US-APWR

Functional Requirements Analysis and Function Allocation Implementation Plan

Non-Proprietary Version

May 2014

Revision History

Revision	Date	Page (Section)	Description
0	August 2013	All	Original issued
1	May 2014	Page 2 (Section 2.0), Page 9 (Section 3.1.3, Section 3.2), Page 51 (Section 8.0)	Updated the revision numbers and the issued dates of the references and revised the associated descriptions
		Page 28 (Section 4.6.4.1), Page 49 (Table 7-1)	Editorial correction
		Page 51 (Section 8.0)	Revised the associated descriptions, which were affected by MUAP−08014 withdrawal letter (UAP−HF−14023)

Mitsubishi Heavy Industries, Ltd.
16-5, Konan 2-chome, Minato-ku
Tokyo 108-8215 Japan

Abstract

This document provides the functional requirements analysis (FRA) and the function allocation (FA) implementation plan (IP) for the US Advanced Pressurized Water Reactor (US-APWR). FRA is a top-down analysis, starting with plant goals for safety and power production. High-level functions (critical functions) that are required to achieve these goals are then defined. Success paths (plant configurations responsible for performing the high-level functions) are identified from the plant design to control (maintain or restore) the high-level functions for plant operating modes and conditions, ensuring plant goals are achieved. FA is the allocation of the actions associated with each success path to human, machine (automation), or shared control. FA is performed using human factors engineering (HFE) principles to achieve operator workload levels that minimize periods of operator underload and avoid operator overload. FA is an HFE assessment tool that is applied without consideration of other design factors, such as technology and licensing limitations. The HFE allocations are compared to the US-APWR plant system designs. If there is a difference between the engineering design use of automation and the FA results, human engineering discrepancies (HEDs) are generated and recorded as part of the FA. HEDs are resolved in subsequent HFE program elements through additional analysis, such as the more detailed analysis of workload conducted in the task analysis (TA) HFE program element.

The important human actions (IHAs) and the task performance requirements of IHAs, as identified in the probabilistic risk assessment (PRA), transient and accident analysis (TAA), and defense-in-depth and diversity coping analysis (D3CA), are identified in the human reliability analysis (HRA) HFE program element. The FRA/FA confirms the human allocations for IHAs.

The manual allocations defined by FRA/FA and the actions needed to supervise automation are analyzed in more detail in the TA HFE program element to confirm those allocations and to defined detailed human-system interface (HSI) requirements to support those actions. The workload assessments from FRA/FA are used to establish scenarios for operator crew evaluation in the staffing and qualifications (S&Q) HFE program element.

This IP also describes the requirements for documenting the results of the FRA/FA in a results summary report (ReSR). The ReSR serves to demonstrate that the FRA/FA was conducted in accordance with this IP, which is a requirement for inspections, tests, analyses, and acceptance criteria (ITAAC) closure.

Table of Contents

List of Tables iii
List of Figures iv
Acronyms v

1.0 PURPOSE 1
2.0 SCOPE 2
3.0 METHODOLOGY OVERVIEW 4
3.1 Functional Requirements Analysis and Function Allocation 4
3.1.1 FRA 8
3.1.2 FA 8
3.1.3 IHAs and OER 9
3.1.4 HEDs 9
3.2 Program Interfaces 9
4.0 METHODOLOGY 11
4.1 FRA/FA Structure 11
4.2 FRA/FA Configuration Control 11
4.3 FRA Methodology 11
4.3.1 Plant Goal (Table 4-3, Column 1) 13
4.3.2 High-Level Functions (Table 4-3, Column 2) 13
4.3.3 High-Level Function Decomposition 14
4.3.4 Comparison to Reference Plant Systems 17
4.4 High-Level Function Purpose and Description 18
4.4.1 Purpose of the High-Level Function 18
4.4.2 Condition Indicating High-Level Function Is Needed (Table 4-3, Column 10) 18
4.4.3 Parameters Indicating High-Level Function Is Available (Table 4-3, Column 11) . 19
4.4.4 Parameters Indicating High-Level Function Is Operating (Table 4-3, Column 12) 19
4.4.5 Parameters Indicating High-Level Function Is Achieving Purpose (Table 4-3, Column 13) 19
4.4.6 Parameters Indicating Operation of the High-Level Function Can or Should Be Terminated (Table 4-3, Column 14) 19
4.4.7 References (Table 4-3, Column 15) 19
4.4.8 Time Available (Table 4-3, Column 16) 19
4.4.9 Frequency (Table 4-3, Column 17) 20
4.4.10 Postulated Accidents and Anticipated Operational Occurrences 20
4.5 Predecessor Design 22
4.6 Function Allocation 22
4.6.1 Function Description (Table 4-12, Column A) 22
4.6.2 Load (Table 4-12, Columns 18 and 19) 23
4.6.3 Time Available (Table 4-12, Columns 20 and 21) 27
4.6.4 Rate (Table 4-12, Columns 22 and 23) 28
4.6.5 Action Logic Complexity (Table 4-12, Columns 24 and 25) 29
4.6.6 Decision Types and Complexity (Table 4-12, Columns 26 and 27) 29
4.6.7 Final Allocation (Table 4-12, Columns 28, 29, and 30) 30
4.6.8 FA to DCD Comparison 31
4.7 Operating Experience Review 37
4.7.1 Important Human Actions 39
4.8 Monitoring and Automation Failure 43
4.9 Role of Control Room Staff 43

4.10 Verification ... 43
4.11 Modification Requiring Additional FRA/FA Consideration ... 46
5.0 IMPLEMENTATION TEAM ... 47
5.1 Implementation Team Summary Table ... 47
5.2 Minimum Qualifications ... 47
5.3 Expert Opinion and Judgment for FRA/FA ... 47
6.0 RESULTS SUMMARY REPORT CONTENT ... 48
7.0 NUREG-0711 COMPLIANCE EVALUATION ... 49
7.1 Compliance with NUREG-0711 ... 49
7.2 Justification of Deviations from NUREG-0711 ... 50
8.0 REFERENCES ... 51
DEFINITIONS ... 52

List of Tables

Table 4-1 High-Level Functions 13
Table 4-2 FRA/FA Modes 15
Table 4-3 Functional Requirements Analysis 21
Table 4-4 Load Table Rated Values 27
Table 4-5 Time Available Rated Values 28
Table 4-6 Rate Rated Value 28
Table 4-7 Action Logic Complexity Rated Values 29
Table 4-8 Decision Types and Complexity Rated Values 30
Table 4-9 Allocation Assignment 31
Table 4-10 Power Production Load Evaluation 33
Table 4-11 Safety Load Evaluation 34
Table 4-12 Function Allocation 35
Table 4-13 FRA/FA HEDs 36
Table 4-14 OER Issues 38
Table 4-15 IHA FRA/FA 42
Table 5-1 FRA/FA Implementation Team Summary 47
Table 7-1 Compliance with NUREG-0711 49

List of Figures

Figure 3-1 FRA/FA Analytical Data Flow 4
Figure 3-2 FRA/FA Process Overview 6
Figure 3-3 FRA Hierarchical Structure 7
Figure 4-1 FRA/FA Combined Data Sheet Example 12
Figure 4-2 Aggregate Workload Evaluation Example 24
Figure 4-3 IHA Table Example 41
Figure 4-4 Plant Operations Review Checklist 1 44
Figure 4-5 FRA/FA Team Review Checklist 2 45

Acronyms

AOO	anticipated operational occurrence
BA	boric acid
BAT	boric acid tank
CCW	component cooling water
CCWS	component cooling water system
CET	core exit thermocouple
CS	containment spray
CVCS	chemical and volume control system
DCD	design control document
D3CA	defense-in-depth and diversity coping analysis
ECCS	emergency core cooling system
EFW	emergency feedwater
ESF	engineered safety features
ESW	essential service water
°F	degrees Fahrenheit
FA	function allocation
FCV	flow control valve
FRA	functional requirements analysis
FRG	functional restoration guideline
HED	human engineering discrepancy
HFE	human factors engineering
HRA	human reliability analysis
HSI	human-system interface
I&C	instrumentation and control
IHA	important human action
IEC	International Electrotechnical Commission
IP	implementation plan
ITAAC	inspections, tests, analyses, and acceptance criteria
MS	main steam
MSDV	main steam depressurization valve
MSIV	main steam isolation valve
MSRV	main steam relief valve
LCV	level control valve
LDP	large display panel
MHI	Mitsubishi Heavy Industries, Ltd.
NIS	nuclear instrumentation system
NRC	U.S. Nuclear Regulatory Commission
OER	operating experience review
O-VDU	operational video display unit
PA	postulated accident
PMP	program management plan
PRA	probabilistic risk assessment

PWR	pressurized-water reactor
PZR	pressurizer
QAM	quality assurance manual
RCP	reactor coolant pump
RCS	reactor coolant system
ReSR	results summary report
RHR	residual heat removal
RTS	reactor trip system
RX	reactor
S&Q	staffing and qualifications
SDV	safety depressurization valve
SG	steam generator
SGTR	steam generator tube rupture
SI	safety injection
SIS	safety injection system
SME	subject-matter expert
TA	task analysis
TAA	transient and accident analysis
US, U.S.	United States
US-APWR	U.S. Advanced Pressurized-Water Reactor
VCT	volume control tank
VLV	valve

1.0 PURPOSE

This document provides the functional requirements analysis (FRA) and function allocation (FA) implementation plan (IP) for the US Advanced Pressurized Water Reactor (US-APWR). The purpose of the FRA/FA is to define the plant's high-level functions and the success paths used to control those functions and allocate the success path actions to human and system resources resulting in a role for personnel that takes advantage of human strengths and avoids human limitations.

This IP conforms to the FRA/FA guidance and satisfies the criteria of NUREG-0711, Revision 2, "Human Factors Engineering Program Review Model," issued February 2004, Section 4.4 (Reference 8-1).

2.0 SCOPE

FRA/FA considers high-level functions to address the goals of safety and power production for the US-APWR. A graded approach only addressing changes to a predecessor plant is not being used. Instead, the FRA/FA for the US-APWR uses a detailed analysis of high-level functions. High-level functions are addressed as follows:

- For power production high-level functions, the FRA/FA evaluates the preferred normal success paths used to maintain or control each high-level function

- For safety-related high-level functions, the FRA/FA evaluates the preferred normal success path and the preferred emergency success path used to maintain or control each high-level function

The FRA/FA does not identify contingency actions or alternate success paths that are deployed in the event of failure of the preferred normal or emergency success path(s) (e.g., key components, as identified in Table 4-3) or by failures in auxiliary systems, such as electrical power sources, component cooling water (CCW), or heating, ventilation, and air conditioning). The plant design defines these contingency actions or deployment of alternate success paths as manual. These manual actions are analyzed during the task analysis (TA). Therefore, further evaluation of human factors engineering (HFE) considerations for machine allocation is unwarranted.

FRA/FA does not consider other factors that may affect the allocation, such as technical feasibility, regulatory design compliance issues (e.g., separation and independence), or cost of automation

Where the FRA/FA identifies allocations that are different from those of the US-APWR system design, human engineering discrepancies (HEDs) are documented. HEDs are resolved and tracked to closure using a multidisciplinary team with oversight and final approval by the HFE Expert Panel as described in MUAP-09019, “Human Factors Engineering Program Management Plan,” (hereafter referred to as the “HFE PMP”), Part 1, Section 3.0 (Reference 8-2). HED resolution is an ongoing process that is outside the scope of the FRA/FA HFE program element. The success path allocations, which reflect the HFE allocation results as documented in the FRA/FA results summary report (ReSR), and subsequent HED resolutions, where necessary, are ultimately reflected in the plant system design. If resolution of the FRA/FA generated HEDs change the allocations that may impact the operating crew staffing evaluation, those HEDs are resolved prior to establishing the staffing baseline in the staffing and qualifications (S&Q) HFE program element.

To ensure that the preferred normal and emergency success paths for the US-APWR are identified and allocated, the FRA/FA evaluates the events and human actions from the following documents:

- “Design Control Document for the US-APWR” (hereafter referred to as the “DCD”), Chapter 15, Table 15.0-1, “Postulated Accidents and Anticipated Operational Occurrences” (Reference 8-3)

- Important human actions (IHAs) developed from the probabilistic risk assessment (PRA), MUAP-07030 (Reference 8-5), transient and accident analyses (TAAs) (Chapter 15 of DCD) (Reference 8-3), defense-in-depth and diversity coping analysis

(D3CA), MUAP-07014 (Reference 8-6). The FRA/FA analyzes the events and success path actions that correlate to the IHAs identified to confirm the human allocations assumed in the PRA, TAA, and D3CA.

3.0 METHODOLOGY OVERVIEW

3.1 Functional Requirements Analysis and Function Allocation

Figure 3-1 FRA/FA Analytical Data Flow

Figure 3-2 FRA/FA Process Overview

Figure 3-3 FRA Hierarchical Structure

3.1.1 FRA

3.1.2 FA

3.1.3 IHAs and OER

3.1.4 HEDs

3.2 Program Interfaces

4.0 METHODOLOGY

4.1 FRA/FA Structure

4.2 FRA/FA Configuration Control

4.3 FRA Methodology

Figure 4-1 FRA/FA Combined Data Sheet Example

4.3.1 Plant Goal (Table 4-3, Column 1)

4.3.2 High-Level Functions (Table 4-3, Column 2)

Table 4-1 High-Level Functions

4.3.2.1 Safety High-Level Functions

4.3.2.2 Power Production High-Level Functions

4.3.3 High-Level Function Decomposition

4.3.3.1 Plant Mode (Table 4-3, Column 3)

Table 4-2 FRA/FA Modes

4.3.3.2 Condition (Table 4-3, Column 4)

4.3.3.3 Purpose of the Success Path (Table 4-3, Column 5)

4.3.3.4 Sub-function (Table 4-3, Column 6)

4.3.3.5 System (Table 4-3, Column 7)

4.3.3.6 Key Components (Table 4-3, Column 8)

4.3.3.7 Action (Table 4-3, Column 9)

4.3.4 Comparison to Reference Plant Systems

4.4 High-Level Function Purpose and Description

4.4.1 Purpose of the High-Level Function

4.4.2 Condition Indicating High-Level Function Is Needed (Table 4-3, Column 10)

4.4.3 Parameters Indicating High-Level Function Is Available (Table 4-3, Column 11)

4.4.4 Parameters Indicating High-Level Function Is Operating (Table 4-3, Column 12)

4.4.5 Parameters Indicating High-Level Function Is Achieving Purpose (Table 4-3, Column 13)

4.4.6 Parameters Indicating Operation of the High-Level Function Can or Should Be Terminated (Table 4-3, Column 14)

4.4.7 References (Table 4-3, Column 15)

4.4.8 Time Available (Table 4-3, Column 16)

4.4.9 Frequency (Table 4-3, Column 17)

4.4.10 Postulated Accidents and Anticipated Operational Occurrences

Table 4-3 Functional Requirements Analysis

4.5 Predecessor Design

4.6 Function Allocation

4.6.1 Function Description (Table 4-12, Column A)

4.6.2 Load (Table 4-12, Columns 18 and 19)

4.6.2.1 Aggregate Load Evaluations

Figure 4-2 Aggregate Workload Evaluation Example

4.6.2.2 Load Rated Value (Table 4-12, Column 18)

Table 4-4 Load Table Rated Values

4.6.2.3 Load Explanation Rated Value Basis (Table 4-12, Column 19)

4.6.3 Time Available (Table 4-12, Columns 20 and 21)

4.6.3.1 Time Available

4.6.3.2 Time Available Rated Values (Table 4-3 Column 20)

Table 4-5 Time Available Rated Values

4.6.3.3 Time Available Rated Value Basis (Table 4-12, Column 21)

4.6.4 Rate (Table 4-12, Columns 22 and 23)

4.6.4.1 Rate Rated Value (Table 4-12, Column 22)

Table 4-6 Rate Rated Value

4.6.4.2 Rate Rated Value Basis (Table 4-12, Column 23)

4.6.5 Action Logic Complexity (Table 4-12, Columns 24 and 25)

4.6.5.1 Action Logic Complexity Rated Value (Table 4-12, Column 24)

Table 4-7 Action Logic Complexity Rated Values

4.6.5.2 Action Logic Complexity Rated Value Basis (Table 4-12, Column 25)

4.6.6 Decision Types and Complexity (Table 4-12, Columns 26 and 27)

4.6.6.1 Decision Types and Complexity Rated Value (Table 4-12, Columns 26)

Table 4-8 Decision Types and Complexity Rated Values

4.6.6.2 Decision Types and Complexity Rated Value Basis (Table 4-12, Column 27)

4.6.7 Final Allocation (Table 4-12, Columns 28, 29, and 30)

Table 4-9 Allocation Assignment

4.6.8 FA to DCD Comparison

4.6.8.1 Initial Assignment (Table 4-12, Column 31)

4.6.8.2 HED (Yes/No) (Table 4-12, Column 32)

4.6.8.3 DCD Reference for Initial Allocation (Table 4-12, Column 33)

Table 4-10 Power Production Load Evaluation

Table 4-11 Safety Load Evaluation

Table 4-12 Function Allocation

Table 4-13 FRA/FA HEDs

4.7 Operating Experience Review

Table 4-14 OER Issues

4.7.1 Important Human Actions

4.7.1.1 Identify IHAs

4.7.1.2 Identify Success Paths Associated with the IHA

4.7.1.3 Categorize the IHA Events

4.7.1.4 Ensure IHA Allocated to Human

Figure 4-3 IHA Table Example

Table 4-15 IHA FRA/FA

4.8 Monitoring and Automation Failure

4.9 Role of Control Room Staff

4.10 Verification

Figure 4-4 Plant Operations Review Checklist 1

Figure 4-5 FRA/FA Team Review Checklist 2

4.11 Modification Requiring Additional FRA/FA Consideration

5.0 IMPLEMENTATION TEAM

5.1 Implementation Team Summary Table

The SMEs who conduct the FRA/FA program element are described in Section 4 above and summarized in Table 5-1 below.

Table 5-1 FRA/FA Implementation Team Summary

Implementation Activity	Section	Subject Matter Expert
Performer for FRA/FA Participate in the review of FRA/FA ReSR (Checklist 1). FRA/FA Team Member	4.3, 4.4, 4.6, 4.7, 4.10	Plant Operations
FRA/FA Team Member	4.10	HFE
FRA/FA Team Member	4.10	I&C Engineering
FRA/FA Team Member Provide knowledge of the purpose, operating characteristics, and technical specifications of major plant systems. Perform comparison of FA design allocation (Table 4-12). Participate in the review of FRA/FA ReSR.	4.3, 4.4, 4.6, 4.7, 4.10	Systems Engineering
FRA/FA Team Member Participate in the review of FRA/FA ReSR.	4.7, 4.10	PRA
FRA/FA Team Member	4.7, 4.10	Safety System Engineering

The SME qualifications are defined in the HFE PMP (Reference 8-2).

5.2 Minimum Qualifications

The HFE PMP (Reference 8-2) provides the minimum qualifications for expertise used on the FRA/FA team.

5.3 Expert Opinion and Judgment for FRA/FA

Development of FRA/FA data sheets proceeds as follows:

- The plant operations SME's opinion is used in the development of FRA/FA data sheets (Section 4.0).
- The data, including any opinions, are reviewed by an independent SME (Section 4.10). Resolution is reached between these two individuals (Section 4.10). Differences in opinion are resolved by the engineering manager.
- A final review with resolution of concerns is performed by the FRA/FA team. This team has a diverse background, as indicated by Section 5.1 above (Section 4.10).

6.0 RESULTS SUMMARY REPORT CONTENT

All results of the FRA/FA program element are compiled in a ReSR. This report is used to demonstrate that the FRA/FA have been performed in accordance with this IP. The FRA/FA IP documented through this ReSR is a requirement of the ITAAC closure defined in the US-APWR DCD, Tier 1.

The FRA/FA ReSR includes the following:

- Each implementation team member's name and the SME position they fulfill.
- The FRA/FA results overview, which includes the principal findings of the HFE program element.
- The FRA/FA execution results, which include all details that demonstrate compliance with the methodology section of this IP. This includes data sheets with, as a minimum, the attributes contained in the following tables:
  - Table 4-3, "Functional Requirements Analysis"
  - Table 4-10, "Power Production Load Evaluation"
  - Table 4-11, "Safety Load Evaluation"
  - Table 4-12, "Function Allocation"
  - Table 4-13, "FRA/FA HEDs"
  - Table 4-14, "OER Issues"
  - Table 4-15, "IHA FRA/FA"
- A conclusion that the FRA/FA program element has been conducted in accordance with the FRA/FA IP and that (with consideration of resolutions for any HEDs generated by FRA/FA) the success path actions have been allocated appropriately considering the strengths and weaknesses of human and machine.

7.0 NUREG-0711 COMPLIANCE EVALUATION

7.1 Compliance with NUREG-0711

Table 7-1 indicates where in this IP each NUREG-0711, Revision 2 (Reference 8-1), criterion for FRA/FA is addressed.

Table 7-1 Compliance with NUREG-0711

Review Criteria Stated in NUREG-0711, Rev. 2	FRA/FA IP Section No. and paragraph
4.4 Review Criteria	
(1) Functional requirements analysis and function allocation should be performed using a structured, documented methodology reflecting HFE principles. An example functional allocation process and considerations is shown in Figure 4.1. The functional requirements analysis and function allocation may be graded based on: • the degree to which the functions of the new design differ from those of the predecessor • the extent to which difficulties related to plant functions were identified in the plant's operating experience and will be addressed in the new design.	Section 3.1; Figure 3-1; Figure 3-2; Figure 3-3; Sections 4.1, 4.3, 4.4, 4.6 Section 4.3.4; Section 4.5 Section 4.7
(2) The functional requirements analysis and function allocation should be kept current over the life cycle of design development and held until decommissioning so that it can be used as a design basis when modifications are considered. Control functions should be re-allocated in an iterative manner, in response to developing design specifics, operating experience, and the outcomes of ongoing analyses and trade studies.	Section 4.2, paragraph 2; Section 4.11
(3) A description of the functions and systems should be provided along with a comparison to the reference plants/systems, i.e., the previous plants or plant systems on which the new system is based. This description should identify differences that exist between the proposed and reference plants/systems. Safety functions (e.g., reactivity control) include functions needed to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public. For each safety function, the set of plant system configurations or success paths that are responsible for or capable of carrying out the function should be clearly defined. Function decomposition should start at “top-level” functions where a very general picture of major functions is described, and continue to lower levels until a specific critical end-item requirement emerges (e.g., a piece of equipment, software, or HA). The functional decomposition should address the following levels • high-level functions [e.g., maintain reactor coolant system (RCS) integrity] and critical safety functions (e.g., maintain RCS pressure control) • specific plant systems and components	Section 3.1; Section 4.3 and all of its subsections; Table 4-3
(4) A description should be provided for each high-level function which includes: • purpose of the high-level function • conditions that indicate that the high-level function is needed • parameters that indicate that the high-level function is available • parameters that indicate the high-level function is operating (e.g., flow indication) • parameters that indicate the high-level function is achieving its purpose (e.g., reactor vessel level returning to normal) • parameters that indicate that operation of the high-level function can or should be terminated Note that parameters may be described qualitatively (e.g., high or low). Specific data values or setpoints are not necessary at this stage.	Section 4.4; Table 4-3 Section 4.4.1 Section 4.4.2 Section 4.4.3 Section 4.4.4 Section 4.4.5 Section 4.4.6
(5) The technical basis for modifications to high-level functions in the new design (compared to the predecessor design) should be documented.	Section 4.5

Review Criteria Stated in NUREG-0711, Rev. 2	FRA/FA IP Section No. and paragraph
(6) The technical basis for all function allocations should be documented; including the allocation criteria, rationale, and analyses method. The technical basis for functional allocation can be any one or combination of the evaluation factors (see Fig 4.1). For example, the performance demands to successfully achieve the function, such as degree of sensitivity needed, precision, time, or frequency of response, may be so stringent that it would be difficult or error prone for personnel to accomplish. This would establish a basis for automation (assuming acceptability of other factors, such as technical feasibility or cost).	Section 4.6 Table 4-10; Table4-11; Table 4-12
(7) The OER should be used to identify modifications to function allocations, if necessary. If problematic OER issues are identified, then an analysis should be performed to (a) justify the original analysis of the function, (b) justify the original human-machine allocation, and (c) identify solutions such as training, personnel selection, and procedure design that will be implemented to address the OER issues.	Section 4.7; Table 4-14
(8) The allocation analysis should consider not only the primary allocations to personnel, but also their responsibilities to monitor automatic functions and to assume manual control in the event of an automatic system failure.	Section 4.8
(9) A description of the integrated personnel role across functions and systems should be provided in terms of personnel responsibility and level of automation.	Section 4.6, Table 4-12; Section 4.9
(10) The functional requirements analysis and function allocation should be verified: • all the high-level functions necessary for the achievement of safe operation are identified. • all requirements of each high-level function are identified. • the allocations of functions result in a coherent role for plant personnel	Section 4.10
(11) When the analyses address plant modifications, the following considerations should also be addressed: • Functional requirements analyses for modifications that are likely to change existing safety functions, introduce new functions for systems supporting safety functions, or involve unclear functional requirements that may be important to safety. The functional requirements analysis should address new functions resulting from changes in the degree of integration between plant systems. For example, installing higher-level automation may bring systems that were formerly controlled separately under a single controller. Also, the modifications may change the degree to which different plant systems share common resources (e.g., power sources, cooling water, and data-transmission buses). These may be important in diagnosing malfunctions or planning responses. The functional requirements analyses should be revised and updated to reflect the modification; the scope of the analyses may be restricted to functions related to the modification. • Function allocation analyses for modifications that are likely to change the allocation between personnel and plant systems of functions important to safety. The analyses should be revised and updated to reflect the modification; their scope may be restricted to functions involving the modification. • A change in an operator's role due to a modification should be examined within the context of its effects on the operator's overall responsibilities. Increases in certain task demands may affect the ability of the operator to carry out others that are risk-important	Section 4.2; Section 4.11

7.2 Justification of Deviations from NUREG-0711

NUREG-0711, Section 4.4, Criterion (8), actions to take manual control following automation failure, are not addressed in FRA/FA. These actions are analyzed in TA.

8.0 REFERENCES

8-1 Human Factors Engineering Program Review Model, NUREG-0711, Revision 2, U.S. Nuclear Regulatory Commission, February 2004

8-2 Human Factors Engineering Program Management Plan, MUAP-09019, Revision 4, MHI, May 2014

8-3 Design Control Document for the US-APWR, Revision 4, MHI, August 2013

8-4 Human Reliability Analysis Implementation Plan, MUAP-13014, Revision 1, MHI, May 2014

8-5 US-APWR Probabilistic Risk Assessment, MUAP-07030, Revision 3, MHI, June 2011

8-6 Defense-in-Depth and Diversity Coping Analysis, MUAP-07014, Revision 6, MHI, September 2013

8-7 Design for Control Rooms of Nuclear Power Plants, IEC 60964, Edition 2, International Electrotechnical Commission, 2009

8-8 Nuclear Power Plants – Design of Control Rooms – Functional Analysis and Assignment, IEC 61839, Edition 1, International Electrotechnical Commission, 2000

8-9 NUREG-0800, Chapter 18, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition – Human Factors Engineering," Revision 2, March 2007

8-10 Deleted

8-11 Operating Experience Review Implementation Plan, MUAP-13005, Revision 1, MHI, May 2014

8-12 Human-System Interface Design Implementation Plan, MUAP-10009, Revision 4, MHI, May 2014

8-13 Task Analysis Implementation Plan, MUAP-13009, Revision 1, MHI, May 2014

8-14 Quality Assurance Manual − Nuclear Safety Related for Non ASME Code Job, 2CAS-20130004, Revision 0, MHI, November 2013

8-15 Human Factors Verification and Validation Implementation Plan, MUAP-10012, Revision 4, MHI, May 2014

DEFINITIONS

Action – Action is the operation of system components or systems to control required parameter(s) at an acceptable state and maintain that state so the high-level function is not challenged or is no longer challenged (e.g., increase flow, decrease reactivity, reduce pressure, initiate SIS).

Complexity of Action Logic – Complexity of action logic identifies potential error-likely situations. Where multiple parameters and complex analysis are required to complete actions, human performance may not be consistent due to differences in mental capabilities.

Component – An individual piece of equipment having a unique function, such as a pump, VLV, or vessel.

Decision Types and Complexity – The decision types and complexity function separates those decisions that cannot be performed by machines from those that can. Where parameters monitored or criteria for evaluation are not well defined, requiring human judgment, the decision type is considered to be ill-structured.

High-Level Function – A process or group of processes that must be maintained to achieve the ultimate purpose of the plant, which is to generate electricity (power production goal) and prevent uncontrolled release of radiation (safety goal). The term "high-level function" from NUREG-0711 (Reference 8-1) and the US-APWR FRA/FA is interchangeable with "critical function" used in IEC 60964 (Reference 8-7).

Load – Load analysis identifies mental and physical capacity for humans supervising (including monitoring automatic functions) and/or manually controlling success paths to maintain a specific high-level function while concurrently supervising or controlling other success paths to concurrently maintain all other high-level functions. Load is evaluated for each high-level function during three defined plant modes.

Plant Goal – Goals are at the top of the hierarchy for FRA. These goals are similar to IEC 61839 (Reference 8-8) goals.

Rate – Rate is a relationship between the load and time available; it relates the time needed to complete the success path to the number of actions that must be taken for control of a specific success path and the concurrent control/supervision of all high-level functions in temporal proximity. Due to physical limitations, humans can perform a limited number of functions over a given time period.

Sub-function – Sub-functions are those functions that serve to support higher-level objectives and are often defined in terms of a boundary or entity that is important to plant integrity and the prevention of the release of radioactive materials. A typical sub-function is "reactivity control." A high-level objective, such as preventing the release of radioactive material to the environment, is one that designers strive to achieve through the design of the plant and that plant operators strive to achieve through proper operation of the plant. The function is often described without reference to specific plant systems and components or the level of human and machine intervention that is needed to carry out this action. Functions are often accomplished through some combination of lower-level functions, such as "reactor trip." The process of manipulating lower-level functions to satisfy a higher-level function is defined here as a control function. During FA, the control function is assigned to human and machine elements.

Sub-function is the highest level of success path decomposition. The sub-function either maintains or mitigates the loss of the high-level function under the mode and condition specified. Sub-function is subsequently the highest level in the definition of the success path, which is used to restore, control or maintain the high-level function.

Success Path – The aggregate of sub-functions, plant systems, key components, and the actions to be performed to maintain or restore a high-level function.

System – An integrated collection of plant equipment or components working together to accomplish one or more objectives.

Time Available – The elapsed time (seconds, minutes, hours, or days) from when a parameter deviates from its preferred value to when a success path action must be completed to protect the high-level function.