Identification of Important Human Actions via a Combination of Probabilistic and Deterministic Analyses

Juntao Hu[1], Yongping Qiu[2], Yucheng Zhuo[3], Jiandong He[4]

[1]*Shanghai Nuclear Engineering Research and Design Institute, No. 29 Hongcao Road, Shanghai, China, 200233 and hujuntao@snerdi.com.cn*
[2]*Shanghai Nuclear Engineering Research and Design Institute, No. 29 Hongcao Road, Shanghai, China, 200233 and qiuyp@snerdi.com.cn*
[3]*Shanghai Nuclear Engineering Research and Design Institute, No. 29 Hongcao Road, Shanghai, China, 200233 and zhuoyucheng@snerdi.com.cn*
[4]*Shanghai Nuclear Engineering Research and Design Institute, No. 29 Hongcao Road, Shanghai, China, 200233 and hejd@snerdi.com.cn*

For the large advanced passive nuclear power plant in China, important Human Actions (HAs) are identified via a combination of probabilistic and deterministic analyses, which include 26 risk-important HAs from Probabilistic Safety Assessment/Human Reliability Analysis (PSA/HRA) in Chapter 19 of Preliminary/Final Safety Analysis Report (PSAR/FSAR), 6 important HAs from Accident Analysis in Chapter 15 and another one important HA from Diversity and Defense in Depth (D3) in Chapter 7 of PSAR/FSAR. These important HAs are addressed by the Human Factors Engineering (HFE) program, in Function Allocation, Task Analysis, Human System Interfaces (HSI) design, Procedural Development, and Training Program Development, in order to minimize the likelihood of human error and facilitate error-detection and recovery capability.

I. INTRODUCTION

Risk analyses are used to prioritize activities and to ensure that both regulators and applicants focus their efforts and resources on those activities that best assure the public's health and safety. Human Factors Engineering (HFE) programs contribute to this by applying a graded approach to plant design by focusing greater attention to those Human Actions (HAs) most important to safety.

According to the requirements of NUREG-0711 (Ref. 1), applicants should identify those HAs most important to safety via a combination of probabilistic and deterministic analyses, and then address them when conducting the HFE program. The former is typically done using a probabilistic safety assessment (PSA) or probabilistic risk assessment (PRA), including its human reliability analysis (HRA). These analyses identify the risk-important HAs described in Chapter 19 of the PSAR/FSAR/DCD. Deterministic engineering analyses are generally completed as part of the suite of analyses in the PSAR/FSAR/DCD in Chapters 7, Instrumentation and Controls, and 15, Accident Analysis. These analyses sometimes include credit for HAs by operators as part of an evaluation. Thus, a full identification of important HAs depends on analyses and methods that are reviewed by regulators using Chapters 7, 15, and 19 of the Standard Review Plan (NUREG-0800) (Ref. 2).

Figure 1 illustrates the relationship between the treatment of important HAs and the rest of the HFE program. The important HAs are specifically addressed in many HFE elements, where the applicant describes how each of the important HAs is addressed in the HFE program.

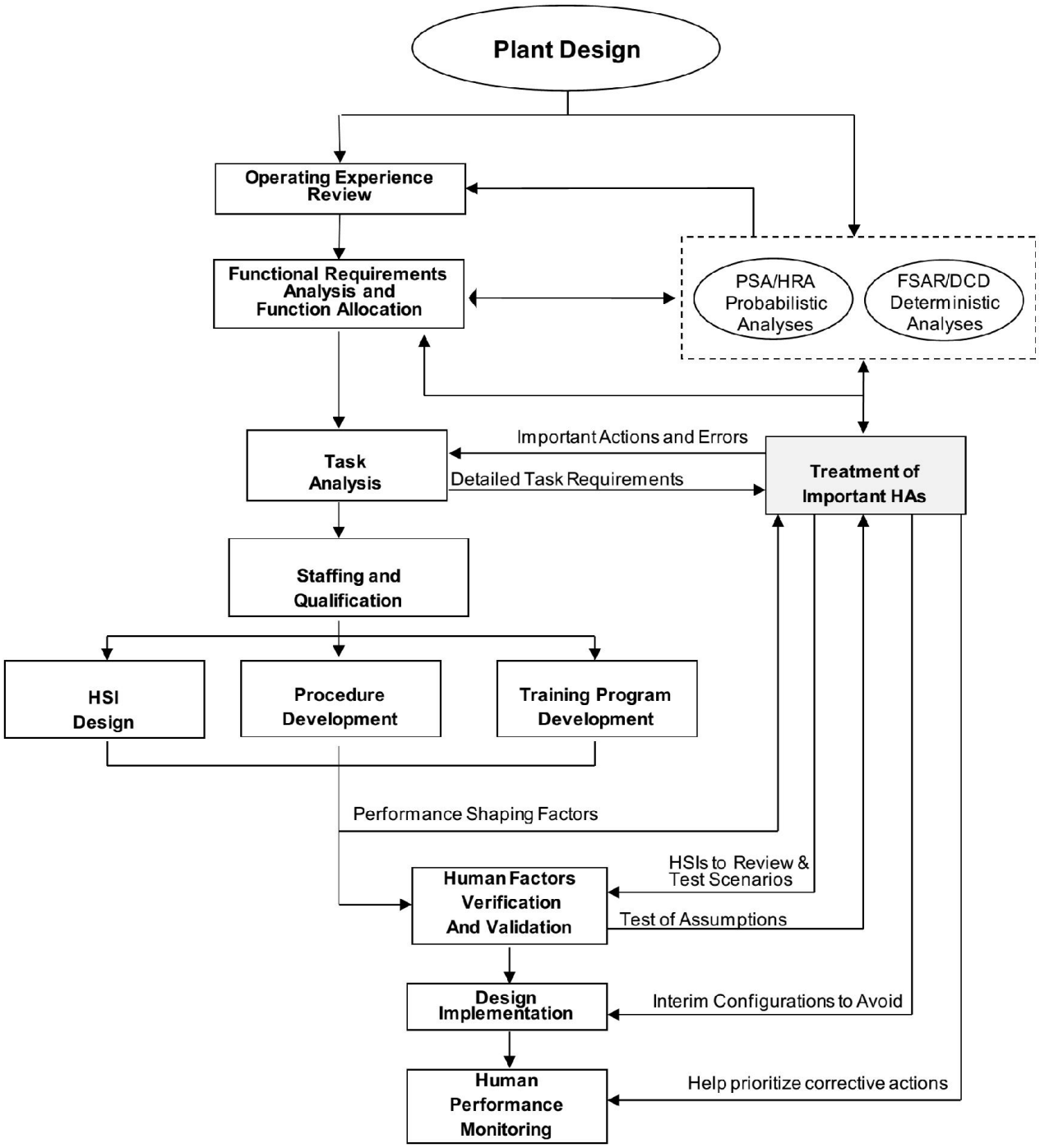

Figure 1 The role of important human actions in the HFE program

II. ANALYSES CRITERIA

Probabilistic and deterministic analyses criteria are used to identify important human actions used to mitigate accidents. These criteria are summarized below.

II.A. Probabilistic Analyses Criteria

HRA is an integral part of a completed PSA. Applicants submit PSAs in accordance with the regulators' current requirements. An HRA evaluates the potential for, and mechanisms of human error that might affect plant safety. Thus, it is an essential feature in assuring the HFE program goal of generating a design to minimize personnel errors, support their detection, and ensure recovery capability. The HRA is an integrated activity supporting both the HFE design and PSA activities. The robustness and quality of the HRA largely depends on the analyst's understanding of the causes, modes and probabilities of human error, the personnel tasks to be performed, information about those tasks, and any task-specific factors that may influence the human performance of them. Analysts should employ the descriptions and analyses of personnel functions and tasks, along with the operational characteristics of the HSIs. The HRA provides valuable insights into the desirable characteristics of the HSI design. Consequently, the HFE design should pay special attention to those plant scenarios, risk-important HAs, and HSIs that the PSA/HRA highlights as vital to plant safety and reliability.

The PSA and HRA should begin early in the design process to provide insights and guidance for both systems design and for HFE purposes. Thus, the applicant should use, as appropriate, the first version of the PSA/HRA (depending on the amount of design information available) to identify the important HAs, so that they can be considered in the early HFE design elements. The analyses should be updated iteratively as the design progresses (including the final PSA/HRA) to ensure the actual important HAs are captured and considered. At least, the initial PSA/HRA, and the set of important HAs, should be finalized when the design of the plant and HSI are complete.

II.A.1. Critical Human Actions Analyses Criteria

Any one human action, if assumed to fail, would result in a core damage frequency greater than 1E-5/yr or a large release frequency greater than 1E-6/yr.

The evaluation considered the baseline PSA quantitative results including at-power and shutdown conditions as well as internal events, internal fire and internal flood events.

II.A.2 Risk-Important Human Actions Criteria

Risk-important human actions used to mitigate an accident are identified using both quantified PSA importance measures and an expert panel.

The quantified PSA importance measures include evaluating both the Risk-Achievement worth (RAW) and Risk-Reduction worth (RRW) caused by the human action.

1. Risk-Achievement Worth: This measure examines the increase in risk that would result if a single human action were to fail. The CDF and LRF are requantified for each human action by setting its failure probability to 1. The RAW value is then calculated as the percentage increase in CDF or LRF due to the human failure. For the baseline PSA study, a human action is considered risk-important if the CDF or LRF increase is 200%, i.e. the RAW is > 3.0. For the "focused" PSA study (with assumed failure of nonsafety mitigating features), a human action is considered risk-important if the percentage increase is 100%, i.e. the RAW is >2.0. Any value below these criteria is considered to be not risk-important.

2. Risk-Reduction Worth: This measure examines the decrease in risk that would result if a human action were made perfectly reliable. The CDF and LRF are requantified for each human action by setting its failure probability to 0. The RRW value is then calculated as the percentage decrease in CDF or LRF. For the baseline PSA study, a human action is considered risk-important if the CDF or LRF decreases by more than 10%, i.e. the RRW is > 1.1. For the "focused" PSA study (with assumed failure of nonsafety mitigating features), a human action is considered risk-important if the percentage decrease is 5%, i.e. the RRW is >1.05. Any value below these criteria is considered to be not risk-important.

These importance would be determined for the following initial conditions and events:

		CDF	LRF
Baseline PSA	At-power--internal events	yes	yes
	--internal fire	yes	-
	--internal flood	yes	-

	Shutdown--internal events	yes	yes
Focused PSA	At-power--internal events	yes	yes
	--internal fire	yes	-
	--internal flood	yes	-
	Shutdown--internal events	yes	yes

In addition to the quantified risk importance measures, an expert panel is required to review the human action RAW / RRW values and to determine if any actions not meeting the quantitative screening criteria should be included. In making this determination, the following factors are to be considered:

- If the RAW / RRW values were less than but close to the criteria and
  a) The time available for the operator to act is close to the available time
  b) The actions are complex, unique, or potentially challenging
  c) The actions are needed to prevent conflicting safety goals
- Actions that are judged to be risk-important by the panel based on their experience

Note that in general, the greater the difference between the RAW / RRW values and the criteria, the more qualitative considerations were required to include an human action.

The expert panel should have representatives from HRA/PSA, systems engineering design, HSI design, and HFE.

II.B. Deterministic Analyses Criteria

II.B.1. Accident Analyses Criteria

Probabilistic analyses are supplemented by identifying important HAs in the FSAR/DCD deterministic analyses. To establish a licensing basis, applicants must analyze transients and accidents in accord with the requirements of 10 CFR 50.34 and 10 CFR 50.46; these events are described in the Standard Review Plan. The analyses appear in Chapter 15 of a DCD, or an FSAR and in some cases include HAs that are credited in the analyses to prevent or mitigate the accidents and transients. These HAs may, or may not, be found as risk-important by the PSA. Nonetheless, all credited HAs should be considered deterministically as significant for the purposes of the HFE program.

II.B.2. Diversity and Defense in Depth Analyses Criteria

The NRC I&C staff has established a position on common cause failures of digital I&C in a nuclear power plant (currently in the Interim Staff Guidance on Diversity and Defense in Depth (D3) Issues - NRC, 2009). Applicants are to perform a D3 analysis to demonstrate that their designs adequately address vulnerabilities to common cause failures. The applicant may identify backup systems or HAs necessary for accomplishing the required safety functions. These HAs should be treated as important human actions in the HFE program.

III. HUMAN ACTIONS IMPORTANCE ANALYSES

Human actions importance analyses processes are summarized below for the large advanced passive nuclear power plant in China.

III.A. Probabilistic Analyses

III.A.1. Critical Human Actions Analyses

As shown in the following paragraphs, no critical human actions have been identified by probabilistic analyses criteria. This is not surprising given the reduced dependence on human actions in the large advanced passive nuclear power plant in China.

The most risk important human actions are shown in Tables 1 and 2. These tables show the basic event probabilities from the PSA and the re-calculated CDF or LRF values that result by assuming the failure of an human action. Note that

these tables also show RAW / RRW values although they are not used in determining "critical" human actions. Table 1 shows the top 10 human failure events with the highest CDF. Table 2 shows the top 10 human failure events with the highest LRF. None of the resulting CDF or LRF is above the criteria listed in Section II.A.1 (CDF > 1E-5/yr or LRF > 1E-6/yr).

Table 1 Human Actions Sorted by Resulting CDF (Baseline PSA)

Basic Event ID	Basic Event Description	Basic Event Prob.	Resulting CDF (/yr)	Criteria for CDF(/yr)
CIB-MAN01	Failure to isolate the faulted steam generator, given a steam generator tube rupture event	2.48E-03	7.08E-07	<1.0E-05
CIB-MAN00	Failure to diagnose a steam generator tube rupture event	1.25E-03	7.06E-07	<1.0E-05
OPA-01	Operator fails to deactivate the Protection and Safety Monitoring System (PMS) division involved in the fire	3.00E-02	5.61E-07	<1.0E-05
REC-MANDAS	Failure to detect the need to perform an activity by using the cues provided by diverse actuation system, or the probability to perform an activity by using the controls that are DAS related	8.62E-02	5.40E-07	<1.0E-05
ADN-MAN01	Failure to actuate the ADS for RCS depressurization as recovery from failure of automatic actuation or for manual ADS actuation	1.47E-03	4.80E-07	<1.0E-05
RTN-MAN01	Failure to perform a controlled shutdown of the reactor during RCS leakage	4.69E-04	4.50E-07	<1.0E-05
LPM-MAN02	Failure to recognize the need for RCS depressurization during a medium LOCA	8.23E-02	3.97E-07	<1.0E-05
HPM-MAN01-FIRE	Failure to recognize the need for high-pressure decay heat removal during fire scenarios	4.75E-02	3.37E-07	<1.0E-05
PRN-MAN01-FIRE	Failure to align the PRHR system during fire scenarios	3.88E-03	3.20E-07	<1.0E-05
RHN-MAN01	Failure to recognize the need and failure to align the NRHR system after ADS actuation, during a LOCA, LOOP, or transient in the reactor coolant system cooling mode	3.04E-02	2.69E-07	<1.0E-05

Table 2 Human Actions Sorted by Resulting LRF (Baseline PSA)

Basic Event ID	Basic Event Description	Basic Event Prob.	Resulting LRF (/yr)	Criteria for LRF(/yr)
CIB-MAN01	Failure to isolate the faulted steam generator, given a steam generator tube rupture event	2.48E-03	1.21E-07	<1.0E-06
REC-MANDAS	Failure to detect the need to perform an activity by using the cues provided by diverse actuation system, or the probability to perform an activity by using the controls that are DAS related	8.62E-02	7.03E-08	<1.0E-06
CIB-MAN00	Failure to diagnose a steam generator tube rupture event	1.25E-03	6.82E-08	<1.0E-06
DAN-REC01	Failure to recognize the need and failure to actuate the ADS though DAS after core damage	8.40E-02	4.21E-08	<1.0E-06
RHN-MAN01	Failure to recognize the need and failure to align the NRHR system after ADS actuation, during a LOCA, LOOP, or transient in the reactor coolant system cooling mode	3.04E-02	3.50E-08	<1.0E-06
ADN-MAN01	Failure to actuate the ADS for RCS depressurization as recovery from failure of automatic actuation or for manual ADS actuation	1.47E-03	3.38E-08	<1.0E-06
RTN-MAN01	Failure to perform a controlled shutdown of the reactor during RCS leakage	4.69E-04	3.38E-08	<1.0E-06
LPM-MAN02	Failure to recognize the need for RCS depressurization during a medium LOCA	8.23E-02	3.25E-08	<1.0E-06
VLN-MAN01	Failure to recognize the need and failure to actuate the hydrogen control system, given core damage following a LOCA	2.94E-02	2.79E-08	<1.0E-06
REN-MAN03	Failure to recognize the need and failure to open recirculation valves to flood reactor cavity after core damage	5.88E-03	2.52E-08	<1.0E-06

III.A.2 Risk-Important Human Actions Analyses

Risk-important human actions used to mitigate accident are identified using both quantified PSA importance measures and an expert panel.

A total of 26 risk-important human actions are identified from probabilistic analyses. Six of them were added by the expert panel; the other 20 actions were identified by the RAW / RRW criteria. Table 3 lists 10 risk-important human actions as an example. The human actions are listed alphabetically by basic event ID.

Table 3 Some Important Human Actions Sorted by Basic Event ID

No.	Basic Event ID	Basic Event Description	Baseline PSA				Focused PSA			
			CDF		LRF		CDF		LRF	
			RAW (>3.0)	RRW (>1.1)	RAW (>3.0)	RRW (>1.1)	RAW (>2.0)	RRW (>1.05)	RAW (>2.0)	RRW (>1.05)
1	ADN-MAN01	Failure to actuate the ADS for RCS depressurization as recovery from failure of automatic actuation or for manual ADS actuation	—	—	—	—	2.24	—	—	—
2	CIB-MAN00	Failure to diagnose a steam generator tube rupture event	3.72	—	4.46	—	—	—	—	—
3	CIB-MAN01	Failure to isolate the faulted steam generator, given a steam generator tube rupture event	3.74	—	7.93	—	—	—	—	—
4	CIS-RECDAS	Failure to recognize the need and failure to isolate the containment through DAS	—	—	—	—	—	—	—	1.05
5	DAN-REC01	Failure to recognize the need and failure to actuate the ADS though DAS after core damage	—	—	—	1.19	—	—	2.58	1.17
6	HPM-MAN01	Failure to recognize the need for high-pressure decay heat removal following a loss of main feedwater during an accident	—	—	—	—	32.0	1.17	12.0	1.06
7	HPM-MAN01-FIRE	Failure to recognize the need for high-pressure decay heat removal during fire scenarios	3.88							
8	IVR-RECDAS	Failure to recognize the need and failure to open recirculation valves to flood reactor cavity through DAS after core damage	—	—	—	1.13	—	—	—	1.06
9	LPM-MAN01	Failure to recognize the need for RCS depressurization during a small LOCA or loss of high-pressure heat removal system	—	—	—	—	2.47	—	—	—
10	LPM-MAN02	Failure to recognize the need for RCS depressurization during a medium LOCA	—	1.11	—	1.11	—	—	—	—

III.B. Deterministic Analyses

III.B.1. Accident Analyses

The following human actions are credited to prevent or mitigate the accidents and transients in accident analyses in Chapter 15：

1）Loss of Normal Feedwater Flow（Section 15.2.7 in PSAR）

A loss of normal feedwater (from pump failures, valve malfunctions, or loss of ac power sources) results in a reduction in the capability of the secondary system to remove the heat generated in the reactor core. I The specific operator action assumed in this case is to open the reactor vessel head vent to prevent pressurizer overfill.

2）Chemical and Volume Control System Malfunction that Results in a Decrease in the Boron Concentration in the Reactor Coolant（Section 15.4.6 in PSAR）

An inadvertent boron dilution is caused by the failure of the demineralized water transfer and storage system or chemical and volume control system, either by controller, operator or mechanical failure.

During full power operation (Mode 1) with the reactor in automatic rod control, a boron dilution results in a power and temperature increase in such a way that the rod controller attempts to compensate by slow insertion of the control rods. This action by the controller results in at least three alarms to the operator. Given the many alarms, indications, and the inherent slow process of dilution at power, the operator has sufficient time for action. The operator has at least 2 hours from the rod insertion limit low-low alarm until shutdown margin is lost at the beginning of the cycle.

3）Inadvertent Loading and Operation of a Fuel Assembly in an Improper Position（Section 15.4.7 in PSAR）

The inadvertent loading event comprises core misloading scenarios such as the loading of one or more fuel assemblies into improper positions, the loading of a fuel rod during manufacture with one or more pellets of the wrong enrichment, or the loading of a full fuel assembly during manufacture with pellets of the wrong enrichment.

Should misloadings occur, the system of fixed incore detectors, which is used to verify power distributions during startup and throughout the operating cycle, is capable of revealing enrichment errors or misloadings which would cause the kind of substantial power distribution perturbation that would be necessary to induce large numbers of fuel rod failures.

4）Inadvertent Operation of the Core Makeup Tanks During Power Operation（Section 15.5.1 in PSAR）

Spurious core makeup tank operation at power could be caused by an operator error, a false electrical actuation signal, or a valve malfunction.

The specific operator action assumed in this case is to open the reactor vessel head vent to preclude overfill 45 minutes following the high-2 pressurizer level signal.

5）Chemical and Volume Control System Malfunction That Increases Reactor Coolant Inventory（Section 15.5.2 in PSAR）

The increase of reactor coolant system coolant inventory may be due to the spurious operation of one or both of the chemical and volume control system pumps or by the closure of the letdown path. The specific operator action assumed in this case is to open the reactor vessel head vent to preclude pressurizer overfill 30 minutes following the high-2 pressurizer level signal.

6）Failure of Small Lines Carrying Primary Coolant Outside Containment（Section 15.6.2 in PSAR)

The small lines carrying primary coolant outside containment are the reactor coolant system sample line and the discharge line from the chemical and volume control system to the liquid radwaste system. The specific operator action assumed in sample line break is to isolate the break upon indication of a sample line break.

Six human actions are credited to prevent or mitigate the accidents and transients from the above analyses. The six human actions are not included in the list of important HAs identified through probabilistic analyses, which shall be treated as important human actions in HFE program.

III.B.2. Diversity and Defense in Depth Analyses

In D3 analyses in Chapter 7, the required safety functions are automatically actuated by diversity actuation system (DAS) or manually actuated by operators when anticipated functions of PMS was lost as a result of common cause failures of digital I&C in the large advanced passive nuclear power plant in China. HAs associated with manual DAS actuation are important because they assure the actuation of the required safety functions in case of PMS failure. The safety functions that can only be actuated manually by DAS are hydrogen igniters control, ADS depressurization, IRWST injection, sump recirculation, reactor cavity flooding, and most of HAs associated with the actuation of these safety functions have been modeled and identified in PSA (REC-MANDAS、DAN-REC01、IVR-RECDAS). Only one human action of manual actuation of hydrogen igniters (VLS-RECDAS) is not included in the list of important HAs identified through probabilistic analyses, which shall be treated as important human actions in HFE program.

IV. RESULTS AND CONCLUSIONS

For the large advanced passive nuclear power plant in China, important HAs are identified via a combination of probabilistic and deterministic analyses, which include 26 risk-important HAs from PSA/HRA in Chapter 19 of PSAR/FSAR, 6 important HAs from accident analysis in Chapter 15 and another one important HA from D3 analyses in Chapter 7 of PSAR/FSAR. These important HAs are addressed by the HFE program, in Function Allocation, Task Analysis, Human System Interfaces (HSI) design, Procedural Development, and Training Program Development, in order to minimize the likelihood of human error and facilitate error-detection and recovery capability.

ACKNOWLEDGMENTS

It was acknowledged that the supports for this study from my colleague, Huimin QIN, Yaoyao ZHENG, Qingxiang YANG, Shanshan ZHANG, Dongling XU.

REFERENCES

1. Human Factors Engineering Review Program Model, NUREG-0711, Rev.3, United States Nuclear Regulatory Commission, November 2012.
2. Stand Review Plan, NUREG-0800, United States Nuclear Regulatory Commission.