WCAP-14651

DRAFT

INTEGRATION OF HUMAN RELIABILITY ANALYSIS WITH HUMAN FACTORS ENGINEERING DESIGN IMPLEMENTATION PLAN

May, 1996

by

S. P. Kerch
E. M. Roth
S. Sancaktar

WESTINGHOUSE ELECTRIC CORPORATION
P. O. Box 355
Pittsburgh, Pennsylvania 15230-355

TABLE OF CONTENTS

LIST OF FIGURES

ACRONYMS

ADS	-	Automatic Depressurization System
COL	-	Combined License
CVS	-	Chemical and Volume Control System
HFE	-	Human Factors Engineering
HRA	-	Human Reliability Analysis
IRWST	-	In-Containment Refueling Water Storage Tank
LOCA	-	Loss-of-Coolant Accident
MMI	-	Man-Machine Interface
M-MIS	-	Man-Machine Interface System
MLOCA	-	Medium LOCA
MOV	-	Motor-Operated Valve
MTIS	-	Maintenance, Inspection, Test and Surveillances
PMS	-	Protection and Safety Monitoring System
PRA	-	Probabilistic Risk Assessment
RCS	-	Reactor Coolant System
RNS	-	Normal Residual Heat Removal
SLOCA	-	Small LOCA
SSC	-	Systems, Structures, and Components
THERP	-	Technique for Human Error Rate Prediction
V&V	-	Verification and Validation

1.0 INTRODUCTION

This document provides an implementation plan for the integration of Human Reliability Analysis (HRA) with Human Factors Engineering (HFE) design. It describes the interrelation among the activities to be conducted by the Man-Machine Design group, the Procedures Development group, and the HRA and Probabilistic Risk Assessment (PRA) group.

1.1 Scope and Objective of Implementation Plan

The objective of the HRA/HFE integration implementation plan is to enable:

- The HRA activity to integrate the results of the HFE design activities
- The HFE design activities to address risk-important tasks and human error mechanisms in order to minimize the likelihood of personnel error and to provide for error detection and recovery capability

This document does not cover HRA methodology. HRA methodology and results are described as part of the AP600 PRA Study documents.

1.2 Use of HRA/PRA Insights to Guide HFE Design

The AP600 design draws on lessons learned from existing plant experience and results of past HRAs and PRAs to reduce the potential for human error and increase safety. In response, one approach to increase plant safety in the AP600 has been to simplify the plant design and reduce the number of human actions required. For example, one of the design bases for the AP600 is that there are no human actions required to respond to design basis events. As described in Section 2.0, this substantially reduces the potential risk associated with human errors.

This HRA/HFE integration implementation plan describes the process by which insights from HRA/PRA will continue to be used to improve the HFE design and limit the risk to humans and the risk of errors.

Figure 1 provides an overview of how HRA activities are integrated within the HFE program. There are three primary points of interaction:

1. Task Analysis: Results of HRA/PRA analyses will be used to identify *risk-important* tasks and performance requirements as input to HFE task analysis activities.

2. Man-Machine Interface System (M-MIS) Design and Procedure Development: Results of M-MIS design and procedure development activities will be used to confirm and/or refine HRA assumptions. Tasks that are identified in the HRA/PRA that pose serious challenges to plant safety and reliability will be re-examined by task analysis, M-MIS design, and procedure development, to identify changes to the operator task, procedures, or the control and display environment to minimize the likelihood of operator error and provide for error detection and recovery capability.

3. HFE Verification and Validation (V&V): HRA performance assumptions (e.g., actions to be performed; time within which they are completed) will be validated as part of the HFE Integrated System Validation.

While training is an important contributor to human reliability, it is not explicitly addressed in this HRA/HFE integration implementation plan because training program development is a Combined License (COL) Applicant responsibility. Westinghouse will provide the COL applicant with the AP600 PRA Study documentation that includes description of HRA assumptions and results relevant to training. In addition, insights relevant to the training program will be provided in a report following the HFE V&V. This will include a list of critical human actions (if any), *risk-important* human actions, the performance requirements for those actions (e.g., response time) and any insights gained during the V&V that relate to training requirements for *risk-important* human actions (see Section 13.2.1 of the AP600 SSAR).

2.0 PRA/HRA IDENTIFICATION OF CRITICAL HUMAN ACTIONS AND RISK-IMPORTANT TASKS

In order to enable human actions and tasks (that are important to plant safety) to be explicitly addressed as part of the HFE design effort, the results of the HRA will be used to identify critical human actions (if any) and *risk-important* tasks. The human actions and tasks identified will be used as input to task analysis and HFE design activities.

2.1 Critical Human Action

Two alternative criteria are used to define critical human actions:

Deterministic criteria: Human actions that are required to prevent core damage or severe release in design basis accidents.

or

PRA criteria: Human actions (as identified from those baseline PRA studies with quantitative results) that if failed, would result in total core damage frequency equal to or greater than 1E-4 ($1x10^{-4}$) or severe release frequency equal to or greater than 1E-5 ($1x10^{-5}$).

The baseline PRA studies include internal at-power events and internal shutdown events.

2.2 *Risk-Important* Tasks

Risk-important tasks that involve human actions will be identified using two *risk-important* measures that are commonly used in PRA studies:

1. Risk Increase Measure: This measure examines the increase in risk that would result if the probability of failing to take human action were set to 1. The objective of this measure is to identify human actions that, if failed to be taken, would result in a significant increase in risk. These tasks would be included in the task analyses and integrated V&V activities to ensure that they are adequately supported by the M-MIS, so as to minimize the potential for error.

2. Risk Decrease Measure: This measure examines the decrease in risk that would result if the probability of failing to take the human action were set to 0. The objective of this measure is to identify human actions, that if executed correctly, would result in a significant reduction in risk. These tasks would be included in the task analyses and integrated V&V activities to ensure that they are adequately supported by the M-MIS, so as to maximize the potential for correct performance.

PRA studies calculating core damage and severe release frequencies are being performed for:

- Internal at-power events
- Internal shutdown events
- Fire, flood, seismic events (only core damage bounding assignment is being performed)

In addition, a focused PRA sensitivity study is being performed to provide input to regulatory treatment of non-safety systems. In this study, no credit is taken for nonsafety-related systems in the calculation of core damage and severe release frequencies. Credit is only taken for safety-related systems. The focused PRA sensitivity study is being performed for:

- Internal at-power events
- Internal shutdown events
- Fire and flooding events (core damage bounding assignment only)

The results of these PRA studies, performed for AP600, are examined to identify *risk-important* tasks.

In some cases quantitative measures of risk increase and risk decrease are automatically generated as part of the standard output of the PRA results. In those cases quantitative thresholds for risk increase and risk decrease can be defined for use in identifying *risk-important* tasks. In other cases, there is no clear quantitative measure that can be used in establishing a threshold for risk increase and risk decrease. In those cases, qualitative criteria, based on expert judgment, can be used to identify *risk-important* tasks.

Quantitative criteria to be used in identifying *risk-important* tasks, in cases where quantitative measures of risk increase and risk decrease are available, are described below. The qualitative criteria to be used to identify *risk-important* tasks in cases where quantitative measures are not available are also described.

Quantitative Criteria for *Risk-Important* Tasks:

A task is defined to be *risk-important* if its importance, as calculated by one of these two measures, is above a risk threshold associated with that measure.

The two measures are formally quantified as follows:

1. Risk Increase Measure: This measure provides the importance of a human action for core damage or severe release with respect to maintaining the existing risk level. For this purpose, the core damage or severe release is requantified for each human action by setting its failure probability to 1.0. The risk-importance of a human action is then defined as the percentage increase in core damage or severe release frequency. For example a risk-importance of 100 is the same as doubling the base core damage frequency when the task failure probability is set equal to 1.0. The larger the percentage, the more important the human action is in maintaining the existing risk level.

The risk increase importance threshold used for AP600 is 200% for internal events, at power and shutdown, for both core damage and severe release. Any value below this is deemed to be too small to be considered as worthwhile to pursue.

In the case of the focused PRA sensitivity study, the risk increase importance threshold used is 100%.

2. Risk Decrease Measure: This measure provides the importance of a human action for core damage or severe release with respect to reducing the existing risk level. For this purpose, the core damage or severe release is requantified by setting each operator action failure probability to zero. The importance of a human action is then defined as the percent decrease in core damage or severe release frequency. For example, a risk decrease value of 10% indicates that the maximum benefit that can be obtained by improving task failure probability is 10%. The larger the percent decrease, the more important the human action is in potentially reducing the existing risk.

   The risk decrease importance threshold used for AP600 is 10% for internal events, at-power and shutdown, for both core damage and severe release. Any value below 10% is deemed to be too small to be considered as worthwhile to pursue.

   In the case of the focused PRA sensitivity study, the risk increase importance threshold used is 5%.

The definition of *risk-important* tasks provided above utilizes well-recognized and quantifiable concepts of risk increase and risk decrease measures, which take into account different aspects of risk-importance. Defining *risk-important* tasks in terms of risk increase and risk decrease is consistent with the risk-importance measures used for other applications, such as the NRC maintenance rule. A uniform definition of risk-importance across different application areas allows consistency, as well as efficiency, since importance tables created for all basic events may be used for different applications.

Qualitative Criteria for *Risk-Important* Tasks

For those PRA core damage and severe release studies where quantitative measures of risk increase and risk decrease are not available, qualitative criteria, based on expert judgment are employed in identifying *risk-important* tasks. In those cases, input from HRA experts, system designers, M-MIS designers, and human factors specialists are used in identifying *risk-important* tasks.

In addition, the HRA/PRA group, system designers, or M-MIS group determine the human actions or task sequences that need to be analyzed in greater detail (e.g., cases where the current estimates of time to completion is close to the time window available for completion, or cases where the nature of the operator activities required, or the demands placed on operators are considered to be unique or potentially challenging).

Qualitative Criteria for *Risk-Important* Maintenance, Inspection, Test, and Surveillances

Qualitative criteria is used to identify *risk-important* maintenance, inspection, test, and surveillances (MTIS). *Risk-important* MTIS are identified by examining "risk-significant" Systems, Structures, and Components (SSCs). The criteria used to identify "risk-significant" SSCs are provided in SSAR 16.2, "Reliability Assurance Program." A subset of these "risk-significant" SSCs and a representative set of associated MTIS are selected by an expert panel. This panel is to be comprised of representatives with expertise from relevant groups in the design process, such as systems engineering, reliability engineering, PRA, HFE, and man-machine interface (MMI) design. The set of MTIS tasks identified through the expert panel process are defined to be *risk-important* tasks and examined in task analysis, procedures, M-MIS design, and V&V activities.

2.3 Preliminary Results Based on 1995 PRA Studies

Below are some preliminary results based on applying the deterministic and PRA criteria for critical human actions and the quantitative criteria for *risk-important* tasks to the results of the AP600 PRA studies of core damage and severe release that were performed in 1995. These results are provisional and may change as PRA studies are updated. The results are provided as illustration of the methodology for identifying *risk-important* tasks and the types of human actions that may be identified to be *risk-important*.

As PRA studies are completed and/or updated, quantitative or qualitative criteria for *risk-important* tasks will be applied as applicable to identify *risk-important* tasks.

Critical Human Actions

Based on results of the 1995 PRA there are no critical human actions, as defined in Section 2.1, for the AP600 plant.

***Risk-Important* Tasks Identified for Internal At-Power Events:**

When the risk-important measures and threshold values are applied to the output of the AP600 core damage frequency (Core Damage Frequency Quantification, Feb. 1995), a total of five *risk-important* tasks result from the application of risk increase and risk decrease measures to plant core damage. These are:

- Operator fails to fulfill manual actuation of Automatic Depressurization System (ADS) (ADN-MAN01)

- Operator fails to recognize the need for Reactor Coolant System (RCS) depressurization during small loss-of-coolant accident (SLOCA) (LPM-MAN01)

- Operator fails to recognize the need for RCS depressurization during medium LOCA (MLOCA) (LPM-MAN02)

- Operator fails to manually trip reactor via Protection and Safety Monitoring System (PMS) (ATW-MAN03)

- Conditional probability of ATW-MAN04 (Operator fails to trip reactor) (ATW-MAN04C)

Note that the above *risk-important* tasks relate to either manual ADS actuation or manual reactor trip.

Initiating events are also examined to determine whether there are any cases where operator actions substantially contribute to the frequency of the initiating event. No operator actions have been identified to substantially contribute to the frequency of the initiating event for at-power events.

***Risk-Important* Tasks Identified for Internal At-Power Events based on the Focused PRA:**

When the results of the focused PRA sensitivity study for core damage frequency are examined (Focused PRA for RTNSS Analysis, June, 1995), using a risk increase threshold of 100% and a risk decrease threshold of 5%, no new *risk-important* tasks are identified. A total of three *risk-important* tasks result from the application of risk increase and risk decrease measures to the focused PRA for plant core damage. These are:

- Operator fails to fulfill manual actuation of ADS (ADN-MAN01)
- Operator fails to recognize the need for RCS depressurization during SLOCA (LPM-MAN01)
- Operator fails to manually trip reactor via PMS (ATW-MAN03)

Note that all three of these operator actions were already identified to be *risk-important* based on the internal at-power events PRA.

***Risk-Important* Tasks Identified for Internal Shutdown Events:**

When the *risk-important* measures and threshold values are applied to the output of the AP600 core damage frequency for shutdown events (Low Power and Shutdown Assessment, June 1995) a total of three *risk-important* tasks result from the application of risk increase and risk decrease measures. These are:

- Operator fails to recognize a need for RCS depressurization (LPM-MAN-05)
- Operator fails to open two IRWST Motor-Operated Valves (MOVs) (IWN-MAN-00)
- Operator fails to recognize the need to open Normal Residual Heat Removal (RNS) MOV V023 (RHN-MAN-05)

Initiating events are also examined to determine whether there are any cases where operator actions substantially contribute to the frequency of the initiating event. Three initiating events were identified that met the criteria for risk increase and/or risk decrease and where assumptions of a human error substantially contributed to the frequency of the initiating event. These initiating events are:

- RCS overdrain during drainage to mid-loop condition initiating event occurs

- LOCA due to inadvertent opening of RNS-V024 initiating event occurs -- hot/cold shutdown
- LOCA due to inadvertent opening of RNS-V024 initiating event occurs -- RCS drained

There are three operator actions identified that substantially contribute to these initiating events and are therefore considered *risk-important* tasks:

- Failure to align the RNS to provide a diversion path to the in-containment refueling water storage tank (IRWST) during cold shutdown, and terminate the event by reclosing the valve

- Failure to observe failure of the hot-leg-level instruments and failure to close the air-operated valves chemical and volume control system (CVS)-V045 and V047 to preclude initial overdraining of the RCS, during draining of the system to mid-loop

- Failure to detect failure of automatic closure of air-operated valves CVS-V045 and V047, and failure to manually close the valves, when low hot-leg-level is reached during draining of the system to midloop

***Risk-Important* Tasks Identified for Internal Shutdown Events based on the Focused PRA:**

When the results of the focused PRA sensitivity study for core damage frequency are examined (Focused PRA for RTNSS Analysis, June, 1995), using a risk increase threshold of 100% and a risk decrease threshold of 5%, no new *risk-important* tasks are identified for shutdown events. A total of one *risk-important* task results from the application of risk increase and risk decrease measures to the focused PRA sensitivity study for shutdown events. This is:

- Operator fails to open two IRWST MOVs (IWN-MAN-00)

Note this operator action was already identified to be *risk-important* based on the shutdown PRA.

3.0 TASK ANALYSES FOR CRITICAL HUMAN ACTIONS AND RISK-IMPORTANT TASKS

The HRA/PRA group specify human actions and task sequences to be used as input to the task analyses performed as part of the HFE program. This includes all critical human actions (if any) and *risk-important* human actions.

3.1 Input to Operational Sequence Task Analyses

The human actions and tasks identified by HRA activities are included in the set of tasks examined using operational sequence task analyses (Description of Operational Sequence Analysis in AP600 Task Analysis Description Document). The inputs to the task analyses include a specification of the task sequences to be performed as well as any performance requirements, such as time windows within which an action needs to be completed. This input guides the design of the M-MIS and the development of the procedures so as to adequately support these *risk-important* tasks.

The MMI and procedures groups submit results of their analyses (e.g., function-based task analyses; operational sequence task analyses) and design activities (e.g., emergency response guidelines (ERGs), functional requirement documents; display descriptions) to the HRA group for review and comment.

3.2 Confirming/Refining HRA Assumptions

HRAs conducted early in the design process, necessarily make assumptions about function allocation, human actions performed, and the quality of the M-MIS design, procedures, and related performance shaping factors, that are confirmed or refined as the design effort progresses.

Once man-machine function allocation becomes finalized, and initial M-MIS designs and procedures are completed, it becomes possible to perform more detailed sequential task analyses that more accurately reflect details of the design. At this point it becomes possible to examine the impact of advanced digital technology, and the details of the M-MIS design and procedures, on the operator actions to be performed, the demands they place on the operator, and the estimated duration time to complete them.

When initial M-MIS designs and procedures are completed, more detailed operational sequence task and workload analyses are performed to obtain more accurate estimates of workload and task completion times for the set of tasks identified by the HRA/PRA group. (These more detailed operational sequence task analyses are referred to as OSA-2 in the description of AP600 Task Analysis Activities, SSAR subsection 18.8.2.5.) The results are documented in a report, and provided to the HRA/PRA group.

The HRA/PRA group then reviews the HFE design and analysis documents for potential impact on HRA assumptions.

4.0 RE-EXAMINATION OF CRITICAL HUMAN ACTIONS AND RISK-IMPORTANT TASKS

If, based on the results of Section 3.0, a critical human action or *risk-important* task is determined to be a potentially significant contributor to risk, it is re-examined by task analysis, M-MIS design, and procedure development, to identify changes to the operator task or the control and display environment to reduce the likelihood of operator error and provide for error detection and recovery capability.

5.0 VALIDATION OF HRA PERFORMANCE ASSUMPTIONS

Validation of HRA operator performance assumptions is performed as part of the Integrated HFE System Validation.

The HRA/PRA group identifies scenarios that involve critical or *risk-important* human actions that are included as part of the set of scenarios used in the Integrated HFE System Validation.

The HRA/PRA group identifies specific performance assumptions that they would like confirmed as part of the validation exercises. Examples of assumptions to be confirmed are: that particular actions needing to be performed are satisfactorily completed, and that they are completed within the time-window specified in the PRA.

The scenarios indicated by the HRA/PRA group are included as part of the Integrated HFE System Validation, and performance measures are collected to support confirmation of the HRA performance assumptions. The results of the analyses are provided to the HRA/PRA group.

No attempt is made to validate the quantitative HRA probabilities.

After reviewing the results of the Integrated HFE System Validation, the HRA/PRA group determines whether any changes need to be made to the HRA modeling assumptions and whether any changes are required to the HRA quantification. If such is determined to be necessary, the HRA is modified, and the impact on the PRA is assessed.

As part of the process of determining whether HRA requantification is necessary, the HRA/PRA group assesses whether the technique for human error rate prediction (THERP) error frequency data base currently employed to generate error probability estimates continues to be the most appropriate source for HRA quantification, or whether new error quantification data bases that more closely match the AP600 modeling assumptions and are accepted by the NRC, have become available.

A report is generated documenting the results of the exercises intended to validate the HRA performance assumptions, and the impact on HRA/PRA quantification, if any. This report is submitted to the NRC for review and constitutes the analysis results report for Element 6 of the Human Factors Engineering Program Review Model (NUREG-0711).

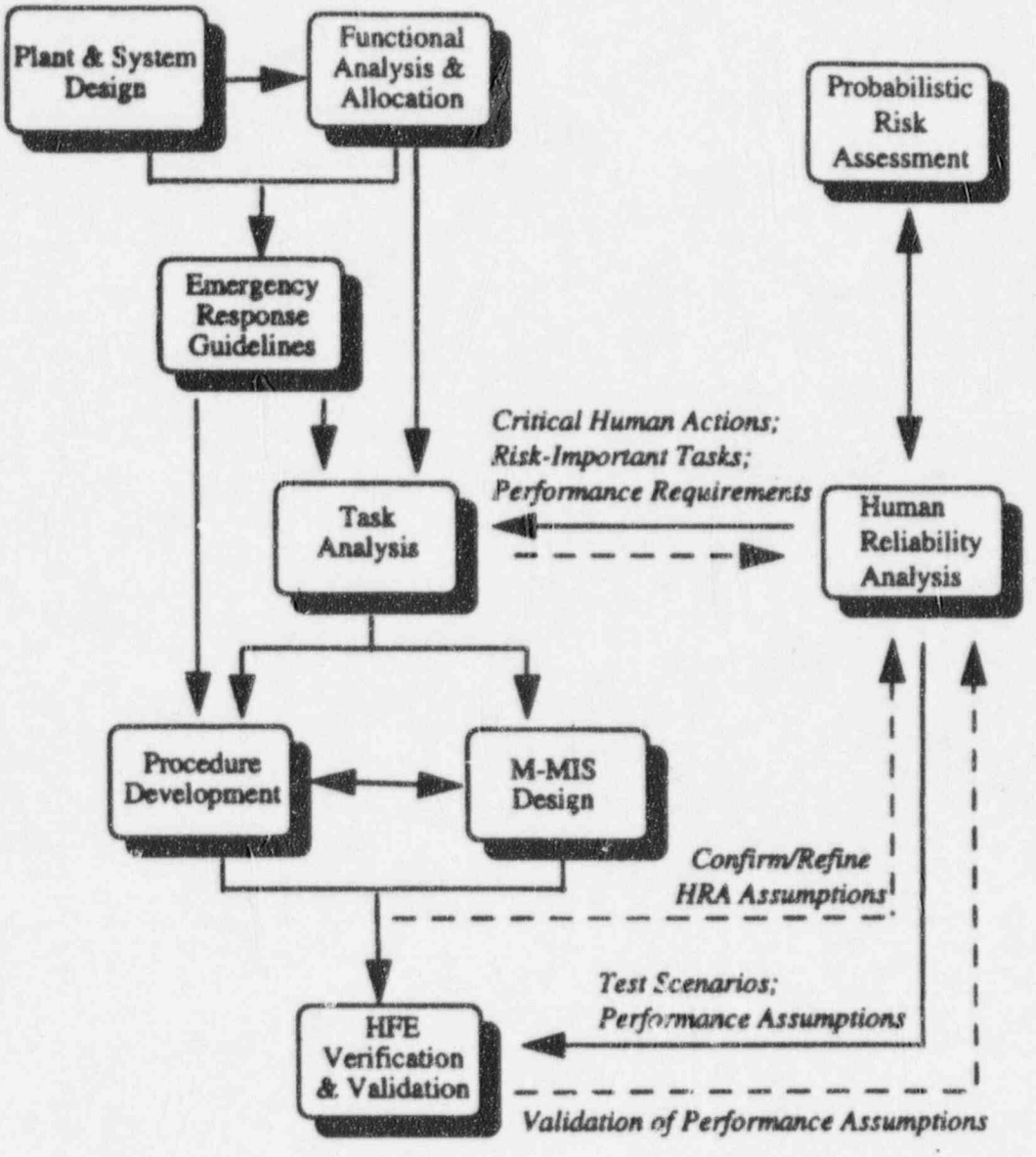

Figure 1. Overview of How HRA Activities are Integrated in the HFE Program