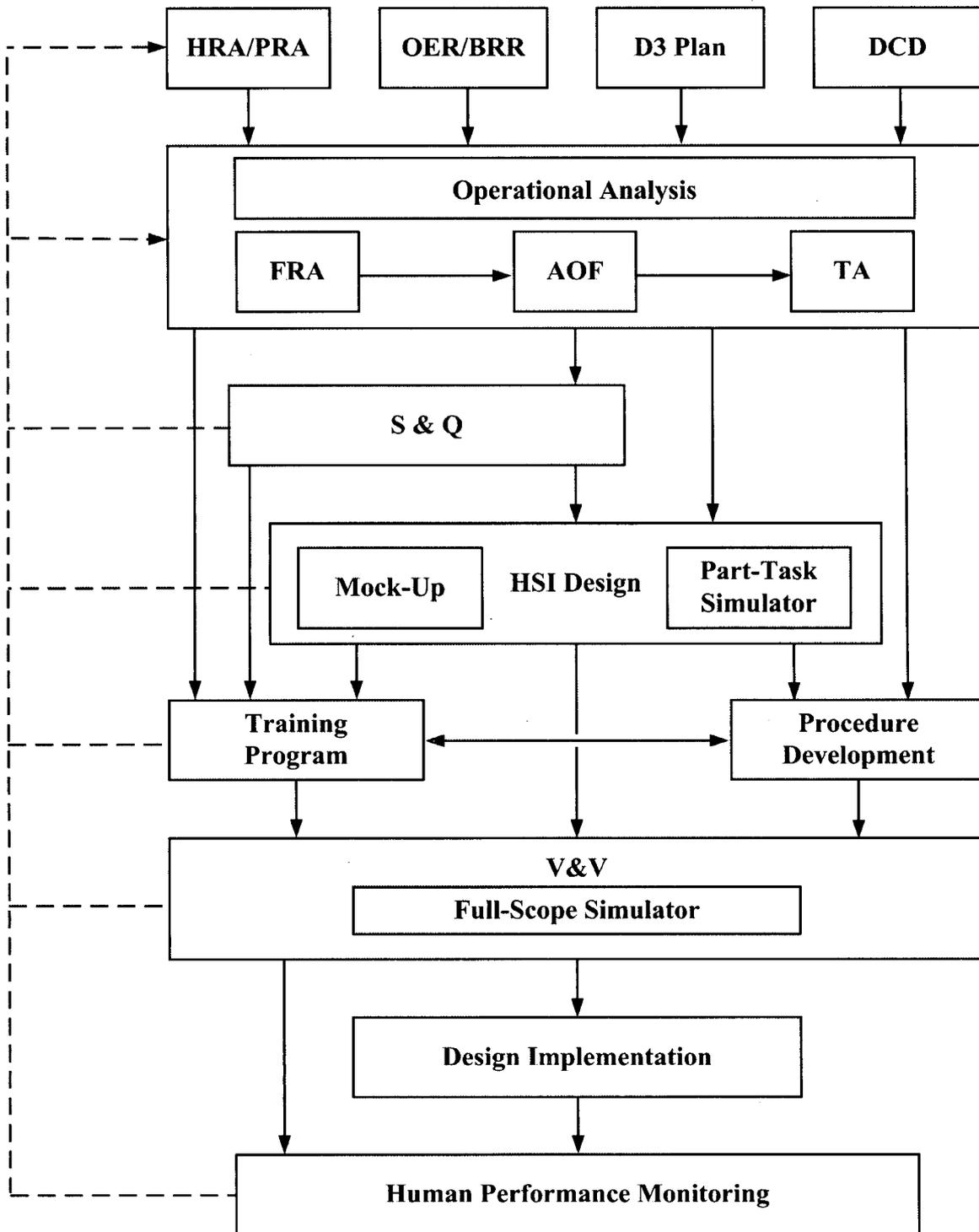
## **5. RESULTS**

### **5.1 RESULTS SUMMARY REPORTS**

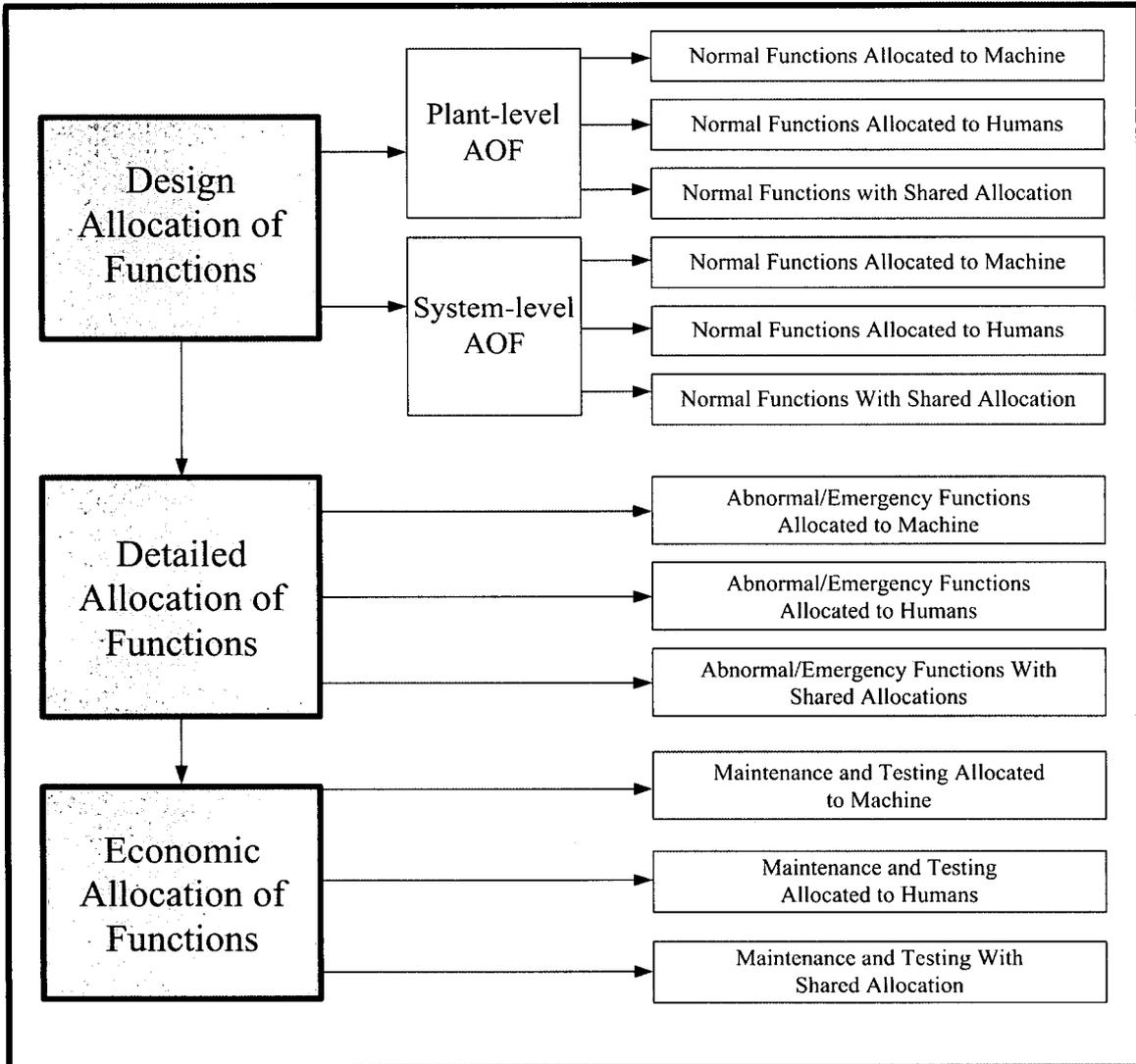
The results of the Allocation of Function are summarized in a Results Summary Report (RSR). This report is the main source of information used to demonstrate that efforts conducted in accordance with the implementation plan satisfy the applicable review criteria of NUREG-0800. The report contains the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

- General approach including the purpose and scope of AOF
- A summary of AOF results
- Safety function allocations
- The process for refining and updating functional allocations

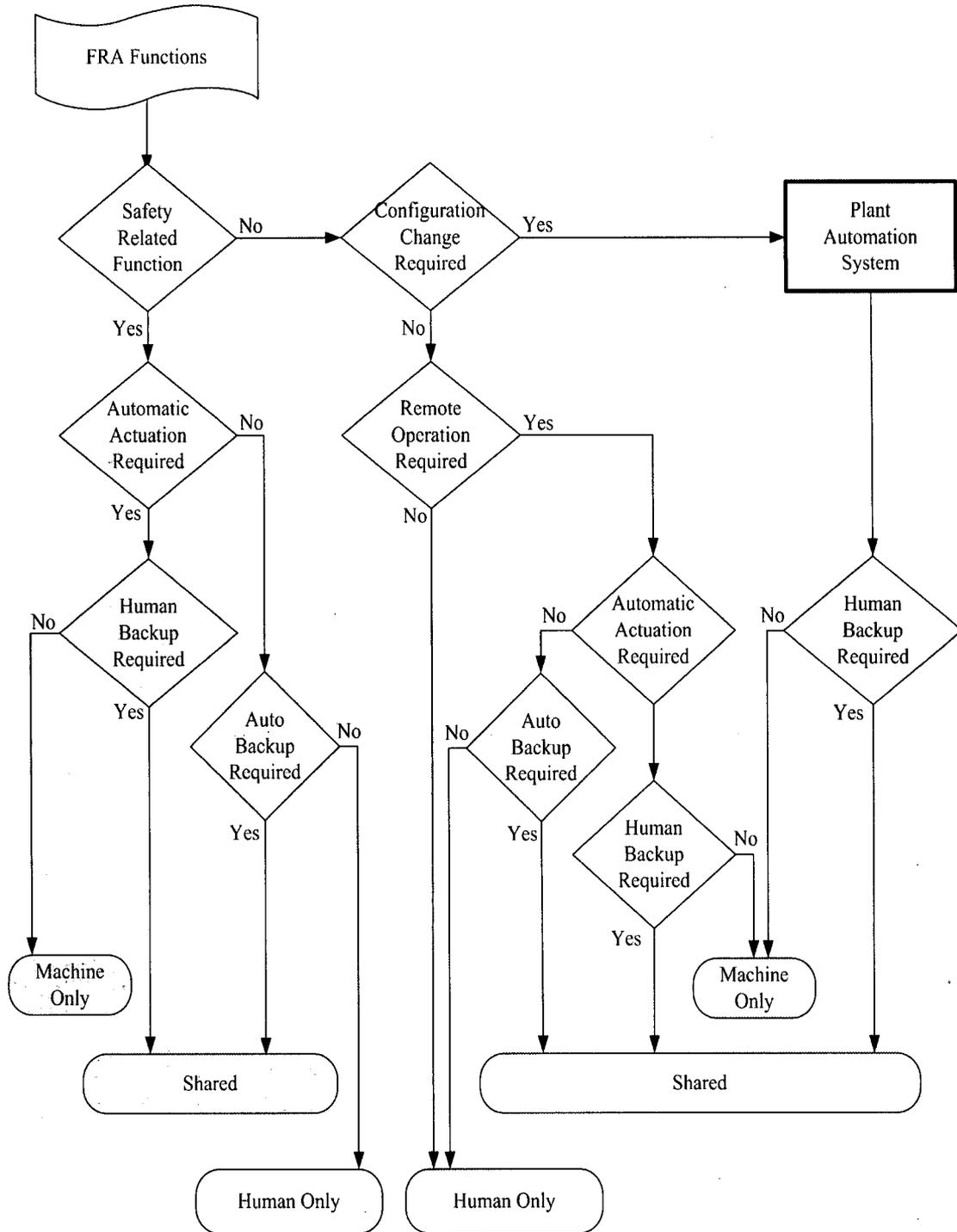
AOF Results Summary Reports (RSR) may be combined with the FRA and/or TA RSRs.



**Figure 1 HFE Implementation Process**



**Figure 2 Allocation of Function Phases**



**Figure 3 Allocation of Function Flowchart**

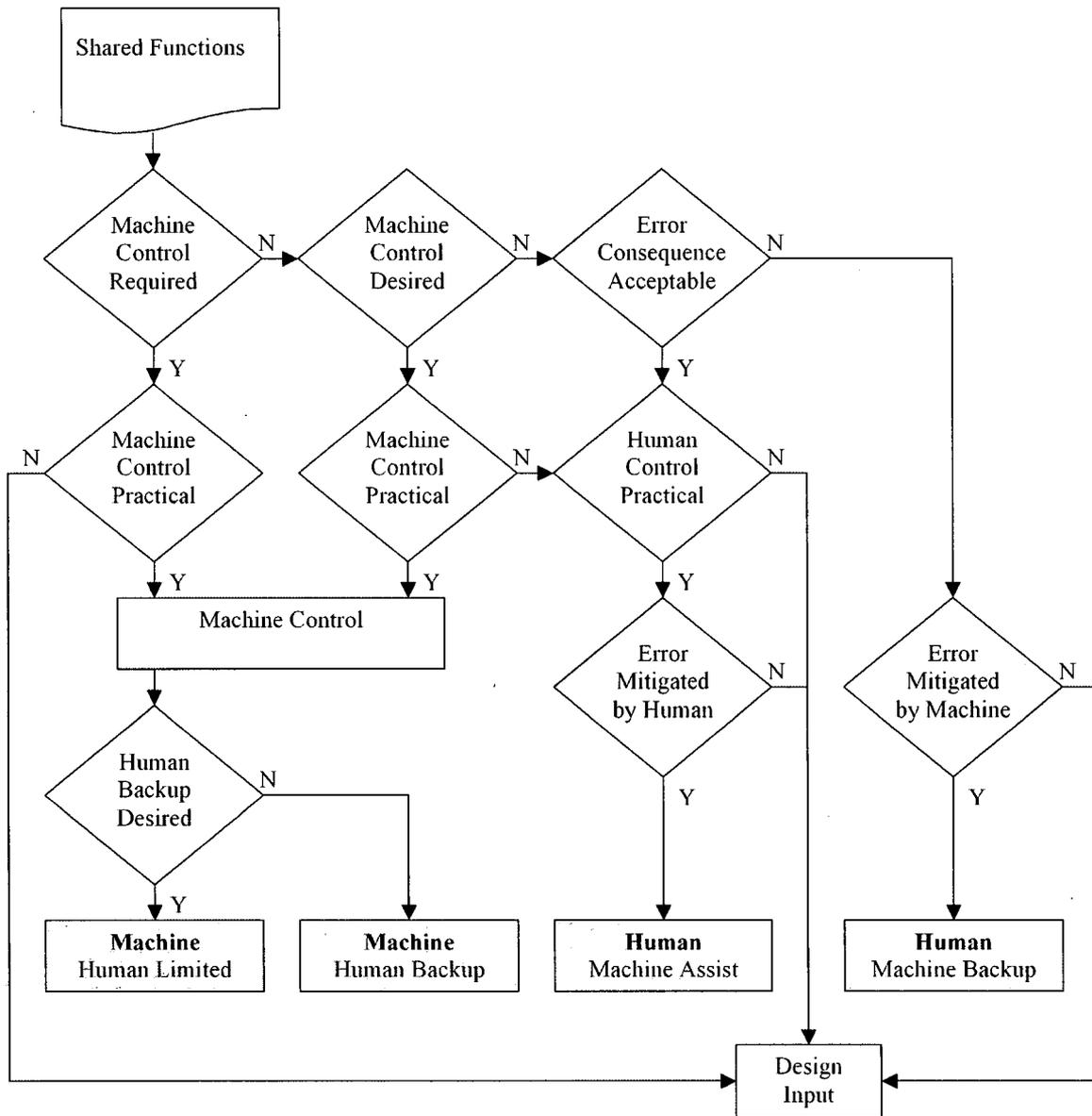


Figure 4 Shared Function Detailed Flowchart

**APPENDIX A HUMAN CAPABILITIES AND LIMITATIONS**

Consideration should be given to the exclusion of the human in performing a function when one or more of the criteria below apply [NUREG/CR-2623]:

**Table A.1  
Criteria that Limit or Preclude Human Participation in a System Function**

<b>Application of Force</b>	Large, precise, or extended applications of force preclude the human. Human instantaneous peak force is limited to a mean force of 50 Newtons (11.24 pounds force).
<b>Response to Stimuli/Signals</b>	The human operator experiences a finite lag between the onset of a stimulus and the ability to make a response to it. This lag varies from a mean of 100 msec for auditory stimuli and approximately 120 msec for visual stimuli, to lags in excess of 1 second for responses involving a choice among alternatives.
<b>Precise Calibration and Measurement</b>	Humans are incapable of making precise measurements and calibrations mentally.
<b>Reliable Response</b>	Because of the variability of human response, humans should be precluded from performing functions which require the unvarying repetition of one or more responses.
<b>Time Sharing</b>	Under most circumstances, humans act as a single-channel information processor and should ordinarily be precluded from performing multiple time-shared tasks.
<b>Continuous Performance</b>	Humans should be precluded from performing functions which cannot be interrupted or which require sustained attention for long periods of time (e.g., in excess of 20 minutes).
<b>Detection of Infrequent Events</b>	Humans should be precluded from performing functions that require detecting rarely occurring stimuli, events, or conditions.

## APPENDIX A: HUMAN CAPABILITIES AND LIMITATIONS

Human participation in the performance of a function is mandatory when the function requires one or more of the following capabilities [NUREG/CR-2623]:

**Table A.2**  
**Criteria that Define Unique Human Capabilities**

<b>Develop a Strategy</b>	Human involvement is mandatory when <ul style="list-style-type: none"> <li>• Operations cannot be reduced to preset procedures</li> <li>• The form and content of all inputs and outputs cannot be specified or predicted</li> <li>• The relationship between inputs and outputs may require restructuring during task performance.</li> </ul>
<b>Integrate a Large Amount of Information</b>	Humans must be included in the accomplishment of a function when: <ul style="list-style-type: none"> <li>• Signals must be detected against a noisy background</li> <li>• Patterns of information and trends must be extracted from several sources.</li> </ul>
<b>Make and Report Unique Observations</b>	Humans must be included when a function requires that observation be made of: <ul style="list-style-type: none"> <li>• The performance of others;</li> <li>• The performance of the individual;</li> <li>• Ephemeral (continuous, endless events, etc.)</li> </ul>
<b>Assign Meaning and Value to Events</b>	Humans must be included when performance of a system or function requires that meaning and relative values be assigned to events.

## **APPENDIX B ALLOCATION OF FUNCTION CRITERIA**

[[

]]

### **B.1 REGULATORY REQUIREMENT**

[[

]]

**B.2 DESIGN REQUIREMENT**

[[

]]

**B.3 PRA BASIS ASSUMPTION**

[[

]]

**B.4 PRA/HRA RISK SIGNIFICANCE**

[[

]]

**B.5 OER/BRR SIGNIFICANCE**

[[

]]

**B.6 HUMAN COGNITIVE LIMITATIONS**

[[

]]

**B.7 HUMAN RESPONSE TIME LIMITATIONS**

[[

]]

**B.8 HUMAN PHYSICAL LIMITATIONS**

[[



]]

**B.9 HOSTILE ENVIRONMENT INCLUDING ATMOSPHERE, TEMPERATURE,  
AND RADIATION**

[[

]]

**B.10 ECONOMIC RISK**

[[

]]

**B.11 CONSEQUENCE OF AUTOMATION FAILURE**

[[

]]

**B.11.1 HUMAN BACKUP REQUIRED**

[[

]]

**B.11.2 HUMAN BACKUP DESIRED**

[[

]]

**B.12 VESTING ULTIMATE CONTROL IN THE HUMAN**

[[

]]

**B.13 ENSURING THE HUMAN RETAINS NECESSARY EMERGENCY CONTROL**

[[

]]

**B.14 QUALITATIVE, DISCRETIONARY, OR DEDUCTIVE DECISION MAKING  
REQUIRED**

[[

]]

**B.15 CONSEQUENCE OF HUMAN FAILURE**

[[

]]

**B.16 HUMAN LIMITATIONS/MACHINE CAPABILITIES**

[[




]]

**B.17 COGNITIVE OVERLOAD**

[[

]]

**B.18 HUMAN WORKLOAD**

[[



]]

**B.19 DESIGN LAYOUT – IS THE SSC ACCESSIBLE?**

[[

]]

**B.20 BROADER PLANT CONTROL OR MONITORING REQUIREMENTS THAN IS AVAILABLE LOCALLY**

[[

]]

**B.21 SAFETY OR ECONOMIC RISK ASSOCIATED WITH LOCAL OPERATION**

[[

]]

**B.22 ECONOMIC BENEFIT – CENTRALIZED WORK LOCATION, FEWER HUMANS REQUIRED, OR OTHER CONSIDERATIONS**

[[

]]

**B.23 TECHNICAL FEASIBILITY**

[[

]]

**B.24 ECONOMIC FEASIBILITY**

[[

]]

**B.25 RELIABILITY**

[[

]]

**B.26 PREDICTABILITY**

[[

]]

**B.27 DEVELOPMENT TIME**

[[

]]

**B.28 COMPONENT AVAILABILITY**

[[

]]

**B.29 COST**

[[

]]

**B.30 RISK TO THE OPERATOR**

[[

]]

**B.31 DEGREE TO WHICH FUNCTION IS PREDICTABLE OR REPEATABLE**

[[

]]

**B.32 IMPACT ON VIGILANCE AND SITUATIONAL AWARENESS**

[[

]]

**B.33 HUMAN LIMITATIONS**

[[

]]

**B.34 CAN THE ERROR BE CORRECTED TO ELIMINATE ADVERSE CONSEQUENCES?**

[[

]]

**B.35 COULD THE ERROR CAUSE A SCRAM, TURBINE TRIP, OR INITIATE A TRANSIENT?**

[[

]]

**B.36 COULD THE ERROR PREVENT THE PERFORMANCE OF A SAFETY-RELATED FUNCTION?**

[[

]]

**B.37 COULD THE ERROR RESULT IN A RELEASE OF RADIONUCLIDES?**

[[

]]

**B.38 COULD THE ERROR RESULT IN UNPLANNED RADIATION EXPOSURE?**

[[

]]

**B.39 COULD THE ERROR RESULT IN EXCEEDING ENVIRONMENTAL OR  
OTHER REGULATORY LIMITS?**

[[

]]

**B.40 REGULATORY MARGIN**

[[

]]

**B.41 INFORMATION AND CONTROLS AVAILABLE TO THE OPERATOR**

[[

]]

**B.42 TIME PERIOD BETWEEN THE ERROR AND UNACCEPTABLE  
CONSEQUENCE**

[[

]]

**B.43 SPEED WITH WHICH ERROR CONSEQUENCES MANIFEST THEMSELVES**

[[

]]

**B.44 METHODS BY WHICH ERROR CAN BE IDENTIFIED**

[[

]]

**B.45 ERROR TYPE: ACTIVE OR LATENT**

[[

]]

**B.46 IS ERROR REVERSIBLE PRIOR TO THE OCCURRENCE OF AN UNDESIRE  
RESULT?**

[[

]]

**B.47 HUMAN ABILITY TO PROPERLY DIAGNOSE AND RESPOND TO THE ERROR**

[[

]]

**B.48 ABILITY OF THE MACHINE TO DETECT THE ERROR**

[[

]]