Functional Requirements Analysis and Function Allocation Implementation Plan

Revision 2

Non-Proprietary

January 2018

REVISION HISTORY

Revision	Date	Page	Description
0	December 2014	All	First Issue
1	March 2017	17 (4.3.3)	Description for the normal and emergency success paths information are revised R_383-8458(113)
		29 (6)	Description for FRA/FA ReSR are revised R_351-8381(60)
		19, 30 (Overall)	Editorial corrections. (typos, references)
2	January 2018	14 (4.3.3)	Description for APR1400 HSI design related are revised R_553-9084(137R)
		30 (7.1)	Revision No. and Issue Year/Month updated

ABSTRACT

This document provides the implementation plan (IP) for the human factors engineering (HFE) functional requirements analysis (FRA) and functional allocation (FA) program element (PE), which is one of twelve PEs within the Advanced Power Reactor 1400 (APR1400) HFE program. This IP governs the technical activities conducted in the FRA/FA PE by defining its scope, methodology, products, and the qualifications of the personnel who conduct the PE.

The primary purposes of the FRA/FA PE are to:

1. Define the critical functions that have to be accomplished to the plant's safety goals (critical safety functions [CSF]) and the power production goals (critical power production functions [CPPF]).

2. Define the preferred normal and emergency success paths that are used to maintain or restore the critical functions and delineate the hierarchical composition of the success paths through plant systems, processes components and control actions.

3. Provide a framework for determining the roles and responsibilities of personnel and automation.

4. Allocate the actions associated with each success path to a level of automation ranging from manual to fully automatic.

This plan describes the APR1400 approach to FRA/FA, and provides reasonable assurance that HFE principles are systematically incorporated into the APR1400 design. This plan provides the process used in achieving each of the four purposes described above, including the decomposition of success paths and the evaluation of those success paths to identify attributes of system/human orientation used in the FA process. In addition, this plan describes how FRA/FA PE results are used in the HFE task analysis (TA) PE, the HFE staffing and qualifications (S&Q) PE, and the HFE human systems interface design (HD) PE.

As an evolutionary pressurized water reactor (PWR) design, APR1400 has been developed by incorporating the success and experience accrued from prior generations of similar large two-loop PWRs and a predecessor design. In particular, the CSF approach, defined in the CEN-152, "Combustion Engineering Emergency Procedure Guidelines," has proved to be a sufficient and effective framework for emergency operations and maintaining plant safety.

The evolutionary design improvements of the APR1400 relative to the predecessor design have added or modified some plant processes, systems and components. During the FRA, the APR1400 design is analyzed using the structured top down methodology described in this IP to define functions that must be carried out to meet the APR1400's safety goals and power production goals. The FRA process described in this IP was also used for the predecessor design. The success paths, including the success path control actions needed to maintain or restore those functions for normal, abnormal and emergency plant conditions are identified.

The FA is the process of allocating the success path control actions identified in the FRA, to system and/or human action. A set of factors that influence the choice between system and human adapted from

NUREG/CR-3331 are used to make the allocation by characterizing each control action relative to the factors. Based on the characteristics, one of a set of discrete automation configurations, ranging from manual to fully automatic, is selected. If the selected automation configuration is not consistent with the APR1400 design, a human engineering discrepancy (HED) is created for resolution in subsequent elements of the HFE program.

FRA/FA is a one-time, non-recurring HFE PE whose closure is marked by the issuance of the FRA/FA results summary report (ReSR). However, the functional requirement and function allocation analyses are iterative in that HEDs generated by other HFE PEs are evaluated for any potential changes needed in those analyses. Similarly, APR1400 plant design changes are evaluated for their impact to the output of all HFE PEs, including the output of the FRA/FA PE. HEDs are generated as needed. Therefore, any changes as a result of analyses that may be needed after completing the FRA/FA ReSR are managed through the HED resolution process. HEDs that affect FRA/FA outputs are resolved prior to completing the HD, which establishes the APR1400 HSI design for verification and validation (V&V).

After completion of the V&V, site-specific changes, including any required FRA/FA output changes, are managed within the APR1400 HFE design implementation (DI) PE, which is a recurring program element for each plant. The DI PE also provides reasonable assurance that all HEDs are closed.

Section 1 of this document defines the FRA/FA purpose. Section 2 defines the scope. Section 3 provides a methodology overview. Section 4 provides the details of the methodology, including the format and content of each FRA/FA output product. Section 5 establishes the qualification requirements for the FRA/FA implementation team. Section 6 defines the required content of the FRA/FA ReSR, which demonstrates that the FRA/FA was conducted in accordance with this IP. Appendix A demonstrates conformance of this IP to the NUREG-0711 review criteria for the FRA/FA.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS AND ABBREVIATIONS

AAM	automatic-AND-manual
AOM	automatic-OR-manual
APR1400	Advanced Power Reactor 1400
Auto	automatic
AXM	automatic-XOR-manual
CESSAR-DC	Combustion Engineering Standard Safety Analysis Report-Design Certification
COL	combined license
CPPF	critical power production function
CSF	critical safety function
D3CA	diversity and defense-in-depth coping analysis
CVCS	chemical and volume control system
DCD	design control document
DPS	diverse protection system
ESF	engineered safety feature
FA	function allocation
FDT	function definition table
FRA	functional requirements analysis
FRG	functional recovery guidelines
HD	HSI design
HED	human engineering discrepancy
HFE	human factors engineering
HSI	human-system interface
IHA	important human action
IP	implementation plan
IR	independent review
ITS	issue tracking system
KEPCO	Korea Electric Power Corporation
KHNP	Korea Hydro & Nuclear Power Co., Ltd.
MCR	main control room
OER	operating experience review
PAR	passive autocatalytic recombiner.
PE	program element
PP	program plan
PRA	probabilistic risk assessment
PWR	pressurized water reactor

PZR	pressurizer
RCS	reactor coolant system
ReSR	results summary report
SG	steam generator
S&Q	staffing and qualifications
SME	subject matter expert
SSC	structure, system, and component
TA	task analysis
TAA	transient and accident analysis
TIHA	treatment of important human actions
TS	trade secret
V&V	verification and validation
xfmr	transformer

Page intentionally blank

1. PURPOSE

This document provides the implementation plan (IP) for the human factors engineering (HFE) functional requirements analysis (FRA) and function allocation (FA) program element (PE), which is one of 12 PEs within the Advanced Power Reactor 1400 (APR1400) HFE program. This IP governs the technical activities conducted within the FRA/FA PE by defining its scope, methodology, products, and the qualifications of the personnel who conduct the PE.

The FRA is performed to:

- Define the critical functions that have to be accomplished to meet the plant's safety goals (critical safety functions [CSF]) and the power production goals (critical power production functions [CPPF]).
- Define the preferred normal and emergency success paths that are used to maintain or restore the critical functions and delineate the hierarchical composition of the success paths through plant systems, processes components and control actions.
- Provide a framework for determining the roles and responsibilities of personnel and automation.

The FA is performed to:

- Allocate the actions associated with each success path to a level of automation ranging from manual to fully automatic.

The FRA/FA supports the HFE task analysis (TA) PE, the human-systems interface (HSI) design (HD), and staffing and qualifications (S&Q) PE. The allocations to humans for all important human actions (IHAs) are confirmed at a high level in FRA/FA and again through additional analysis in the TA and S&Q PEs. The HD PE defines the HSI design for those IHAs.

This IP provides reasonable assurance that HFE issues are systematically incorporated in the APR1400 design, particularly plant safety functions. This IP is provided to satisfy the process requirements of the HFE Program Plan (PP) for the APR1400 (Reference 1).

This IP provides a methodology that enables the design engineers to analyze and describe the functions that must be provided by the automation system in conjunction with operator-performed functions and also addresses the FRA/FA review criteria of NUREG-0711, rev.3 (Reference 7). Appendix A shows the conformance of the FRA/FA PE with NUREG-0711 review criteria.

2. SCOPE

The scope of FRA/FA includes all of the functions needed to achieve plant safety and power production goals. The preferred success paths for CSFs and CPPFs are specified considering both safety class paths and non-safety class structures systems and components (SSCs) for emergency success paths and normal success paths respectively. All IHAs identified in the treatment of important human actions (TIHA) PE that are needed to implement the preferred success paths are analyzed to confirm the allocation is correct.

The FRA/FA considers all operating modes (modes 1 through 6) for normal, abnormal and emergency conditions. The FRA/FA does not consider alternate success paths that may be deployed to accommodate preferred success path failure and does not consider failures in auxiliary systems (e.g., electrical power sources, component cooling water, heating, ventilation, and air conditioning) that may adversely affect preferred success paths. Contingency actions or deployments of alternate success paths are defined by the plant design; any manual actions are analyzed during the TA PE. Severe accident conditions are not examined since the results of their extensive analysis are reported separately. CPPF success paths that are plant specific (e.g., paths using the switchyard, ultimate heat sink) are specified only to the system level. All references to success paths in this IP are the preferred success paths unless stated otherwise.

The reviewed and approved FRA/FA results summary report (ReSR) of the predecessor design System 80+, issued as NPX80-IC-RR790-02, “Human Factors Evaluation and Allocation of System 80+ Functions” (Reference 2) is used as input in the FRA/FA and as such is within the scope of the analysis.

The FRA/FA results are documented in the FRA/FA ReSR. Changes to the FRA/FA results needed after completion of the FRA/FA ReSR are documented through the design change process or HED process.

3. METHODOLOGY OVERVIEW

3.1 General Approach

TS

TS

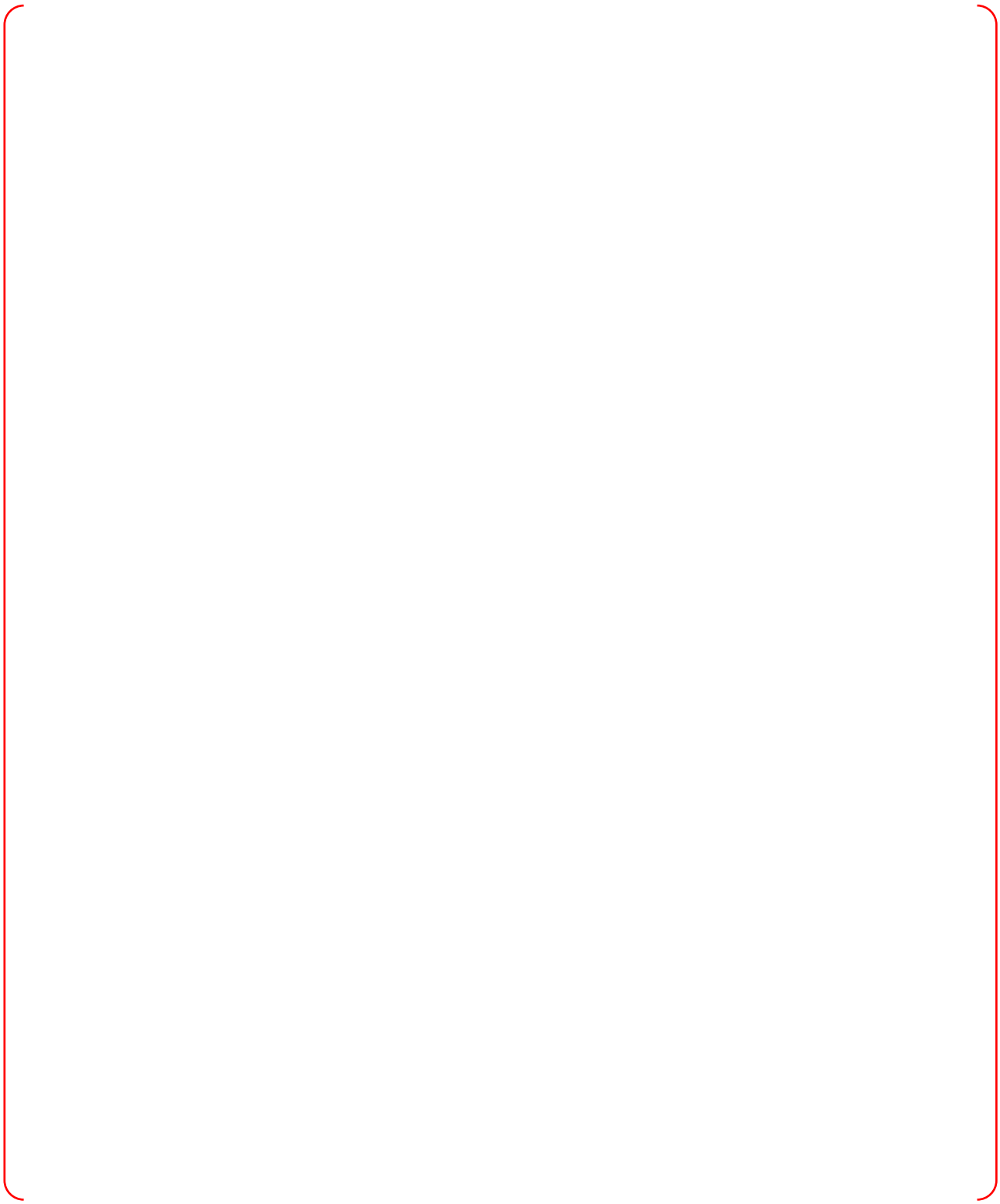

Figure 3-1 FRA/FA Process Flow Diagram

3.2 FRA Process Summary

3.2.1 Identification of Critical Safety Functions

TS

TS

Table 3-1 CSF Comparison

3.2.2 Identification of Critical Power Production Functions

TS

3.2.3 Specification of Functional Hierarchy and Requirements

TS

TS

3.3 Function Allocation Process Summary

TS

3.3.1 Analyze Function Characteristics

TS

3.3.2 Selection of Automation Configuration

TS

3.3.3 Independent review

TS

3.4 Interfaces

3.4.1 Operating Experience Review Program Element

TS

3.4.2 Treatment of Important Human Actions Program Element

TS

3.4.3 Task Analysis Program Element

TS

[ ]

3.4.4 Staffing and Qualifications Program Element

TS

[ ]

3.4.5 Human-System Interface Design

TS

[ ]

3.4.6 Plant Design

TS

[ ]

4. IMPLEMENTATION

4.1 Methodology Structure and Documentation

TS

4.2 Analysis Updates (Iterations)

TS

TS

4.3 Functional Hierarchy

TS

TS

TS

Figure 4-1 Upper Functional Hierarchy

Figure 4-2 illustrates the concept of the success path hierarchy for the safety goal below the reactor control CSF. There are multiple success paths to maintain reactivity control. Each success path is broken down into processes, systems, components and control actions.

TS

Figure 4-2 Lower Functional Hierarchy

4.3.1 Identification Critical Safety Functions

TS

TS

4.3.2 Identification of Power Production Functions

TS

4.3.3 Specification of Functional Hierarchy, Success Paths, and Requirements

TS

TS

Table 4-1 Example of a Function Definition Table for a Critical Function

TS

TS

TS

TS

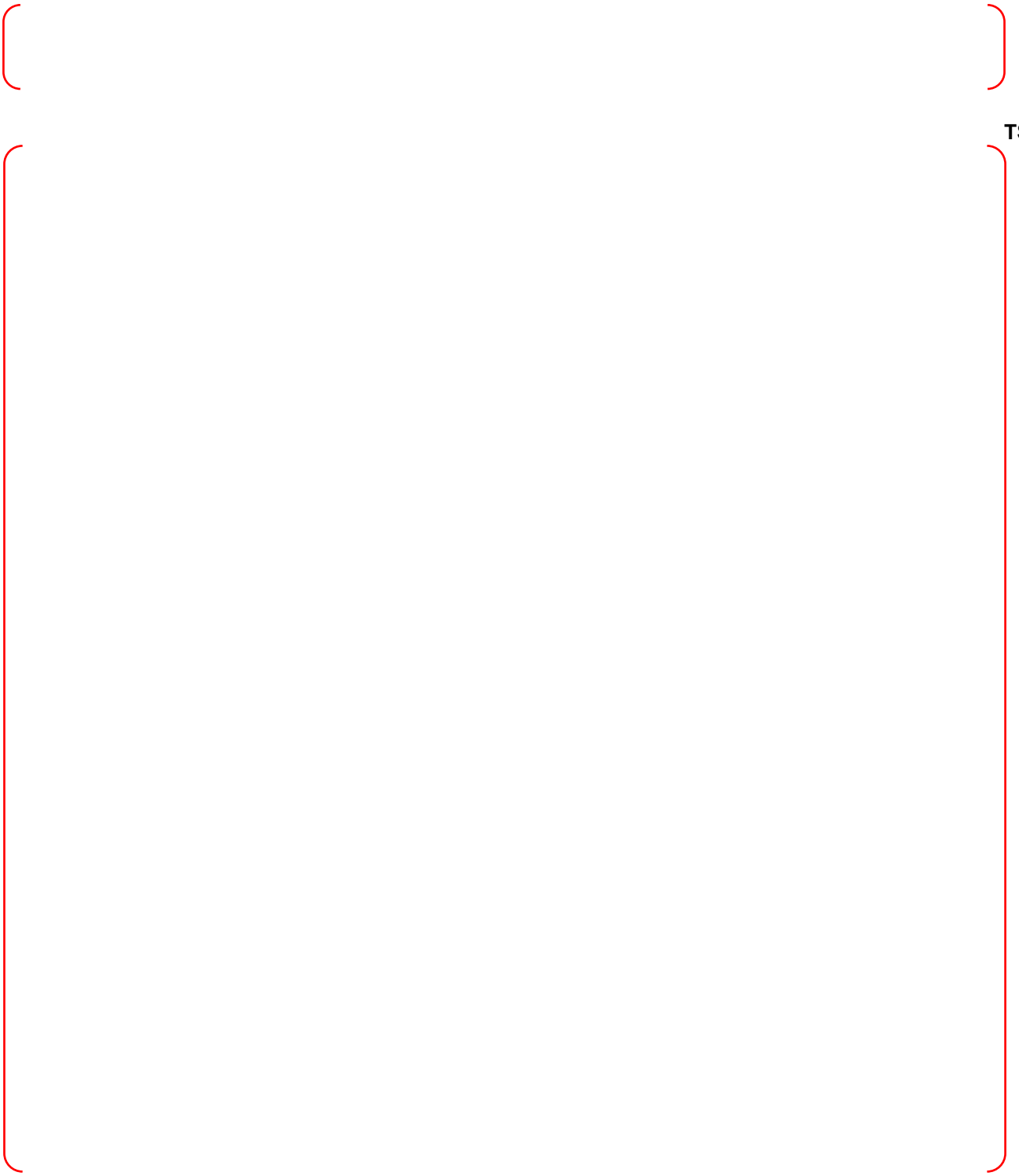

Figure 4-3 Success Path Resource Tree

TS

TS

Table 4-2 Success Path Comparison

TS

TS

TS

[redacted]

4.4 Functional Requirements

TS

[redacted]

4.5 Allocation of Functions

TS

[redacted]

TS

TS

TS

Figure 4-4 Allocation Selection Process

TS

TS

TS

TS

Table 4-3 Allocation Table

TS

TS

4.6 Additional Considerations

TS

TS

4.7 Overall Personnel Roles

TS

4.8 Independent Review

TS

TS

5. IMPLEMENTATION TEAM

TS

6. RESULTS SUMMARY REPORT

The results of the FRA/FA are documented in the ReSR, either directly or through reference to the FDT database. The ReSR demonstrates that the FRA/FA were conducted in accordance with this IP.

In addition to referencing the FDTs, the FRA/FA includes the following:

- The FRA/FA results overview, which describes the principal findings of the HFE program element, including confirmation of IHAs and an overview of any HEDs
- Each FRA/FA team member's name, the SME position fulfilled, and the types of FRA/FA outputs generated by that team member
- A detailed description of any resulting HEDs identifying conflicts between FRA/FA results and the APR1400 plant design.
- An explanation of the methodology used to define the safety functions
- The set of safety functions for the facility
- An explanation of the methodology used to allocate functions and the final set of allocations
- The technical basis for modifying high-level functions of predecessor design in the new design
- A complete set of functional requirements necessary to satisfy the plant goals
- Identification of how personnel and automatic systems perform the functions
- The technical basis for all function allocations

The FRA/FA is a one-time non-recurring HFE PE whose closure is marked by the FRA/FA ReSR. However, the analyses conducted within FRA/FA are iterative, in that HEDs generated by other HFE PEs are evaluated for any potential changes needed in those analyses. Similarly, plant design changes are evaluated for their impact to the output of all HFE PEs, including the output of the FRA/FA; HEDs are generated as needed. Therefore, any FRA/FA analyses changes that may be needed after completing the FRA/FA ReSR are managed through the HED resolution process. HEDs that affect FRA/FA outputs are resolved prior to completing the HD PE, which establishes the APR1400 HSI design for verification and validation (V&V).

After completion of V&V, site-specific changes, including any required FRA/FA output changes, are managed within the DI PE, which is a recurring PE for each plant. DI also ensures that all HEDs are closed.

7. REFERENCES

1. APR1400-E-I-NR-14001-P, “Human Factors Engineering Program Plan,” Rev.2, KHNP, January 2018.
2. NPX80-IC-RR790-02, Human Factors Evaluation and Allocation of System 80+ Functions, Rev.2 Combustion Engineering, Inc., February 1994.
3. CEN152, Combustion Engineering Emergency Procedure Guidelines (CE EPGs), Rev 6, December 2012.
4. APR1400-K-X-FS-14002, "APR1400 Design Control Document Tier 2,” Rev.2, KHNP, January 2018.
5. Combustion Engineering Standard Safety Analysis Report-Design Certification (CESSAR-DC), Amendment W, June 1994.
6. NUREG/CR-3331, “A Methodology for Allocating Nuclear Power Plant Control actions to Human or Automatic Control,” U.S. Nuclear Regulatory Commission, 1983.
7. NUREG-0711, “Human Factors Engineering Program Review Model,” Rev. 3, U.S. Nuclear Regulatory Commission, November 2012.

8. DEFINITIONS

1. Critical Function – The singular purpose of a set of plant processes, systems and components that if not achieved would compromise an overall plant goal such as safe operation or efficient power production. Synonymous with “High Level Function” in NUREG-0711
2. Control Action – An act that changes the status of a success path manually or automatically at the component, system or process level. For example starting a pump, throttling a valve or opening a circuit breaker.

APPENDIX A NUREG-0711 REV. 3 REVIEW CRITERIA CONFORMANCE TABLE

NUREG-0711 Rev. 3 Review Criteria	IP Section and Paragraph
(1) The applicant should use a structured, documented methodology reflecting HFE principles to perform functional requirements analysis (FRA) and function allocation (FA). Additional Information: Figure 4-2 is an example of an FRA and FA process.	Subsection 3.1, 4.1 Figure 3-1, 4-4, Reference 2, 3
The FRA and FA may be graded based on: • the degree to which the functions of the new design differ from those of its predecessor(s)	Subsection 3.2.1, 4.3
• the extent to which problems in operating experience were encountered for the plant's functions in predecessor plants	Subsection 3.1, 4.1, 4.5
(2) The applicant's FRA and FA should be performed iteratively to keep it current during design development and operation up to decommissioning, so that it can be used as a design basis when modifications are considered.	Figure 3-1 Subsection 4.2
(3) The applicant should describe the plant's functional hierarchy, including, as appropriate goals, functions, processes, and systems. The description should include: • comparing them with the predecessor or reference plants and systems, i.e., the previous ones on which the new plant is based	Subsection 3.2.3, 4.3, Appendix B
• identifying the differences between the proposed and reference plants and systems	Subsection 3.2, 4.3 Table 4-2
• documenting the technical basis for modifications to high-level functions in the new design (compared to the predecessor design) defining, for each safety function and other plant function (e.g., electrical power generation), the set of system configurations or success paths that are responsible for, or able to carry out the function	Subsection 3.2.1, 4.3 Table 4-2
• decomposing the functions, starting at "high-level" functions where a very general picture of major functions is described, and continuing to lower levels, until a specific critical end-item requirement emerges (e.g., a piece of equipment, software, or an HA). The functional decomposition should address the following levels: -high-level functions (e.g., maintain reactor coolant system integrity) -the processes, as appropriate, that enable achievement of these functions -specific plant systems and components -HAs, as appropriate	Subsection 3.2.3, 4.3 Figure 4-1, 4-2
Additional Information: Safety functions (e.g., reactivity control) include functions needed to prevent or mitigate the consequences of postulated accidents that could pose undue risk to the public's health and safety. HAs will be further evaluated in the task analyses.	Subsection 4.3

NUREG-0711 Rev. 3 Review Criteria	IP Section and Paragraph
(4) For each high-level function, the applicant should identify requirements related to: • purpose of the high-level function	Subsection 3.2.3, 4.4 Table 4-1
• conditions indicating that the high-level function is needed	Subsection 3.2.3, 4.4 Table 4-1
• parameters indicating that the high-level function is available	Subsection 3.2.3, 4.4 Table 4-1
• parameters indicating that the high-level function is operating (e.g., flow indication)	Subsection 3.2.3, 4.4 Table 4-1
• parameters indicating that the high-level function is achieving its purpose (e.g., reactor vessel level returning to normal)	Subsection 3.2.3, 4.4 Table 4-1
• parameters indicating that the operation of the high-level function can or should be terminated	Subsection 3.2.3, 4.4 Table 4-1
Additional Information: At this stage, parameters may be described qualitatively (e.g., high or low). Specific data values or setpoints are not necessary.	Subsection 3.2.3, 4.4 Table 4-1
(5) Applicants should allocate functions to a level of automation (e.g., from manual to fully automatic) and identify the technical bases for the allocations.	Subsection 3.3, 4.5 Figure 4-4, Table 4-3 Appendix C, Reference 2
Additional Information: The technical basis for the FA can be any one or combination of the factors (see Figure 4-2). For example: • Functions, or parts of them, may be allocated based on operating experience. Successful operating experience may suggest keeping allocations the same as in predecessor designs and operating experience issues may suggest changing the allocations to address the issues.	Subsection 3.3, 4.5 Figure 4-4, Table 4-3 Appendix C, Reference 2
• Functions, or parts of them, may be allocated to automation when their performance requirements exceed human capabilities and human error is likely. Conditions that establish a basis for automation (assuming the acceptability of other factors, such as technical feasibility or cost) include when the required response time is very short, when an action has to be performed repeatedly, or when very precise control is required.	Subsection 3.3, 4.5 Figure 4-4, Table 4-3 Appendix C, Reference 2
• Functions, or parts of them, should be allocated to personnel when human knowledge and judgment is needed to ensure reliable function performance, it is important to keep personnel	Subsection 3.3, 4.5 Figure 4-4, Table 4-3 Appendix C, Reference 2
(6) The applicant's FA should consider not only the primary allocations to personnel (those functions for which personnel have the primary responsibility), but also their responsibilities to monitor automatic functions, detect degradations and failures, and to assume manual control when necessary.	Subsection 4.6, Figure 4-4, Appendix C

NUREG-0711 Rev. 3 Review Criteria	IP Section and Paragraph
(7) The applicant should describe the overall role of personnel by considering all functions allocated to them.	Figure 3-1, Subsection 4.7
Additional Information: The FA to personnel and automation is considered on a function-by-function basis. However, the overall personnel role is an aggregate of all functions allocated to them. While on an individual basis, a single function allocation to personnel may be justified, allocations should also be considered in the context of other responsibilities personnel have to help ensure that together all functions allocated to personnel are acceptable and do not interfere with each other.	Figure 3-1, Subsection 4.7
(8) The applicant should verify that the FRA and FA accomplish the following: • all the high-level functions needed to achieve safe operation are identified	Figure 3-1, Subsection 4.8
• all requirements of each high-level function are identified	Figure 3-1, Subsection 4.8
• the allocation of functions to humans and automatic systems assures a role for personnel that takes advantage of human strengths and avoids human limitations	Figure 3-1, Subsection 4.8
(9) Additional Considerations for Reviewing the HFE Aspects of Plant Modifications -(not needed for new designs)	N/A

APPENDIX B SAFETY FUNCTION APPROACH OF CEN-152

"The concept of safety functions introduces a systematic approach to plant operations based on a hierarchy of protective actions. The protective actions are directed at mitigating the consequences of an event and, once fulfilled, ensure proper control of the event in progress. A safety function is defined as a condition or action that prevents core damage or minimizes radiation release to the public. A complete set of safety functions needs to be fulfilled to ensure proper operator control of the event and public safety. The actions, which ensure fulfillment of a safety function, may result from automatic or manual actuation of systems, from passive system performance, from natural feedback inherent in the plant design, or when the operator follows guidance established in an event recovery guideline. The operator does not have to know what event has occurred but does have to know what success paths are being utilized and what acceptance criteria must be satisfied.

All safety functions are directed at mitigating an event and containing and/or controlling radioactivity releases. These safety functions can be grouped into four major classes as follows:

- Anti-core melt safety functions.
- Containment integrity safety functions.
- Indirect radioactive release safety function.
- Maintenance of vital auxiliaries needed to support the other safety functions.

The anti-core melt safety function class contains five safety functions:

- Reactivity control
- RCS inventory control
- RCS pressure control
- Core heat removal
- RCS heat removal

The purpose of the first anti-core melt safety function, reactivity control, is to shut down the reactor and to keep it shut down, thereby reducing the amount of heat generated in the core. The purpose of Reactor Coolant System (RCS) inventory and pressure control is to keep the core covered with an effective coolant medium. RCS inventory and pressure control are interdependent in a PWR design. That is, actions taken to effect inventory control will affect pressure control and vice versa. The purpose of the fourth anti-core melt safety function, core heat removal, is to remove the decay heat generated in the core and transfer it to a location where it can be removed from the RCS. The fifth anti-core melt safety function is RCS heat removal. The purpose of this safety function is to transfer heat from the primary system coolant to another heat sink. The containment integrity safety function class contains two safety functions:

- Containment isolation.
- Containment temperature and pressure control.

The primary objective of these safety functions is to prevent major radioactive release from the containment by maintaining the integrity of the containment structure. Accomplishing the first safety function, containment isolation, assists in maintaining containment integrity by ensuring that all normal

containment penetrations not required to be open for accident mitigation are closed. The purpose of the containment temperature and pressure control safety function is to prevent overstressing the containment structure and to prevent damage to other equipment in the containment resulting from a hostile environment.

The third safety function class has one safety function associated with it: indirect radioactive release. The purpose of indirect radioactive release control is to prevent radioactive releases to the environment (gaseous, solid, and liquid, including radioactive coolant) from sources outside containment. These sources include the spent fuel pool and the radioactive waste handling and storage facilities. The systems used to control releases from these sources include the radiation monitoring system, the spent fuel pool cooling system, and the waste management and processing systems. In mitigating the types of emergencies for which CEN-152 provides guidance, the indirect radioactive release safety function does not come into play. Consequently, operator actions necessary for control of the indirect radioactive release safety function are not found in CEN-152.

The fourth safety function class also includes only one safety function: maintenance of vital auxiliaries. The systems used to accomplish the other safety functions addressed in CEN-152 are all supported by the maintenance of vital auxiliaries safety function. In general, support systems provide service such as instrument air needed for opening and closing valves, electric power for valve operation, pump motor operation, and operating instruments and an ultimate heat sink to which RCS and core heat can be transferred. Of greatest impact to the operator actions associated with CEN-152 is vital AC and DC power. AC and DC power must be maintained in order to continue to satisfy the acceptance criteria of the other safety functions."

"Because safety functions are a complete set of actions or conditions which will provide for the safety of the public, they form the foundation of all emergency procedure guidelines. In the Optimal Recovery Guidelines (ORGs), specific events such as LOCA or Excess Steam Demand Event are addressed. Because each event affects diverse parts of the plant, proper mitigation of different events will emphasize different safety functions. For example, in a major LOCA, RCS Pressure Control and RCS Inventory control are the two safety functions of immediate concern. Therefore, the operator actions are sequenced to achieve control of these two safety functions first by using equipment designed for that purpose. Nonetheless, since all safety functions must be fulfilled to provide for the safety of the public, each ORG addresses all of the safety functions. In preparing emergency procedure guidelines, the nine safety functions are used to audit the guideline to ensure that sufficient action steps exist to cover all safety functions. Each ORG includes a safety function status check which is used by the operator to continually determine whether the safety functions are being adequately fulfilled.

The Functional Recovery Guideline (FRG) is used by the operator when a diagnosis is not possible, when the Optimal Recovery Guideline being utilized is not adequate (as judged by the safety function status check in each ORG) or when the guideline in use is inappropriate. The FRG's structure includes an expanded version of the safety function status check which is used by the operator to continually check the status of each safety function. For those safety functions which are found to be in jeopardy, possible success paths are provided along with operator actions for implementing each success path and acceptance criteria by which successful safety function restoration is judged. For this guideline the safety functions form the main structure of the guideline.

Nuclear power plants are designed such that each safety function has multiple means of fulfillment. In other words, for each safety function there exists more than one system or means of fulfillment called success paths. For example, Reactivity Control can be achieved by inserting control rods or by increasing RCS boron concentration. With respect to the latter, there are several methods of increasing RCS boron

concentration. It is important that the operator be aware of the various success paths associated with each safety function. During any emergency event, the operator needs information on plant conditions. This monitoring of plant conditions leads to identification of the safety functions in jeopardy and the systems available to satisfy the safety function acceptance criteria. The CEN-152 emergency procedure guidelines clearly indicate the alternate means of satisfying each safety function by providing success path oriented guidance. “

APPENDIX C FUNCTION ALLOCATION SELECTION ANALYSIS

The following guidelines and criteria are adapted from NUREG/CR-3331, “A Methodology for Allocating Nuclear Power Plant Control actions to Human or Automatic Control”.

This provides a framework for evaluators to verify appropriate allocations of plant control actions in any aspect of the design.

1. Is automation mandatory? a. Are working conditions hostile to humans? b. Are tasks included which humans cannot perform? c. Do legal or regulatory requirements require automation? d. Is automation required to assure plant safety or protection? Yes (any) – Go to step 2. No (all) – Go to step 3. (If automation is required only in part, then the design description may detailed to identify that part.)
2. Is automation technically feasible? a. Are proven technologies available? b. Are the costs and development/delivery times acceptable? Yes (all) – Tentatively allocates to auto; go to step 9. No (any) (Tentatively allocates to auto; go to step 9 engineering solution.
3. Is human performance mandatory? a. Is automation technically infeasible? b. Is human required to retain policy-level or ultimate control? c. Does law or regulations require human? Yes (any) – Go to step 4. No (all) – Go to step 5. (If a human operator is required only in part, then the design description may be detailed to identify that part.)

4. Is human performance a feasible solution?

a. Can humans perform the specified tasks?

b. Are the costs and development/delivery times of the necessary support (e.g., procedures, training, etc.) acceptable?

Yes (all) – Allocate to human; go to step 11.

No (any) – Redefine the function(s), allocation, or engineering solution.

5. Is automation clearly preferable to human operators?

a. Is automation technology well established as suitable? (I.e., effective, reliable, cost-effective, etc.)

b. Is human performance acknowledged as less satisfactory?

Yes (all) – Tentatively allocates to auto; go to step 9.

No (any) – Go to step 6.

(If automation is preferable only in part, then expand the design description sufficiently to identify that part.)

6. Is human performance clearly preferable to automation?

a. Is human performance regarded as clearly necessary, or superior to automation?

Yes – Allocate to human; go to step 11.

No – Go to step 7.

(If a human operator is preferable only in part, then the design description may be detailed to identify that part.)

7. Is the segment a suitable candidate for automation?

a. Is the segment comprised of mechanistic or repetitive tasks?

b. Does the segment require sustained vigilance?

c. Does the segment require extremely rapid or consistent responses?

d. Is the segment comprised of well-defined and highly predictable conditions, actions, and outcomes?

e. Is the segment likely to be required at the same time as a large (i.e., excessive) number of other tasks?

f. Does the segment require the collection, storage, manipulation, or recall of data in substantial amounts, or with high accuracy?

Yes (any) – Tentatively allocates to auto; go to step 9.

No (all) – Go to step 8.

8. Is the segment suitable for human operator performance?

a. Is it within the realm of human strengths and capabilities?

b. Will the task form an appropriate and satisfactory part of an operator's job? (i.e., cannot be trivial, demeaning, or comprised of leftovers)

c. Will it allow the operator to maintain satisfactory workload? (i.e., neither too high nor too low)

Yes (all) – Allocate to human; go to step 11.

No (any) – Go to step 10.

9. Reconsider the tentative automatic allocations in terms of their negative impact on human operator performance.

a. Would manual performance of the task help to keep the operator engaged with the plant, informed of process status, or prepared to plan and solve problems?

b. Would manual performance of the task provide the operator with important opportunities to develop or maintain valuable skills or knowledge?

c. Will absolute implementation of the automatic feature(s) contribute to operator under-loading (e.g., boredom)?

d. Would the option for manual control from the control room afford desired flexibility?

e. Would the option for manual control from the control room afford more reliable performance of the function?

f. Would the option for manual control from the control room be desirable for testing, maintenance, or management of off-normal conditions?

Yes (any) – Make a tentative allocation to automation with operator discretion.

If operator discretion is superordinate (man selects auto or manual modes) then go to step 11.

If operator discretion is subordinate (man may initiate but not override automatic action), go to step 12.

No (all) – Allocate to automation; go to step 12.

10. If any segments remain unallocated, apply the following criteria:

a. Comparative cost of human and automated options

b. Consistency with preceding design goals and selections

c. Available technologies

d. Customer preference

e. Operator acceptance

Or, redefine the function(s), allocation, or engineering solution.

If allocated to automation, go to step 9.

If allocated to human operator, go to step 11.

11. Consider residual automated and control system support for the operator: a. Data display and integration b. Monitoring of limits and detection of abnormalities c. Hierarchical access to indicating and control options d. Automatic control of inner loops e. “Fail safe” controls, etc. Complete any required documentation.
12. Consider the residual role of the human operator in support of the automated function: a. Policy-level control (e.g., initiation of transitions to less conservative plant states) b. Awareness of automatic system status, transitions, availability, etc. c. Detection of abnormalities and management of failures, including those in “hidden” or low-level features d. Emergency initiation or shutdown e. Override of selected interlocks under specified conditions f. Removal of equipment from service g. Status of local transfer or test switches Complete any required documentation.

APPENDIX D EXAMPLE CSF SELECTION JUSTIFICATION NARRATIVES

(FROM NPX80-IC-RR790-02)

Safety Function: Reactivity control

Success Path: Reactor Trip

Reactor trip is a protective feature whose rapid and reliable initiation is of the utmost importance to safety. Automatic initiation of reactor trip is mandatory, and occurs in response to RPS or DPS trip signals (see Reference 4, Sections 7.2 and 7.7.1.1.11, respectively); manual initiation is also provided to enable operators to perform assigned supervisory and backup roles. Operator actions will be performed under normal MCR habitability conditions. As a discrete function, Reactor Trip has no continuous control component to be allocated. These system 80+ allocations are unchanged from those in System 80.

Allocation Rationale: Automation is mandatory because of sustained monitoring and rapid response time requirements (1b), federal regulations (1c), and the need to assure plant protection (1d). Automation is feasible, i.e., technically proven (2a) and practically available (2b). Manual initiation is desirable for flexibility and reliability (9d & 9e).

Success Path: Safety Injection

The SI system performs Reactivity Control by direct high pressure injection of borated water into the Rx vessel. This occurs automatically, when a SIAS is generated by the ESF system. Note that SIAS is not generated automatically in order to shut the reactor down, however, SI boration rate is sufficient to maintain shutdown margins even if the most reactive rod were ejected from the core (see Chapter 7, Reference 4). Manual initiation is provided to enable operators to perform assigned supervisory and backup roles. Following initiation, operators have the responsibility to evaluate, adjust, and/or terminate SI. These System 80+ allocations are unchanged from those in System 80.

Allocation Rationale: Automation is preferable based on precedent (5a), and in preference to human performance (5b) based on characteristics of the function (e.g., per 7a, 7b, 7d, 7e). Manual operation is desirable for flexibility and reliability (9d & 9e).

Success Path: Charging & Volume Control (Boration)

The CVCS can be used to inject borated water into the RCS. However, it is a relatively slow, long-term means of adjusting core reactivity, and is not a credited safety system for Reactivity Control. Boration is not a standard lineup for the eves, and it is performed and initiated manually from the control room. However, once aligned, the eves can be operated in either automatic or manual modes. These System 80+ allocations are unchanged from those in System 80.

Allocation Rationale: The function is suitable for allocation to the operator (5a, 5b, & 8c).

Success Path: Rod Control

Rod control provides a backup success path that can be used if rod(s) stick or otherwise fail to return to their bottom travel positions following a reactor trip. This is accomplished by re-shutting the trip breakers and energizing the rod drive mechanisms, then attempting to actively drive the rods inward using the rod control system. The rod control system is not a protective means of reactivity insertion, it is not a credited safety system for Reactivity Control, and the execution of this task is fully manual. These System 80+ allocations are unchanged from those in System 80.

Allocation Rationale: Given the suitability of the associated tasks (e.g., per 5a, 8b, & 8c), human performance is clearly preferable for this application (6a, or 3b) due to the need to deliberately shut the Reactor Trip Breakers as part of the process.