AREVA NP Inc.

U.S. EPR™ Implementation Plan

Document No.: 118 - 9018214 - 004

U.S. EPR Functional Requirements Analysis and Functional Allocation Implementation Plan

Intentionally left blank

Record of Revision

Revision No.	Pages/Sections/ Paragraphs Changed	Brief Description / Change Authorization
000	N/A	Original Issue
001	All	Format Change. Added specific functional allocation procedure for EPR™ design. Added more automation criteria. / Per Procedure 0405-06, DCR not required. No changes to physical plant, functional requirements or operating characteristics of a SSC.
002	All	Complete plan rewrite including title for addition of FRA. This copy is equivalent to 117-9110830-000
003	All	RAI 374 response
004	Sections 3.0, 3.1, 3.2, 4.4	Revisions to incorporate RAI 433 responses

Table of Contents

Page

Table of Contents
(continued)

Page

List of Tables

Page

List of Figures

Page

1.0 INTRODUCTION

1.1 Applicability

This implementation plan applies to engineering for the U.S. EPR™ standard design.

1.2 Owner

Program Manager, Human Factors Engineering (HFE) is responsible for maintaining and assuring the execution of this implementation plan.

1.3 Interfaces

Table 1-1: Functional Requirements and Allocation Correlation with other HFE Elements

HFE Elements	Impact

Task Analysis (TA)	Following FRA/FA, task analysis updates the FRA/FA data structure to address the following:
	• Addition, deletion, or changes to plant functions
	• Addition, deletion, or changes to system functions
	• Addition, deletion, or changes system components
	• Addition, deletion, or changes to functional allocations
	The staffing and qualification assumptions (Reference [1]) are updated to address the following issues:
	• Mismatches between functions allocated to personnel and their qualifications which may require
	  • Changes in staffing levels
	  • Changes to personnel qualifications
	• Changes in the roles of personnel due to plant system and HFE modifications which may require:
	  • Changes to how teamwork is supported
	Changes in task assignments that are made to make them more efficient or to reduce workload

Human System Interface (HSI)	The HSIs are designed to support the operator's role in the plant and to provide appropriate levels of automation, group and component level control and monitoring.
Procedure Development	The procedure modifications address all personnel tasks that are affected by changes in plant and system alignments and operating modes.

1.4 Purpose

This implementation plan establishes methods, criteria, and guidance for functional requirements analysis (FRA) and functional allocation (FA) for the U.S. EPR™ plant design. The FRA identifies those functions that are performed to satisfy plant safety and power generation objectives. This plan also describes how those defined functions are allocated among systems and trains, to automatic, group-level, and component-level control in order to meet regulatory requirements. The plan also uses FA to capitalize on human abilities and to promote situational awareness.

1.5 Objectives and Scope

The HFE design process is illustrated by Figure 1-1: HFE Process Integration. The figure illustrates the FRA/FA process within the framework of the overall HFE integration process. Outputs are used in task analysis and then through other HFE defined processes.

1.5.1 Functional Requirements Analysis

1.5.1.1 Gap Analysis (GA)

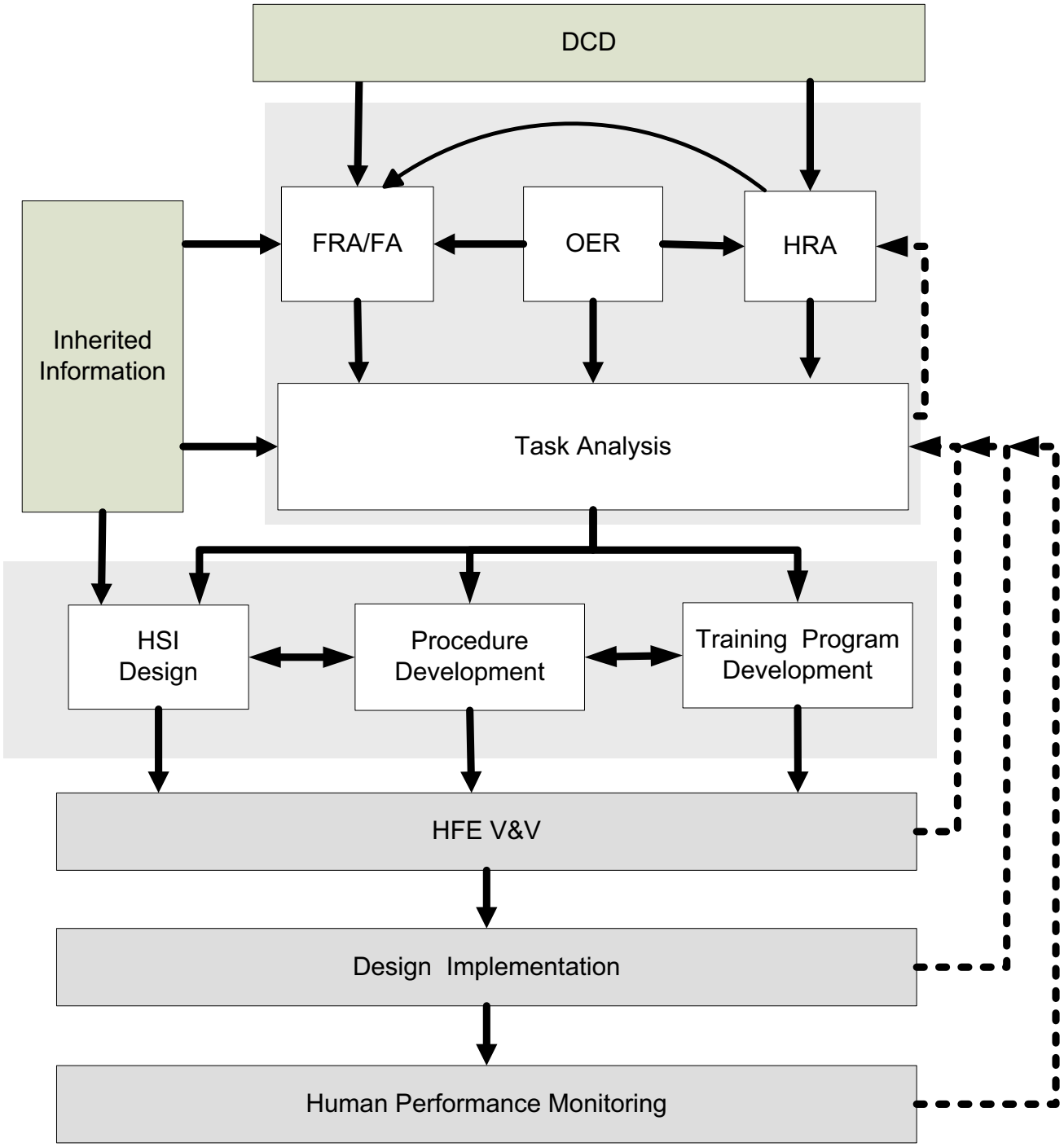
Gap analysis ensures that all the necessary plant-level functions are met by the final system designs. This process compares the required functions to those that exist in the design. Gaps between plant functions and system functions are analyzed for impact. Gaps are submitted for review and reconciliation using the design change process.

1.5.2 Functional Allocation

[

]

Figure 1-1: HFE Process Integration



Refer to section 4.4 for more information regarding the interaction between FRA/FA and other HFE design process elements.

1.6 Definition of Terms

Functional Requirements Analysis	The examination of system goals to determine the functions that are needed to achieve those system goals.
Functional Allocation	FA is the allocation of plant-level functions to systems functions, allocation of system control among 1E, non-safety and diverse control systems, among automatic, group and component-level control, and among control room crew, field operators and other plant personnel.
Human System Interfaces	The HSI is a system of devices, which includes hardware and software, used by personnel use to control, monitor, and interact with the plant including the alarms, displays, controls, and decision support aids.
Operating Experience Review	A systematic review, analysis, and evaluation of operational experience that applies to the development of the man-machine interface design.
Requirements Management Tool	The requirements management tool is a software package that provides the ability to logically link requirements with their implementation in the U.S. EPR™ design. This tool provides a data repository with dynamic requirements traceability capabilities that allow users to trace design features "upward" in the hierarchy to increasingly higher tier requirements, or trace requirements "downward" in the hierarchy to their implementation in human system interface (HSI) design attributes. The requirements management tool also provides the capability to generate requirements traceability matrices to aid in regulatory review of the HSI design.
Risk-Significant Human Action	Actions that are performed by plant personnel to provide reasonable assurance of plant safety. Actions may be made up of one or more tasks. However, this designation shows that the actions have been evaluated and found to be above set criteria. These Human Actions have a FV value greater than or equal to .005 or a RAW score greater than or equal to 2.0. The initial list of these actions is located in Appendix B. These actions are based upon FV and RAW scores relative to the total analysis. The individual scores for each event type can be found in FSAR chapter 19.
Task Analysis	A method for describing what plant personnel must do to achieve the task purposes or goals. The description is in terms of cognitive activities, physical actions, interfaces, cues, supporting equipment, documents, and consequences.
Verification and Validation	The process by which the final product and integrated system is demonstrated to meet its initial design functional requirements as specified in the system design requirement document (SDRD), The HFE design is evaluated to ensure acceptability and to support safe operations. The process of checking and ensuring each step of the design process was implemented appropriately. Verification is the process of determining and documenting that an implemented design (a product, process, procedure, method, and so forth) meets its specifications. Verification answers the question: Was the design implemented appropriately? Validation is the process of determining and documenting that the HFE design effectively serves the purpose for which it was intended. Validation answers the question: Was the appropriate design implemented?

1.7 Abbreviations and Acronyms

Acronym	Description
AOO	Anticipated Operational Occurrence
AOP	Abnormal Operating Procedure
DCS	Distributed Control System
EOP	Emergency Operating Procedure
EPG	Emergency Procedure Guideline
EPR™	Evolutionary Power Reactor
FA	Functional allocation
FBT	Functional Branch Tree
FRA	Functional Requirement Analysis
FSAR	Final Safety Analysis Report
GA	Gap Analysis
GDC	General Design Criteria
HED	Human Engineering Discrepancy
HFE	Human Factors Engineering
HRA	Human Reliability Analysis
HSI	Human System Interfaces
I&C	Instrumentation and Control
IRWST	In Containment Refueling Water Storage Tank
LCS	Local Control Station
MCR	Main Control Room
OER	Operating Experience Review
PRA	Probabilistic Risk Assessment
P&ID	Piping and Instrumentation Drawing
PWR	Pressurized Water Reactor
RCS	Reactor Coolant System
RSS	Remote Shutdown System
SDD	System Description Document
SDRD	System Design Requirements Documents
SFGA	System Function Gap Analysis

SFRA	System Functional Requirements Analysis
TA	Task Analysis
TS	Technical Specification
V&V	Verification and Validation

2.0 CODES, STANDARDS AND REGULATIONS

2.1.1 10 CFR 50, Appendix A, "General Design Criteria for Nuclear Power Plants

2.1.2 NUREG-0711, Rev 2, "Human Factors Engineering Program Review Model"

2.1.3 NUREG-0800, Rev 1, "Standard Review Plan, Chapter 18, Human Factors Engineering", 2007 (Reference [2])

3.0 METHOD

FRA evaluates two function levels: plant functions and system functions. Initially, system interdependence, interaction and defense-in-depth at the plant level are studied. After completion of the plan-level analysis, FRA focuses on the functional capabilities of physical plant systems and equipment.

Plant-level FRA (PFRA) and system functional requirements analysis (SFRA) are followed by a system function gap analysis (SFGA). Due to the EPR™ design being an evolutionary design, the systems are sufficiently developed to allow a concurrent PFRA and SFRA. The system functional capability assumptions that allow the SFRA to be completed in parallel are examined against those derived through the PFRA and either proven or disproved during the SFGA. During the SFGA, plant-level functional requirements are mapped to system functional capabilities. The functional relationships between plant functions and system functions are then reconciled. The output of gap analysis is a functional requirements traceability matrix that:

- Demonstrates that plant design goals are met
- Identifies any design goals that are not met and therefore require resolution
- Identifies any system functional capabilities that do not support any design goals and therefore warrant further consideration for possible elimination.

FA evaluates the results of FRA, U.S. EPR™ design as described in the FSAR, predecessor plant designs, and industry OE and assigns responsibility for functional control. FA allocates control of functions and execution of transitions between functions to automatic, human, or shared control. Functional allocations are optimized during the iterative HFE design process (workload analysis).

The FA process allocates normal, abnormal, and emergency system and plant functions. The Operating Experience Review (OER) input into the FRA/FA process supports FA decision making through the knowledge of prior successes as well as challenges to operator performance in predecessor or similar designs. PRA/HRA analysis input into the FRA/FA process identifies risk-significant human actions so that related allocation decisions can be made with great emphasis placed upon their successful completion.

The FRA/FA process produces a linked data structure of allocated plant level functions, associated functional requirements and system functional capabilities capable of meeting the plant functional needs. These results and resulting design decisions are evaluated during task analysis, and HSI design activities. Ultimately, the HFE V&V process verifies the results of the FRA/FA process.

3.1 Functional Requirements Analysis Implementation

3.1.1 General Method

3.1.2 Plant-Level Function Description and Mapping Include:

3.1.3 Plant System Function Descriptions and Mapping Provides:

3.1.4 The Structure

[

]

3.1.4.1 Plant Mission

The U.S. EPR™ reactor mission is the safe and economical generation of electricity from nuclear power.

3.1.4.2 Plant Level Goals and Objectives

Goals are divided into; nuclear safety goals and critical safety functions, and economic goals and power generation functions. These goals are divided into plant level objectives which are attainable, specific, and measurable.

3.1.4.3 Plant Functions

Plant functions are developed to fulfill the stated goal. This is meant as a high level view of the operational functions of the plant.

3.1.4.4 Plant Processes

Each plant function is divided into the processes necessary to accomplish the function.

3.1.4.5 Plant Diversity

Defense-in-Depth strategies (References [3] [4] [5]) and General Design Criteria (GDC) for diversity requirements to accomplish the function are considered at this level. For example, to control reactivity, GDC 26 directs that two independent reactivity control systems of different design principles shall be provided. The U.S. EPR™ reactor uses control rods and boron to control reactivity.

3.1.4.6 System Process Functions

System processes required to meet plant functions are developed at this level. Each process is stated generically and may not be used in all system functions. Each system process is described in sufficient detail to capture all normal and transient operating conditions and modes.

The SDD identifies initial system functions used to complete the FRA down to the component level. SFGA results are used to update the FRA and system documents (SDRD, SDD, P&ID etc.).

3.1.4.7 System Diversity

System functions and supporting systems that form all processes required to accomplish those functions, including diversity and defense-in-depth, are documented.

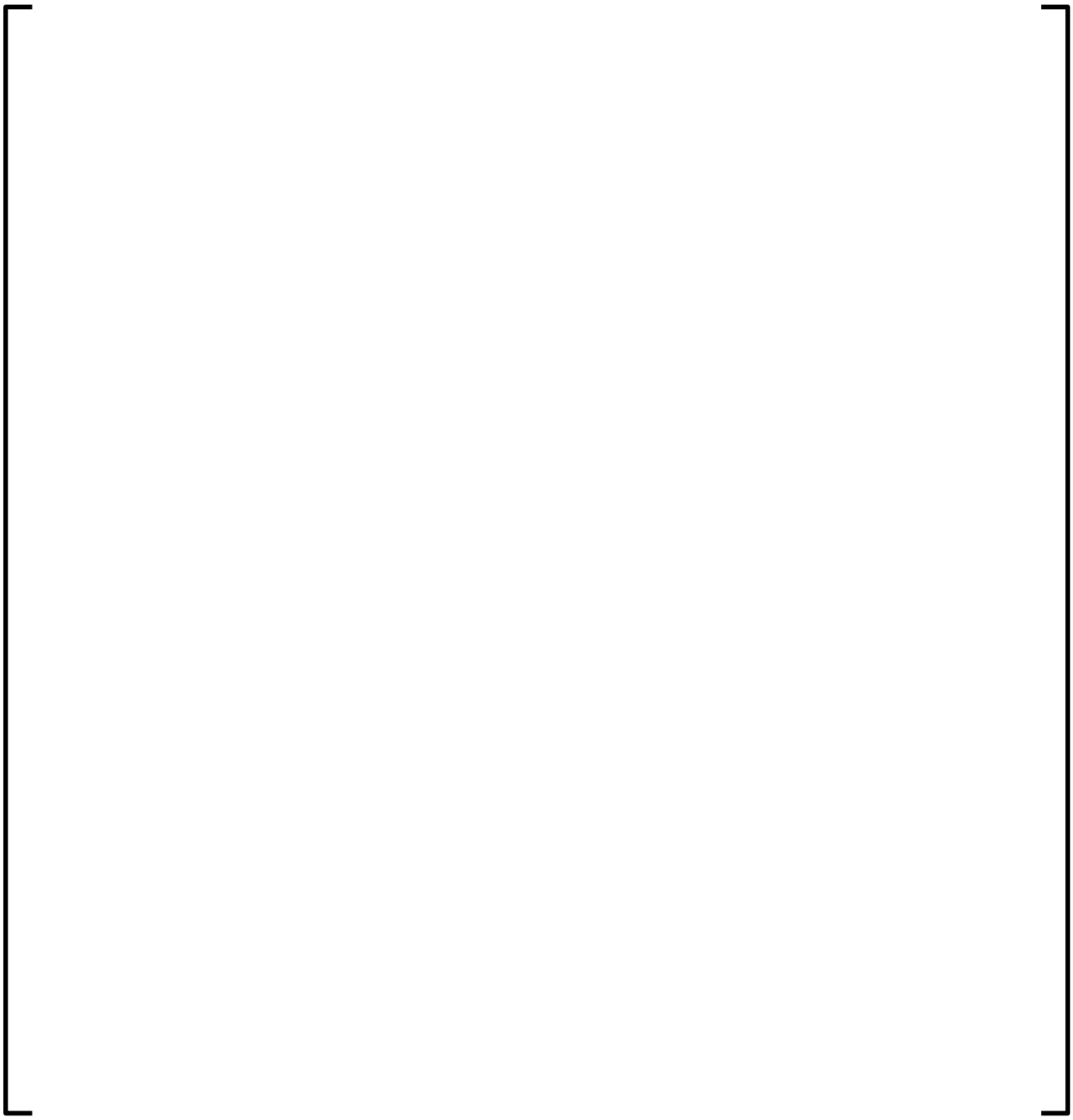
3.1.4.8 System Redundancies

System train, division, and channel redundancies that are designed to perform the same function are identified.

3.1.4.9 System Components

System SDDs identify all physical components that accomplish the system functions. This includes all mechanical components, control and monitoring elements, and alarm functions.

Figure 3-1: Overall General Layout of FRA and Gap Analysis



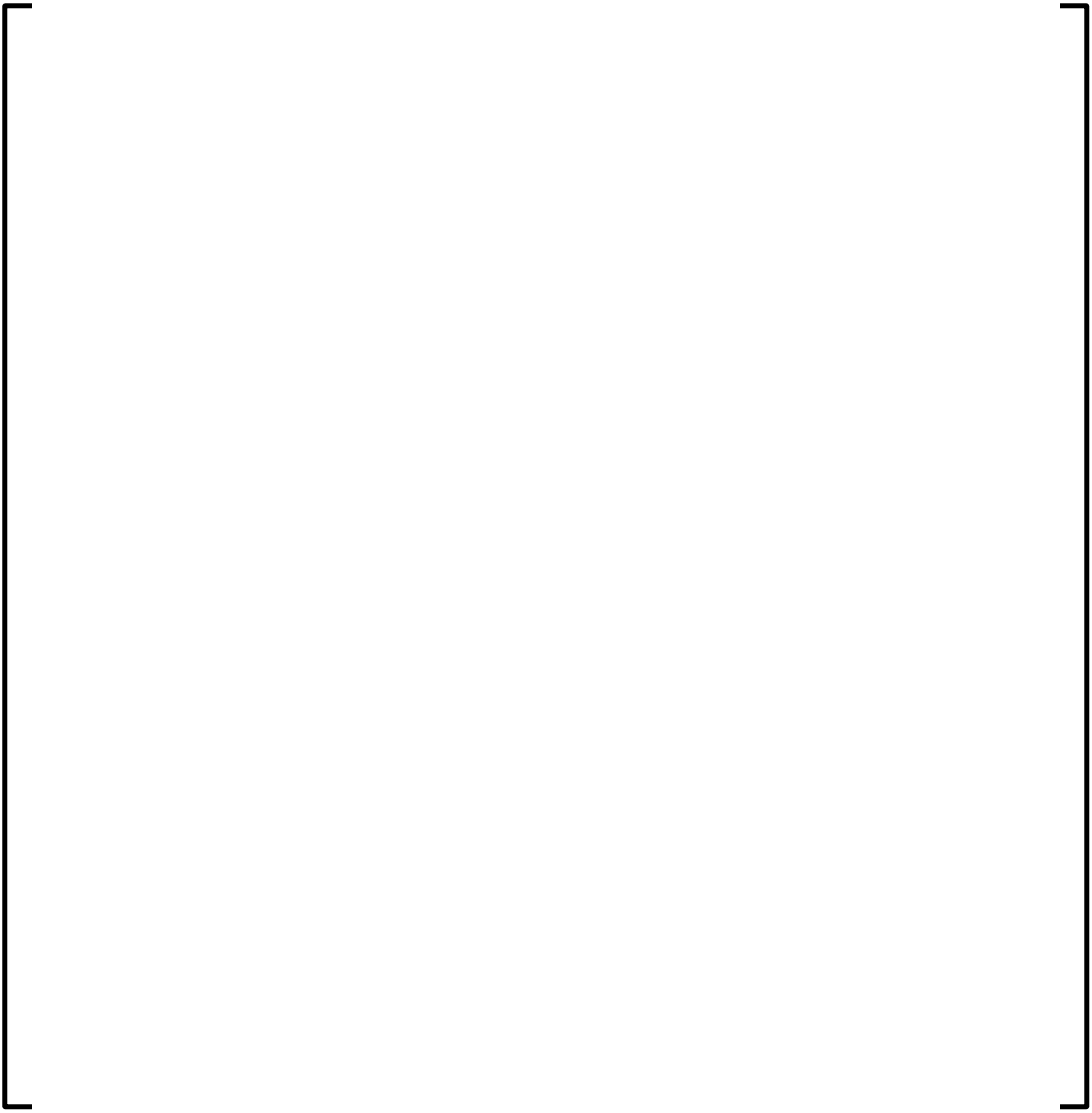
3.1.5 Modifications

3.2 Gap Analysis

3.3 Functional Allocation

3.3.1 General

Figure 3-2: Functional Allocation General Process Flow



3.3.2 The Following are Inputs that are Required to Perform a Thorough Allocation of Each Function and Task:

EPR™ Conceptual Design

The EPR™ conceptual design describes the system performance expectations which are used to determine level of automation for each system. The function and task requirements for each system is found in its corresponding SDRD and SDD.

In addition to tabularizing system functions, each applicable SDD lists the type of control to which functions are allocated and the design basis for the allocation. A description of the personnel role with respect to functions and interfacing with automation is provided in the Concept of Operations (Reference [8]).

Operating Experience

An operating experience review is conducted to identify any Human Factors Engineering (HFE) related safety issues as well as any positive HFE-related experiences. By examining the identified HFE-related safety issues of predecessor designs, negative features from that design can be avoided in the U.S. EPR™ design. Additionally, identified positive features associated with the predecessor designs are retained.

Thus, the OE (Reference [9]) identifies required modifications to functional allocations. If problematic OER issues are identified, then the FA justifies the original analysis of the function, justifies the original human-machine allocation, and identifies solutions such as training, personnel selection, and procedure design that are implemented to address the OER issues.

Vendor Specifications

Systems and components purchased from vendors may be limited on the level automation that can be achieved. Consequently, vendor requirements may dictate the allocation. Therefore, even though the EPR™ conceptual design may have preferred a different allocation, the vendor component may not be able to support certain design decisions. Thus, the FA has to change to be within the limits of the system or component. For example, the selected I&C platform is a key consideration for the allocation of functions.

Selected Digital I&C Platform

The U.S. EPR™ design utilizes diverse digital I&C platforms which results in different HSI. The safety and non-safety platforms are different and have different functional requirements. These differences greatly impact the TA and therefore are considered carefully during FA. More information on the digital I&C platform is found in the Siemens Topical Report (Reference [10]) and the U.S. EPR™ FSAR (Reference [11]). The platform has automation limitations that are considered during functional allocation and task analysis.

3.3.3 Initial Allocation

[ ]

[redacted]

3.3.4 Evaluate FA

[redacted]

3.3.5 Evaluate Operator Performance

[redacted]

4.0 IMPLEMENTATION

4.1 Functional Requirements Analysis

4.1.1 Overview of Implementation

All available plant function documentation is viewed in aggregate for the completion of the entire functional analysis, which includes all operating modes as documented in Chapter 16 of the U.S. EPR™ FSAR (Reference [12]). All PRA and HRA analysis combined with OE documentation are used in various step of the process. It is intended that the output of this process forms a functional branch tree. The FBT can be used to quickly determine the individual components necessary for any safety or non-safety plant function. The FBT also serves to enable coordinated Emergency Procedure Guideline (EPG) development. Although this is not strictly intended to be an iterative process, additions made to the process are analyzed through the same process. Any additions or modifications to FRA consider all items listed in Section 3.1.5.

4.1.1.1 Plant Level Goals

Goals are developed from the plant mission. These represent the existing split of safety functions from economic functions. This is the top of the FBT.

4.1.1.2 Plant Functions

[

]

4.1.1.3 Plant Processes

[

]

4.1.1.4 Plant Diversity

[

]

4.1.1.5 System Process

[

]

4.1.1.6 System Diversity

Diversity and defense-in-depth requirements on a system level are documented. This follows the same process and format of the plant level diversity (4.1.1.4).

4.1.1.7 System Redundancies

System train, division, and channel redundancies that are designed to perform the same function are identified.

4.1.1.8 System Components

System SDDs initially identify all physical components that would create the full accomplishment of the system functions. This includes all mechanical components, control and monitoring capability, and alarm functions. Future iterations of this process include all additions that were input as a result of GA.

4.2 Gap Analysis

[

]

4.3 Functional Allocation

4.3.1 Initial Allocation

Initial allocation is done by the HFE design team. FA from the SDDs is obtained. Comparisons are made between the OL3 EPR™ design and the U.S. EPR™ design to identify FA changes. Similarities and differences are reviewed for applicable necessary changes. Vendor design constraints are considered during this portion of FA.

I&C and System engineers perform reviews of the functional allocation for all design considerations. Changes made to the respective systems are reviewed and approved through a collaborative effort.

4.3.2 Evaluate FA

[

]

Table 4-1: Functional Allocation Considerations

4.3.3 Evaluate Operator Performance

4.4 Interaction with Other HFE Design Process Elements

5.0 SUMMARY REPORT

The FBT that is developed through the entire FRA design process is a living functional document. This is intended for the inclusion of all future modifications to the FRA.

In addition, the results of the outputs describe the level of automation that the U.S. EPR™ reactor uses for the HSI design. The FA details the primary allocations to personnel. Also, operator responsibilities to monitor automatic functions are described. In addition, the allocation considers the actions the operator takes during automation failure. The FBT contains sufficient detail to:

- List allocated functions for U.S. EPR™ design
- List differences and similarities between the predecessor designs and the U.S. EPR™ design
- Explanation of the technical justification for each difference in function automation

The FBT containing FRA/FA is included in the task analysis. This entire structure is presented as one report containing FRA/FA and TA.

A specific objective of the V&V is to validate that the automation design decisions result in interfaces that permit accomplishment of the safety functions within human capabilities and identify as human engineering discrepancies (HEDs) any inappropriate functional allocation observed. This V&V approach verifies that the FA utilizes human strengths and avoids human limitations.

6.0 REFERENCES

1. AREVA NP Document, “Initial Staffing Assumptions for the U.S. EPR.”

2. NUREG-0800, Section 18.0 “Human Factors Engineering”, 2007.

3. NUREG/ CR-3331, “A Method for Allocating Nuclear-Power-Plant Control Functions to Human or Automatic Control.”

4. NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems,” Lawrence Livermore National Laboratory, December, 1994.

5. NUREG-0800 Branch Technical Position 7-19, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems.”

6. AREVA NP Document, “U.S. EPR Task Analysis Implementation Plan.”

7. NUREG-0711, “Human Factors Engineering Program Review Model,” Idaho National Laboratory, 2004.

8. AREVA NP Document, “Concept of Operations: Design of the U.S. EPR Control Rooms.”

9. AREVA NP Document, “U.S. EPR Human Factors Operating Experience Review Implementation Plan.”

10. Siemens Topical Report EMF-2110(NP)(A), “TELEPERM XS: A Digital Reactor Protection System,” Revision 1, May 2000.

11. AREVA NP Document, “Plant Technical Requirements for U.S. EPR.”

12. AREVA NP Document, “U.S. EPR Final Safety Analysis Report.”

13. AREVA NP Document, “U.S. EPR Human Factors Verification and Validation Implementation Plan.”