ENCLOSURE 1

MFN 06-075

Licensing Topical Report

NEDO-33267, "ESBWR Human Factors Engineering Human Reliability Analysis Implementation Plan," March 2006

GE Energy
Nuclear

3901
Castle Hayne Rd
Wilmington, NC 28401

NEDO-33267
Class I
DRF# 0000-0051-6713
March 2006

LICENSING TOPICAL REPORT

ESBWR HUMAN FACTORS ENGINEERING HUMAN RELIABILITY ANALYSIS IMPLEMENTATION PLAN

INFORMATION NOTICE

This document NEDO-33267, Revision 0, contains no proprietary information.

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT PLEASE READ CAREFULLY

The information contained in this document is furnished for the purpose of obtaining NRC approval of the ESBWR Certification and implementation. The only undertakings of General Electric Company with respect to information in this document are contained in contracts between General Electric Company and participating utilities, and nothing contained in this document shall be construed as changing those contracts. The use of this information by anyone other than that for which it is intended is not authorized; and with respect to **any unauthorized use**, General Electric Company makes no representation or warranty, and assumes no liability as to the completeness, accuracy, or usefulness of the information contained in this document.

Table of Contents

List of Tables

List of Figures

1 Introduction

For advanced nuclear power plants such as the ESBWR, the NRC expects that vendors will address severe accidents during the design stage using PRA tools. This will allow the designers to take full advantage of the insights gained from the probabilistic safety assessments, operating experience, severe accident research, and accident analysis by designing features to reduce the likelihood that severe accidents will occur and, in the unlikely occurrence of a severe accident, to mitigate the consequences of such an accident. Incorporating insights and design features during the design phase is more cost effective than modifying existing plants.

Quantification of human interactions is a needed element for making risk-informed performance-based decisions in the context of severe accident sequences. The human reliability analysis (HRA) element of a risk enhances understanding of the impact that operator actions have on measures such as core damage frequency (CDF), and large early release frequency (LERF). The HRA also supports evaluation of margins to safety goals on these risk measures.

Many risk based vulnerability assessments take little credit for planned operator actions that can be taken to avert potential accident conditions or mitigate their consequences, since there is a perceived difficulty in providing quantitative estimates of human reliability due to a lack of data. Key factors that control this operational defense-in-depth element are:

1. Ability of the HSI to detect and present abnormal conditions to the operators,
2. Selection of personnel with abilities for plant and control room operations,
3. General training of operators,
4. Level of operator training for specific actions,
5. Robustness of the procedures for a wide range of accident conditions, and
6. Availability of HSI instruments for monitoring, controlling, and providing feedback on actions taken in response to specific events.

Human reliability analysis (HRA) is a required activity of a probabilistic risk assessment (PRA) for both pre- and post-initiator human actions [ASME, 2002]. This input to the Human Factor Engineering process provides a means for prioritizing the HSI needs based on specific human actions that contribute to the overall safety of the plant.

The use of HRA in the ESBWR HFE will be conducted to screen for important human actions and evaluate their potential for, and mechanisms of, human errors that impact the

frequency of key accident scenarios defined in the PRA. Thus, HRA is an essential tool for identifying, screening and evaluating specific human actions based on the impact of potential errors on plant safety. The HRA also supports the HFE design goal of minimizing personnel errors, detecting errors when they do occur, and recovering from errors and hardware failures through careful design of the HSI. HRA is expected to provide valuable insight into desirable characteristics of the HSI design as the design evolves. Consequently, the HFE design effort will give special attention to those plant scenarios, risk-important human actions, and HSIs that have been identified by PRA/HRA as being important to plant safety and reliability.

1.1 Purpose

This implementation plan describes how information generated by HRA tools can be used to support the HSI HFE design goals. The initial "design level" ESBWR PRA/HRA is submitted in support of NRC licensing requirements using an HSI reference design with generic features from ABWRs. The key ESBWR design features of passive safety systems and natural circulation in the core change the way traditional defense in depth barriers are protected. The design features are also reflected in the design of the HSI as well as updates to advances in control and display technology (e.g., analog to digital).

Risk-informed decision-making can be used to justify the design specific licensing basis for the ESBWR. Changes from the traditional BWR licensing basis will meet a set of key principles. These principles are written in terms typically used in traditional engineering decisions (e.g., defense in depth). While written in these terms, it is understood that risk analysis techniques are encouraged to help ensure and demonstrate that these principles are met. From RG 1.174 they are:

- The proposed change meets the current regulations unless it is explicitly related to a requested exemption or rule change, i.e., a "specific exemption" under 10 CFR 50.12 or a "petition for rulemaking" under 10 CFR 2.802.
- The proposed change is consistent with the defense-in-depth philosophy.
- The proposed change maintains sufficient safety margins.
- When proposed changes result in an increase in core damage frequency or risk, the increases should be small and consistent with the intent of the Commission's Safety Goal Policy Statement.
- The impact of the proposed change should be monitored using performance measurement strategies.

HRA updates will address the impact of human-error mechanisms on the ESBWR HSI design. Through update iterations with the PRA model the impact of HSI changes on core damage frequency and large early release frequency evaluations can be assessed. The evaluations will permit evaluations of the greater margins to safety inherent in the ESBWR HSI over established safety goals (e.g., RG 1.174).

Human errors identified and quantified in the PRA will be analyzed to determine if new or modified HSI design features are needed to reduce the likelihood and impact of those errors on accident sequences. The HRA activity will both qualitatively and quantitatively link the HFE program into the PRA and risk analysis. In addition, the results will be design input to the software safety plan activities.

More specific operator requirements for maintaining plant safety and availability goals over the complete range of transient event conditions will be clarified through systematic examination of the functions, tasks, known priorities, risk importance, procedures and training. Any resulting changes in the recommended baseline ESBWR plant S&Q will be provided in revisions to S&Q Results Summary Report document. The recommended staffing level will be reflected in procedures and training program design.

1.2 Scope

This plan establishes a HRA process in conformance with the ESBWR MMIS Design Implementation Plan [2.1(2)], and NUREG-0711r2, Human Factors Engineering Program Review Model [2.3(4)]. The interaction of the HRA tasks with other HFE tasks is shown in Figure 1.

The scope of this plan includes the following:

- Developing a process for using HRA to support the design of the ESBWR HSI. An initial working process is shown in Figure 2.
- Identifying and selecting HRA elements and key actions that impact the quantitative risk estimates.
- Clarifying the role of operators, through the man machine information interface applicability, emergency procedures and training, for protecting the plant from accident challenges.
- Iterating with the risk assessment, task analysis, and operating experience data to reevaluate the impact of operator actions on measures of risk as a function of changes to the HSI (e.g., modeling the impact on human reliability of proposed HSI designs in different modes of operation and transitions between modes.)

- Updating and integrating the quantification of HRA elements as needed using available data, information interface, performance shaping factors and quantification models.
- Evaluating the effect of operator actions on uncertainties and sensitivities associated with the event sequence.
- Providing input to the HFE Issue Tracking System (HFEITS).

1.3 Definitions

The terms below are defined to provide a common basis for interactions between the HRA and the Task Analysis and are referred to in the subsequent paragraphs.

Accident class: A grouping of severe accidents with similar characteristics (such as accidents initiated by a transient with a loss of decay heat removal, loss of coolant Accidents, station blackout accidents, and containment bypass accidents). (ASME PRA Std.)

Accident sequence: a representation in terms of an initiating event followed by a combination of system, function and operator errors or successes, of an accident that can lead to undesired consequences, with a specified end state (e.g., core damage or large early release). An accident sequence may contain many unique variations of events (minimal cut sets) that are similar. (ASME PRA Std.)

Accident situation: from the operator's perspective, an abnormal plant state occurring during an event, which may lead to a new damage condition. Operating crews' actions can prevent, mitigate or exacerbate the accident progression using the HSI. (IEEE working group)

Action task: The "doing" portion of a task, performed by the control room operators or the plant technicians. This involves use of the HSI to perform physical actions in operating control room switches by the control room operators or manipulating or repairing equipment in the plant by the technicians.

At power: those plant operating states characterized by the reactor being critical and producing power, with automatic actuation of critical safety systems not blocked and with essential support systems aligned in their normal power operation configuration.

Cognitive process: An internal, human activity that receives, manipulates, and stores knowledge or information, or which controls actions according to this knowledge.

Cognitive task: The thinking portion of a task, often performed by the control room operators. This involves identifying the cue, the present condition or state of the plant

based on information from the HSI and determining the proper recovery action(s) to be performed using emergency procedures.

Consequences: The results of (i.e., events that follow and depend upon) a specified event.

Contingencies: Pre-thought out plans for mitigating undesired events that occur during plant operations.

Control Function: "Keeping measured functional parameters within bounds though a process of manipulating low level functions to satisfy a higher level function" (NUREG-0711, Rev. 2, page 96)

Control Room Design team (CRDT): is a subset of the Design Team. The CRDT is responsible for the overall coordination of the design of the Main Control Room (MCR), Remote Shutdown System (RSD) Panels, and applicable Local Control Stations.

Crew: The group of people at the plant that manage and perform activities that are modeled in the PRA and are necessary to operate the plant and maintain its safety

Diagnosis: examination and evaluation of data from the HSI to determine either the condition of a system structures and components (SSC) or the cause of the condition (ASME PRA Std.)

Emergency Response Guidelines: Guidelines developed by the BWR owners group to help each BWR plant develop plant specific emergency operating procedures that are qualitatively consistent with other BWR plants but use unique plant quantitative set points to trigger actions.

Expanded Operator Action Tree (EOAT): a logic tree that combines two or more OATs into logic that describes human error mechanisms in relation to an accident sequence. EOATs are generally applied to the nodes in an event tree or to groups of cutsets. (See Appendix A)

Failure mechanism: any of the processes that results in failure modes, including chemical, electrical, mechanical, physical, thermal, and human error (ASME PRA Std.)

Failure mode: a condition or degradation mechanism that precludes the successful operation of a piece of equipment, a component, or a system (ASME PRA Std.)

Framework: A systematic organization of tasks or activities used in a specified type of analysis.

Front-line system: an engineered safety system used to provide core or containment cooling, reactivity control or pressure control, and to prevent core damage, reactor coolant system failure, or containment failure (ASME PRA Std.)

Function: an activity or role performed by a human, structure, or automated system to fulfill an objective (System Functional Requirements Analysis Implementation Plan).

Human Action (HA): a manual response to a cue involving one person to achieve one task or objective. Potentially risk important actions affect equipment or physical systems. Single human actions can be represented as an event in a fault tree or branch point in an event tree.

Human Error Probability (HEP): a measure of the likelihood that plant personnel will fail to initiate the correct, required, or specified action or response in a given situation, or by commission performs the wrong action (ASME PRA Std.)

Human error recovery: The human ability to recognize and correct an error before the error becomes irreversible.

Human error: Can be defined as a mismatch between a performance demand and the human capability to satisfy that demand.

Human Failure Event: An integrated logic description of HEPs based on the error modes, performance shaping factor assessment, and other qualitative information needed to justify a single input to the risk model (ASME PRA Std.)

Human Interactions (HI): A set of Human Actions that affects equipment or physical systems, or an action that influences other human actions. Human interactions can be represented as an event in a fault tree or branch point in an event tree.

Human Reliability Analysis (HRA): a structured approach used to identify potential human failure events and to systematically estimate the probability of those errors using data, models, or expert judgment (ASME PRA Std.)

Human Task: The activity of a human required to accomplish a function. For example the human user conserves, reduces, or adds information, and supplies or controls energy.

Human-induced initiators: Errors in human activities conducted during normal operation that cause an off normal condition and are typically included as contributors to initiating events or revealed system faults (i. e., Type B human errors).

Human-System Interface (HSI): The organization of inputs and outputs used by personnel at a location to interact with the plant, including the alarms, displays, controls,

and job performance aids. Generically, this includes interfaces that support actions for monitoring, responding to events, maintenance, test, and inspection.

Inherent design features: Reliance on physical properties of systems, structures and components to meet design goals rather than relying on supplemental systems to achieve design goal functions. For example, using properties associated with neutron flux in reactor cores to control reactivity via introduction of voids in the core versus changing control rod position.

Initiating event: any event either internal or external to the plant that perturbs the steady state operation of the plant, if operating, thereby initiating an abnormal event such as transient or LOCA within the plant. Initiating events trigger sequences of events that challenge plant control and safety systems whose failure could potentially lead to core damage or large early release

Intervention: Countermeasures that can be taken (during the design) to either prevent errors from occurring in the first place or correct them once they do occur. Interventions can include tools, computers, software, training, procedures and documentation, guidelines, work practices, man-machine interface, job performance aids, support systems, and work planning aids.

Local Control Station (LCS): An operator interface related to nuclear power plant (NPP) process control that is not located in the main control room. This includes multifunction panels, as well as single-function LCSs such as controls (e.g., valves, switches, and breakers) and displays (e.g., meters) that are operated or consulted during normal, abnormal, or emergency operations.

Machine Task: the activity of a machine in accomplishing a function by supplying whatever information or energy is required. The machine includes both hardware and software.

Maintenance: activities carried out to keep systems and equipment available. Specific types of maintenance include preventive, and corrective. Activities associated with preventive maintenance include testing, surveillance, inspection, and calibration. Activities associated with corrective maintenance include repair, replace, and modify.

Mistake: a category of human errors where a wrong action was taken or the correct action was not taken because the intent for the action was formed incorrectly.

Man-Machine Interface Systems (MMIS): In general the MMIS encompasses all instrumentation and control systems provided as part of the ESBWR for use in performing the monitoring, control, alarming, and protection functions associated with all

modes of plant normal operation (i.e., startup, shutdown, standby, power operation, and refueling) as well as off-normal, emergency, and accident conditions. The details of the MMIS systems which perform the monitoring, control, and protection functions are defined in Chapter 7 of the ESBWR DCD.

MMIS Design Team (Design Team): a team of engineers, as defined in the MMIS Design Implementation Plan, who are responsible for the design of the MMIS systems.

Operating time: total time during which components or systems are performing their designed function (ASME PRA Std.)

Operational experience review (OER): a systematic review, analysis and evaluation of operational experience that can apply to the development of the man machine interface design.

Operator Action tree (OAT): a logic tree that expands the single HEP estimate into its subcomponent failure modes based on the elements of cognitive processing and implementation. (See Appendix A)

Passive safety system: the design of systems and barriers to achieve a function (safety or operational) or increase a safety margin without using active components (such as pumps, valves that change state, use of external electric power, or a human action to operate the system). For example, use of natural circulation versus forced cooling to remove heat.

Performance shaping factor (PSF): a factor that influences human error probabilities as considered in a PRA's human reliability analysis and includes such items as level of training, quality/availability of procedural guidance, time available to perform an action, etc. (ASME PRA Std.)

Plant-specific data: data consisting of observed sample data from the plant being analyzed (ASME PRA Std.)

Post-initiator actions: After a transient has been initiated, human actions are often required to return the plant to normal operation or achieve a safe plant shutdown. These actions are typically described in procedures. Errors in the procedural response actions or additional component failures, lead to new situations where operators must recover inoperable equipment or find alternative methods for controlling the event. Such recovery actions are not specifically described in procedures, but rely on the training knowledge of the crew. Human actions that required a defined response and/or equipment restoration can be defined in the PRA from review of the cutsets, accident sequences or grouped scenarios (i.e., Type C human errors).

Post-initiator human failure events: human failure events that represent the impact of human errors committed during actions performed in response to an accident initiator (ASME PRA Std.)

Pre-initiator actions: human activities such as maintenance, testing and calibration conducted during normal operation can either correct a previously unrevealed fault or lead to inoperable equipment without causing a transient. The important errors are those that defeat redundant or diverse systems required for safety and leave the system in an unrevealed fault state (i. e., Type A latent human errors).

Pre-initiator human failure events: human failure events that represent the impact of human errors committed during actions performed prior to the initiation of an accident, (e.g., during maintenance or the use of calibration procedures) (ASME PRA Std.)

Reactor safety: the development of a reactor design that is built and operated to pose no undue risk to public (ANS position paper). This means that the core is protected from damage under design basis events and the risk from PRA core damage sequences is mitigated through design features, backup systems and operator actions. Additional protection from radiation release is from the containment barrier.

Recovery action: a human action performed to regain equipment or system operability from a specific failure or human error in order to mitigate or reduce the consequences of the failure. (ASME PRA Std.)

Recovery: a general term describing restoration and repair acts required to change the initial or current state of a system or component into a position or condition needed to accomplish a desired function for a given plant state (ASME PRA Std.)

Response: to react to a cue for action in initiating or recovering a desired function.

Revealed Fault: a system or plant fault that is immediately detectable by observation or instruments. They stem from either hardware faults or human induced initiators (Type B human errors).

Safety systems: those systems that are designed to prevent or mitigate a design-basis accident. (ASME PRA Std. amplified)

Screening analysis: an analysis that eliminates items from further consideration based on their negligible contribution to the probability of a significant accident or its consequences. (ASME PRA Std.)

Screening criteria: the values and conditions used to determine whether an item is a negligible contributor to the probability of an accident sequence or its consequences. (ASME PRA Std.)

Severe accident: an accident that involves extensive core damage and fission product release into the reactor vessel and containment, with potential release to the environment. (ASME PRA Std.)

Slip: a category of human errors, where the intent to take the correct action was formed, but because of the physical or mental environment a wrong action is taken or the correct action is not taken.

Success criteria: criteria for establishing the minimum number or combinations of systems or components required to operate, or minimum levels of performance per component during a specific period of time, to ensure that the safety functions are satisfied. (ASME PRA Std.)

Support system: a system that provides a support function (e.g., electric power, control power, or cooling) for one or more other systems. (ASME PRA Std.)

System failure: termination of the ability of a system to perform any one of its critical design functions. Note: Failure of a line/train within a system may occur in such a way that the system retains its ability to perform all its required functions; in this case, the system has not failed. (ASME PRA Std.)

Task: a collection of activities with an identifiable start and end point for which human actions are performed.

Unavailability: the fraction of time that a system or component is not capable of supporting its function including but not limited to the time it is disabled for test or maintenance (ASME PRA Std.)

Unrevealed fault: a system or plant fault undetected by observation or instruments. They stem from either undetected hardware faults or pre-initiator human errors (Type A human errors).

2 References

For all references listed below, revision numbers if applicable have been omitted; the latest revision available is assumed to be the current reference.

2.1 Supporting Documents

1. ESBWR DCD Chapter 18 revision 1, January 2006 (GE 26A6642BX)
2. ESBWR DCD Chapter 19 Revision 0, August 2005 (GE 26A6642BZ)
3. Distributed Control and Information System (DCIS) Hardware/Software Specification
4. Operational Experience Review (OER) Plan
5. System Functional Requirements Analysis Implementation Plan
6. Allocation of Functions Implementation Plan
7. Task Analysis Implementation Plan
8. Human System Interface Design Implementation Plan
9. Staffing and Qualifications Implementation Plan
10. Procedure Development Plan
11. Training Program Development Plan.
12. Human Factors Verification & Validation Implementation Plan
13. Human Performance Monitoring Plan

2.2 Codes and Standards

1. ANSI/ANS 58.8-1994, "Time Response Design Criteria for Safety-Related Operator Actions"
2. ASME, "Standard for Probabilistic Risk Assessment For Nuclear Power Plant Applications," ASME RA-S-2002, April 5, 2002;
3. IEEE Standard 1082, "Guide for Incorporating Human Action Reliability Analysis for Nuclear Power Generating Stations," IEEE 1997;
4. ANSI/IEEE Std. 1023, IEEE Guide to the Application of Human Factors Engineering to Systems, Equipment and Facilities of Nuclear Power Generating Stations, (IEEE);

2.3 Regulatory Requirements and Guidelines

1. NUREG-0700, Rev.2, Guidelines for Control Room Design Reviews, 1981, (US Nuclear Regulatory Commission)
2. NUREG-0711, Rev.2, Human Factors Engineering Program Review Model, 2004, (U.S. Nuclear Regulatory Commission)
3. NUREG-1123 "Knowledge and Abilities Catalog for Nuclear Power Plant Operators: Boiling Water Reactors. 1995 (US Nuclear Regulatory Commission).
4. NUREG-1649: Reactor Oversight Process 2000; (US Nuclear Regulatory Commission)
5. NUREG-0737, Clarification of TMI Action Plan Requirements (Supplement 1 to R.G. 0737 and Item I.C.5, "Feedback of Operating Experience to Plant Staff"); (US Nuclear Regulatory Commission).
6. NUREG-0933 A Prioritization of Generic Safety Issues, Supplements HF (US NRC 2004).
7. Regulatory Guide 1.174 – "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis." Revision 1 2002.
8. NUREG-0800: Standard Review Plan: Chapter 19, Use of Probabilistic Risk Assessment in Plant-Specific, Risk-Informed Decision Making: General Guidance (NRC (2002).
9. NUREG-0800, Standard Review Plan, Chapter 18.
10. NUREG-0654 "Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants, 1980 addenda, 1980.
11. NUREG-1624, Rev. 1.: Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA) (NRC, 2000).
12. NUREG-1792, "Good Practices for Implementing Human Reliability Analysis (HRA)," Draft Report for Comment, Office of Nuclear Regulatory Research, July 2004.

2.4 Departments of Defense and Energy

1. AD-A226 480, U.S. Army Test and Evaluation Command, Human Factors Engineering, Test Operation Procedure 1-2-610 (Part 1), May 1990.

2. DOE Order 5480.19, Conduct of Operations Requirements for DOE Facilities;

3. MIL-H-46855B, Human Engineering Requirements for Military Systems, Equipment and Facilities (Dept. of Defense) May 1999.

4. MIL-STD 1472C, Human Engineering Design Criteria for Military Systems, Equipment and Facilities, Dept of Defense.

2.5 Industry and Other Documents

1. Dougherty. E. M. & J. R. Fragola, "Human Reliability Analysis: A systems engineering approach with nuclear power plant applications," John Wiley, 1988.

2. EPRI 1003329 "Lesson Plans for Human Reliability Assessments in PSAs," 2002.

3. EPRI NP-3583, "Systematic Human Action Reliability Procedure (SHARP)," 1984.

4. EPRI NP-6560-L. "A Human Reliability Analysis Approach Using Measurements for Individual Plant Examination," 1990.

5. EPRI Report TR-100259, "An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment," 1992.

6. EPRI TP-101711, "SHARP1—A Revised Systematic Human Action Reliability Procedure," 1992.

7. EPRI, NP-4350, Human Engineering Design Guidelines for Maintainability, 1985;

8. EPRI-NP-1567, Human Factor Review of Power Plant Maintainability, (Seminara, 1981).

9. EPRI-NP-2360, Human Factors Methods for Assessing and Enhancing Power Plant Maintainability, (Seminara, 1982).

10. EPRI-NP-3701 Computer-generated Display System Guidelines (Vol. II and I), 1984.

11. Hannaman, G. W., "Basic Concepts For Quantifying Human Reliability in PRAs," PSA 2005, proceedings of American Nuclear Society San Francisco Meeting, Sept. 2005.

12. Hollnagel, E., "Cognitive reliability and error analysis method, CREAM," Elsevier, Oxford, 1998.

13. IAEA-TECDOC-632, ASSET Guidelines: Revised. 1991 Edition, Vienna (1991).

14. INPO 85-017 Rev 2, Guidelines for the Conduct of Operations at Nuclear Power Stations.

15. NRC IN 97-78 "Crediting of Operator Actions in Place of Automatic Actions and Modifications of Operator Actions, Including Response Times," 1997.

16. NUREG/CR-1278, Swain & Guttmann, "Handbook of human reliability analysis with emphasis on nuclear power plant applications," 1983.

17. NUREG/CR-4772, Swain, "Accident Sequence Evaluation Program: Human Reliability Analysis Procedure," 1987.

18. NUREG/CR-6350 "A Technique for Human Error Analysis (ATHEANA)," 1996.

19. NUREG/CR-6883, " The SPAR-H Human Reliability Analysis Method," Idaho National Laboratory, Office of Nuclear Regulatory Research, August 2005.

20. NUS-4531, "Human Cognitive Reliability Model for PRA Analysis," EPRI Gray back report (Hannaman, G. W., A. J. Spurgin, and Y. D. Lukic), Dec 1984.

21. Rasmussen, J. "Information Processing and Human-Machine Interaction," North Holland, New York, 1986.

3 Requirements for HRA Implementation Plan

The specific implementation of the requirements for HRA will be developed by the MMIS design team following the iterative links with the HFE program shown in Figure 1, which leads to an "as designed PRA/HRA" at the completion of design. If such a PRA/HRA model is developed, the plant operators can use it to monitor the risk during periods when specific plant equipment is out of service. The requirements to achieve such a model are:

- The HRA will be performed iteratively using a systematic process as the design progresses.

  The PRA and HRA will be performed early in the design process to provide insights and guidance both for systems design and for HFE purposes. The robustness of the HRA depends, in large part, on the analyst's understanding of personnel tasks, the information related to them, and the factors, which influence human performance.

  Accordingly, the HRA will be updated as the design progresses and the initial PRA/HRA will be finalized when the plant design and HFE are complete.

- The HRA is conducted to screen for important human actions and evaluate their potential for, and mechanisms of, human errors that impact the frequency of key accident scenarios for the PRA.

  Thus, HRA is an essential tool for identifying, screening and evaluating specific human actions based on the impact of potential errors on plant safety.

- The HRA also supports the HFE design goal of minimizing personnel errors, detecting errors when they do occur, and recovering from errors and hardware failures through careful design of the HSI.

  HRA is expected to provide valuable insight into desirable characteristics of the HSI design as the design evolves. Consequently, the HFE design effort will give special attention to those plant scenarios, risk- important human actions, and HSIs that have been identified by PRA/HRA as being important to plant safety and reliability.

- The HRA task will interact with the HFE verification and validation program to provide test scenarios and updating quantitative evaluations based on validation results.

- The HRA models will establish a basis for future human performance monitoring and help prioritize corrective actions.

4 HRA methodology

The requirements for a PRA call for, and support the use of, a systematic process for HRA evaluations. There are a number of HRA modeling approaches in use. They have been classified based on the number of key probability elements (Px) in the HRA models. In the current models there are from one to four probability elements or nodes used for quantification. The elements have been defined based on descriptions of the cognitive and implementation steps required to carry out an action. Examples of the basis for each Px are provided in Appendix A. While the examples are not expected to cover all modeling approaches, because there are varying viewpoints on the depth of analysis needed for PRAs within the community of HRA analysts, the consideration of Px should permit the continued development of new methods for quantification. The advantages and disadvantages for the various models are summarized in the Table 1. The models with two or more quantification nodes can satisfy the ASME PSA Category II and III requirements [ASME RA-S-2002] if the effort is placed on collecting plant specific data as listed in the requirements.

The data to support most approaches are very sparse, and judgment is required for quantification. When data are sparse screening quantifications provide a valuable way of differentiating between the actions that contribute to risk and those that don't. Advanced uses of HRA beyond screening, according to the ASME Standard, require at least the two element assessments for all explicitly modeled human actions in a PRA [ASME RA-S-2002]. The models with two or more quantification nodes can satisfy the ASME Category II and III requirements, if sufficient effort is placed on collecting the needed plant specific data.

The HFE design team will establish specific methodology and modeling approaches by using information from HRA reports on data, models and methods [e.g. from sources such as NUREG/CR-1278, 1983, EPRI NP-3583, 1984, NUREG/CR-4772, 1987, EPRI NP-6560-L 1990, EPRI TR-100259, 1992, NUREG/CR-6350, 1996, Hollnagel, 1998, NUREG-1792, Draft 2004, and NUREG/CR-6883, 2005]. Standards include ASME RA-S-2002, and IEEE Std. 1082-1997. Additional HRA standards are under development by the IEEE.

The HRA inputs include descriptions and analyses of operator functions and task requirements, previous PRA identified actions and errors, performance factors associated with the operational characteristics of HSI design, procedures for normal, startup, shutdown and emergency operations as well as training programs.

Although there are many different approaches for conducting HRAs, there are several analysis components that increase the quality of the HRA. These include:

- Performing a design specific PRA/HRA to identify significant risk reduction improvements relating to the reliability of core and containment heat removal systems that can be practically implemented during the plant design.

  The initial ESBWR PRA includes both internal and external events to the extent possible and these will be upgraded during the design phase. The main output of the PRA/HRA will be a listing of potentially risk-important human interactions.

  These risk important human interactions from the PRA/HRA will be used as input to the HFE program (i.e., to support function allocation analyses, task analyses, HSI design, procedure development, and training). The design effort will demonstrate how these human actions are well supported by the HSI design and that there are suitable crew members available and sufficient time to accomplish the action, given that the need is detected.

- Using a multidisciplinary team to analyze human actions within the context of the PRA.

  For some actions the level III requirements in ASME, 2002 may be applied to support quantification of the risk important human actions in dominant accident sequences. The HRA assumptions involving diagnosis, decision-making, and planning and implementation strategies during accident responses may be validated by event simulations using experienced crews, walkthrough analyses using personnel with operational experience to apply procedures for conditions in plant-specific control room mockup or simulator. Such reviews may be conducted to support final quantification of the PRA.

- Obtaining design information related to those factors that affect human performance.

  These include: accident analyses from design basis events, operational experience, and PRAs to define quantification elements such as the time available for action, HSI design details that indicate the cue for an action and the feedback of the effects of taking the action, task analyses to determine the steps, timing and special tools required to carry out the sub steps of the human action, and the applicability of general or specific written procedures. These items are referred to as performance shaping factors that are managed through the design of the HSI.

- Evaluating the effects of new HSI advanced technology on human performance and the potential to change the human error mechanisms due to advanced technology. The evaluation of new design features will assess at a minimum the following effects on the existing HRA:

- That the original HRA assumptions and assessed error mechanisms are valid for the modified design,
- That the human errors analyzed in the existing HRA are still relevant,
- New error mechanisms that may become important and were not modeled in the existing PRA/HRA,
- That the probability of errors by operators and maintenance personnel may need to be refined to address details of the HSI design, which may require use of a different modeling construct and
- That the consequences of errors, as established in the existing PRA/HRA may change as a result of better HSI design information.

- Analyzing human actions with an emphasis on human error mechanisms.

  The likelihood of operator error will be minimized for risk-important HIs by identifying key error mechanisms and then providing means for error detection and recovery capability within the HSI design, procedures, and training elements under the HFE program.

- Obtaining appropriate sources of human error data for the types of human actions and associated error mechanisms that are modeled including human to human dependencies and dependencies between human actions and hardware failures.

  Performing sensitivity and uncertainty analyses on the human success and error probability estimates within the PRA sequences to evaluate the impact of human errors on the plant systems.

  These analyses will use a variety of importance measures and HRA sensitivity analyses assumptions to ensure that risk important actions are not overlooked.

- Integrating the PRA and HRA activities into plant design activities by defining safety important actions, supporting HSI design, procedures and training element development to ensure that HRA performance factor assumptions are met in the design.

- Providing thorough documentation of the HRA process, including: integration with the HFE elements, methods used, assumptions made and the database for the human error probabilities that feed into the PRA. Such document will support evaluation of future COL applicant changes to the HSI design, as well as providing a basis for risk monitoring tools.

5 HRA Processing Framework

The specific HRA systematic processing framework for supporting the HFE HSI design requirements, obtaining input information and for selecting modeling approaches will be established by the MMIS design team. The HRA will bring risk informed thinking into the HSI design by acting as a bridge between the PRA and HSI design process (i.e., Task Analysis) as shown in Figure 1.

5.1 HRA Interactions with HFE tasks

Figure 1 indicates that the HRA task will receive from the baseline PRA a listing of human interactions modeled in the PRA. The HIs will be ranked by their level of importance using several different important measures. These risk important human interactions from the PRA/HRA will be used as input to the HFE design effort (i.e., to support Function Allocation Analyses, Task Analyses, HSI Design, Procedure Development, and Training). The design effort will demonstrate how these human actions are well supported by the HSI design and that there is suitable crew availability and time to accomplish the action given that the need is detected.

The HRA task will interact with the Task Analysis by providing critical human actions and errors to the Task Analysis and receive from the Task Analysis detailed definitions of tasks defined through the Functional Allocation process.

The HRA will interact with the HFE verification and validation program by supporting the design of test scenarios and updating quantitative evaluations based on validation results. The HRA models will establish a basis for future human performance monitoring and help prioritize corrective actions. The HRA task will permit examination of assumptions used in designing the HSI with regard to the ability of licensed operators to perform needed tasks.

The HRA task will provide information on plant configurations to avoid, and to help prioritize corrective actions to be taken during plant operation.

5.2 HRA Interaction with PRA model

A design specific PRA/HRA is performed to identify significant risk reduction improvements relating to the reliability of core and containment heat removal systems that can be practically implemented during the plant design. In this way the PRA/HRA becomes a tool for evaluating design choices including alternative HSI configurations and displays.

The initial baseline ESBWR PRA study which is described in the ESBWR DCD Chapter 19 will be used as the starting point. The study follows ASME RA-S-2002 as applied to

a conceptual design, and will continue to meet more detailed objectives as the design progresses. The HRA development follows IEEE Std. 1082-1997. The PRA includes both internal and external events to the extent possible during the design phase. The main output will be a listing of potentially risk-important human interactions from the PRA/HRA.

As the design progresses the HRA will update the human error data, which becomes input to the PRA, in terms of logic structure and data changes for requantification. The changes will consider performance shaping factors that reflect the HSI, procedure development, and the training program.

These changes to HIs when incorporated into the PRA will refine evaluations for the reliability of core and containment heat removal systems (e.g., quantification of core damage (CD) frequency for level 1 PRA changes and large early release frequency (LERF) for level 2 PRA updates). The PRA will provide refined importance quantifications that include HIs which show how HSI interface improvements and changes increase margins to the quantitative safety goals.

The basic elements for interaction between the PRA model and HFE HRA task are shown in Figure 2. There are four subtasks for the HRA. These are use of the PRA model to produce importance rankings, qualitative evaluation of the tasks identified in HFE program via task analysis, identifying actions for reassessment in the PRA/HRA, and updating the HRA for input to the PRA.

5.2.1 PRA/HRA probabilistic importance evaluation

The ESBWR conceptual design baseline PRA uses a simple approach for initial human reliability quantification. The initial HRA methodology applied is based on a screening approach for the human interactions (HIs). HIs are qualitatively identified during model development at a functional level rather than specific tasks. The HIs identified during PRA modeling of plant systems have been evaluated considering the time available for the HIs to be performed during both normal operation and accidents.

HIs identified for normal plant operation are both those that cause an initiating event and those that fail to restore equipment to their normal condition following a test and/or maintenance.

Human error probabilities (HEPs) selected for the HIs are based on the maximum value expected based on the time available to perform the action. Until ESBWR design details are established no credit (e. g., a lower HEP value) is allowed for improvements based on special HSI features, additional training or special procedures or instructions.

Four general time periods are considered for human actions that must occur following an initiating event:

(1) HIs that must be completed within 30 minutes

(2) HIs that must be completed within 60 minutes

(3) HIs that must be completed within 24 hours

(4) HIs that must be completed within 72 hours

In this conceptual design HI screening process no credit is taken for actions in the first category (e.g., the HEP =1.0). In general, the failure probability for the other categories is approximately one order of magnitude below the previous (e.g., HEP ~ .1, .01 and .001 for categories 2, 3, and 4).

The output of the initial PRA model is a set of accident sequences that contribute to CD and LERF. The HIs are included in the accident sequence descriptions. The importance ranking tools are then used to determine important systems, structures components, and supporting HIs. Through the review and evaluation of the results insights are developed for those systems, structures and components as well as HIs that need attention during the design and operation.

Since simple screening values have been used for the HRA quantification, the insights about human interactions are not yet fully developed. As the design develops it is important to obtain design information related to those factors that affect human performance. These include: HSI design details that indicate the cue for an action and the feedback of the effects of taking the action, task analyses to determine the steps, timing and special tools required to carry out the sub steps of the human action, and the applicability of general or specific written procedures. Additional HRA support comes from accident analyses of design basis events, operational experience, and key PRA accident sequences to define quantification elements such as the time available for action and system availability. As these details of the HSI design become available, refinements to the PRA through the HRA can be used to upgrade the PRA model to address the HSI issues. When the "as designed elements" from the other plant systems are incorporated into the ESBWR PRA, it will become an "as built PRA/HRA."

5.2.2 HRA qualitative evaluation for HFE tasks

The first HFE HRA sub task is to expand the detailed description of risk important actions currently identified in the ESBWR PRA. The functional allocation and task analysis results will provide a basis for applying more detailed HRA models with expanded elements. The appropriate model can be selected using the guidelines from

Appendix A to link HSI specific performance shaping factors to HRA model. Additional human error data for specific HSI designs can be obtained from tests of the systems using part task simulators during verification and validation.

The second HFE HRA sub task is to reexamine the qualitative basis of HEP. A possible method for linking the initial HRA screening models to more advanced applications is to apply an expanded operator actions tree (EOAT). This process breaks the overall HI into sub elements at the level of HSI design issues that can be quantified for their impact operator error.

The third HFE HRA sub task is to expand the qualitative human error description to meet needs of HSI design objectives. This will provide qualitative assumptions about procedures and training, and other performance shaping factors. Information from HRA reports on data, models and methods from sources such as [NUREG/CR-1278, 1983, EPRI NP-3583, 1984, NUREG/CR-4772, 1987, EPRI NP-6560-L 1990, EPRI TR-100259, 1992, NUREG/CR-6350, 1996, Hollnagel, 1998, Julius, 2001, NUREG-1792, Draft 2004, and NUREG/CR-6883, 2005] provide structures, data and documentation tools.

5.2.3 Identify actions for reassessment in PRA/HRA

The HRA inputs will include descriptions and analyses of operator functions and task requirements, previous PRA identified actions and errors, performance factors associated with the operational characteristics of HSI design, procedures for normal, startup, shutdown and emergency operations as well as training programs.

For some actions the level III requirements in ASME, 2002 may be applied to support quantification of the risk important human actions in dominant accident sequences. The HRA assumptions involving diagnosis, decision-making, and planning and implementation strategies during accident responses may be validated by event simulations using experienced crews, walkthrough analyses using personnel with operational experience to apply procedures for conditions in plant-specific control room mockup or simulator. Such reviews may be conducted to support final quantification of the PRA.

5.2.4 HRA Update evaluation

The goal of this sub task which is shared by the HEF team for qualitative aspects and the PRA modeling team for quantification elements is to regenerate the importance listing for the ESBWR accident sequences. To update the PRA/HRA model the qualitative results developed to support the basis for HSI design selections are used to update the HRA models and data. This is done in detail only for those HIs that can be shown to impact reactor safety.

The following steps as shown in Figure 2 are undertaken to generate each new importance listing.

- Update HEP database and quantify detailed HRA models
- Evaluate dependencies at detailed level (sequence, timing, procedure, training and M
- Evaluate uncertainty in quantitative assessment

Once these elements are completed, the PRA and HFE HRA analysts can develop new insights about the risk of specific manual tasks and the HSI.

5.3 Assumptions for HRA

The ESBWR design represents a major shift in management of reactor safety from active systems that are controlled by both automation and operational staff to passive safety functions that rely primarily on inherent features of the design. These inherent features shift the fundamental operator tasks from manual back up on active systems that protect against CD and LERF, to monitoring and supporting operation of the natural circulation systems during transient events that inherently protect against CD and LERF.

5.3.1 Design impacts

Throughout the design phases the following assumptions support development of, and changes to the HRA models

- The cognitive role for operators that manage reactor safety is expected to change to meet altered ESBWR control and monitoring needs. For conservative HRA evaluations at the accident sequence level, it is assumed that the operators will manage the event sequence using a knowledge based cognitive approach; unless the relevant displays, procedures and charts, which operators would use to manage the sequence specific event, are available for review by the HFE team.
- A licensed operator will remain in control of plant operation through the HSI during all states of operation. During normal operations the operator will monitor the automated control functions, perform automated surveillance and testing, and maintenance tasks allowed with containment sealed.
- One of the considerations in evaluating licensed operators' actions such as maintaining or restoring residual heat removal is the number of operators available and their qualifications in terms of skills, knowledge and training; and applicability of procedures.
- The operator will be able to assume manual control of those functions that have been automated during the function allocation. Operator training will include manual

operation of an automated function that has been returned to manual monitoring and control. Without simulator training or a procedure walk/talk through it is assumed that the crew will use an "opportunistic strategy" for dealing with events, (i.e., base future actions on the most recent information without regard for long term goals). Other strategies are tactical (i.e., follow a preplanned use of known procedures or rules) or strategic (i.e., by considering the global context uses procedures within the circumstances to look ahead and take actions that accomplish long term goals)

- During outage periods the licensed operators remain in control by monitoring the systems that are unavailable during repairs and maintaining sufficient system operation to ensure protection of fuel integrity.

- The shift team will observe appropriate limits and conditions for shift work including overtime, shift duration, and shift rotation. Updates to the HRA models evaluate the workload in terms of available crew both quantitatively and qualitatively.

- The HSI design minimizes the potential for human factor problems that will negatively affect plant safety and performance, (e.g., (1) knowledge, skills and ability of recommended staff can operate and maintain the HSI; (2) the HSI is consistent throughout the MCR and local plant stations for supporting both pre and post initiator actions; (3) maintenance, surveillance and calibration activities using the HSI are not unnecessarily complex; and (4) additions, changes or modifications to the HSI do not violate HRA assumptions). The required level of skill and knowledge can vary significantly depending on the accident sequence. For example, restoration of the shutdown cooling during a normal shutdown can be considered routine, whereas the same action during a loss of station electric power or during a fire can be more challenging and require a significant level of adaptability to effectively use the procedures. This difference is due to the specific HSIs used to provide cues for action and feedback, available crewmembers, their skill and knowledge, and the time allowed for the action. These factors are reflected in the qualitative human action logic and application of sublevel human error probabilities (HEP) to identify overall HEP-related changes to the HRA inputs to the PRA/HRA model.

5.3.2 Pre-initiator HRA

The assumptions for Pre-initiator actions include:

- A systematic process will be used to identify those specific routine test, surveillance calibration and maintenance activities which, if not completed correctly, may impact the availability of equipment necessary to perform system function modeling in the PRA. In many cases the failure rate of equipment includes contributions from human actions.

- Identify those test, surveillance calibration and maintenance activities that if performed incorrectly can have an adverse impact on the automatic initiation of standby safety equipment via review of operating experience typical procedures and concept of design anticipated procedures and work practices.

- Identify those work practices that could introduce a mechanism which simultaneously affects equipment in either different trains of a redundant system or diverse systems (e.g., use of common calibration equipment by the same crew on the same shift, a maintenance or test activity that requires realignment of an entire system). The correction of such a mechanism before the equipment is demanded can be performed either locally or with assistance from the control room. For the control room to be effective in recovering before resuming normal plant operations, the equipment must be instrumented and alarmed. The ESBWR is designed to prevent inadvertent isolation of a standby system. For example, the plant can't be started until the alarm that indicates a closed maintenance valve in the Gravity Driven Cooling System is cleared by opening the valve.

Screening of activities that need not be addressed explicitly in the PRA model will be based on an assessment of how plant-specific operational practices limit the likelihood of errors in such activities.

Test, surveillance and maintenance activities can be screened from the PRA if:

1. The equipment is automatically re-aligned on system demand, following the activities,

2. A post-maintenance functional test is performed that reveals misalignment,

3. Equipment position is indicated in the control room, status is routinely checked, and realignment can be effected from the control room, or·

4. Equipment status is required to be checked frequently (i.e., at least once a shift)

Through the review of plant specific or applicable generic operating experience add failure modes discovered that leave equipment unavailable for response in accident sequences, become a direct cause of an initiating event.

For each activity that is not screened, an appropriate human failure event (HFE) will be defined to characterize the impact of the failure as an unavailability of a component, system, or function modeled in the PRA. Consideration the following issues should be addressed when quantifying pre-initiator actions.

1. Assess the joint probability of the HFEs for dependency with other HFEs (i.e., having some common elements in their causes, such as performed by the same crew in the same time-frame).

2. Provide an assessment of the uncertainty in the HEPs. Use mean values when providing point estimates of HEPs.

3. Check the reasonableness of the HEPs in light of the operating history, procedures, operational practices, and experience. Operating experience may be used to support quantification of impact that test, surveillance, maintenance and calibration activities have on overall system unavailability.

The HEP for pre-initiator human failure events will be performed using a systematic assessment process that addresses the plant-specific and activity-specific influences on human performance. For example, each detailed human error probability assessment, addresses task -specific relevant information such as:

1. The quality of written procedures (for performing tasks) and administrative controls (for independent review), and

2. The quality of the human machine interface based on the equipment configuration, displays, instrumentation type and control layout.

5.3.3 Post Initiator HRA

The assumptions for post-initiator actions are:

A systematic review of relevant functions, task definitions and procedures will be used to identify the set of operator responses required (e.g., HI) for each important accident sequence generated by the PRA. When identifying the key human response actions to initiating event cues:

1. Review the emergency operating procedures, and other relevant procedures (e.g., AOPs, annunciator response procedures) in the context of the accident scenarios, and

2. Review system operation such that an understanding of how the system(s) functions and the human interfaces with the system are obtained.

3. Include in the PRA model those actions required to initiate (for those systems not automatically initiated), operate, control, isolate, or terminate those systems and components used in preventing or mitigating core damage as defined by the success criteria (e.g., operator initiates shutdown cooling).

4. Also include those actions performed by the control room staff either in response to procedural direction or as skill-of-the-craft to recover a failed function, system or component that is used in the performance of a response action in dominant sequences (e. g., manual start of a standby pump following failure of auto-start).

Human failure events will be defined that represent the impact of not properly performing the required responses, consistent with the structure and level of detail of the accident sequences.

1. Analysts can use talk-through (i.e., review in detail) with plant operations and training personnel the procedures and sequence of events to confirm that interpretation of the procedures is consistent with plant observations and training.

2. Analysts can use simulator observations or talk-through with operators to confirm response models for dominant scenarios

A set of Human Failure Events (HFEs) will be defined as unavailability of functions, systems or components as appropriate to the level of detail in the accident sequence and system models. Failures to correctly perform several responses may be grouped into one HFE if the impact of the failures is similar or can be conservatively bounded. Some of this information is available in the Task Analysis. To complete the qualitative definition of the HFE the accident sequence context is specified by including:

- The specific timing of cues, and time window for successful completion,
- The accident sequence specific procedural guidance (e. g., AOPs and EOPs),
- The availability of cues and other indications for detection and evaluation errors, and
- The specific detailed tasks (e.g., component level) required to achieve the goal of the response.

The assessment of the probabilities of the post-initiator HFEs will be performed using a well defined and self-consistent process that addresses the plant-specific and scenario-specific influences on human performance, and addresses potential dependencies between human failure events in the same accident sequence

Example models for performing detailed estimation of the HEPs of the HFEs are shown in Appendix A. The approach should addresses failure in cognition as well as failure to execute tasks. When estimating HEPs the impact of performance shaping factors the following plant-specific and scenario specific examples can be considered in the evaluation. The analysis is not limited to these specific items should others become important.

a. Quality (type (classroom or simulator) and frequency) of the operator training or experience

b. Quality of the written procedures and administrative controls

c. Availability of instrumentation needed to take corrective actions

d. Degree of clarity of the cues/indications

e. Human System Interface

f. Complexity of the required response

g. Environment (e.g., lighting, heat, radiation) under which the operator is working

h. Accessibility of the equipment requiring manipulation

i. Necessity, adequacy, and availability of special tools, parts, clothing, etc., and

j. Time Available and Time Required.

When long time periods are available screening can be used. The time available to complete actions should be based on plant-specific thermal/hydraulic analysis, or simulations. The time window is determined by the point in time at which operators are expected to receive relevant indications and the estimate of time available. The time for implementation of HFEs in dominant scenarios on actual time measurements in either walkthroughs or talk-through of the procedures or simulator observations.

Recovery actions (at the cutset or scenario level) may be modeled if it has been demonstrated that the action is plausible and feasible for those scenarios to which they are applied. Estimates of probabilities of failure will address dependency on prior human failures in the scenario. The relative consistency of the post-initiator HEP quantifications is evaluated by checking the following:

1. Review the HFEs and their final HEPs relative to each other to check their reasonableness given the scenario context, plant history, procedures, operational practices and experience.

2. For multiple human actions in the same accident sequence or cut set, assess the degree of dependence. This limits the problems associated multiplying HFEs that are assumed to be independent, but are not. For example, the models can account for the influence of success or failure in preceding human actions and system performance on the human event under consideration including:

- The time required to complete all actions in relation to the time available to perform the actions, and
- Factors that could lead to dependence (e.g., common instrumentation, common procedures, increased stress, etc.).

3. Define and justify the minimum probability to be used for the joint probability of multiple human errors occurring in a given cutset.
4. Finally, characterize the uncertainty in the estimates of the HEPs, and use mean values for quantification of the PRA results.

5.4 HRA Risk Importance for HSI Design Updates

The set of HIs defined in the PRA will be used during the ESBWR HFE design effort to support evaluations of the risk importance of personnel interactions with plant systems, HSIs, procedures, and training that involve new concepts within the MMIS ESBWR design. Consideration will be given to the following effects on HRA when modifications from previous designs and concept of design changes for the ESBWR are introduced:

1. whether the HRA assumptions used for reference design remain valid for the ESBWR design,
2. whether the human errors analyzed in the reference design HRAs are still relevant for the ESBWR,
3. whether the probability of errors by operators and maintenance personnel may change when considering the ESBWR HSI,
4. whether errors may be introduced by ESBWR HSI design features that are not modeled by reference design HRA and PRA, and
5. whether the consequences of errors, established in the reference design HRAs, may change for the ESBWR.

The qualitative answers to these questions indicate the need for requantification of an HI.

5.5 HRA Documentation

The HRA for both Pre- and Post- initiators will be documented in a manner that facilitates PRA applications, upgrades to the model and peer review. The HRA for both Pre- and Post- initiators will be documented in a manner that facilitates PRA applications, upgrades to the model and peer review. An example HRA will be documented in enough detail to permit reviewers to reproduce results and understand limitations imposed by the models, assumptions, and data, including the following:

A discussion of the HRA methodology and process used to identify pre- and post-initiator HEPs· should be included.

Generic and plant specific assumptions that were made in the HRA, including:

- The bases for the assumptions, and
- Their impact on the CDF and LERF results.

Factors used in the quantification of the human action, how they were derived (their bases), and how they were incorporated into the quantification process·

Source(s) of data used to quantify human actions, including:

- Screening values and their bases
- Best estimates with uncertainties and their bases
- The method and treatment of dependencies for post-initiator actions
- A listing of all pre- and post-initiator human actions evaluated by model, system, initiating event and function
- A listing of all HEPs for each post-initiator human action and significant dependency effects

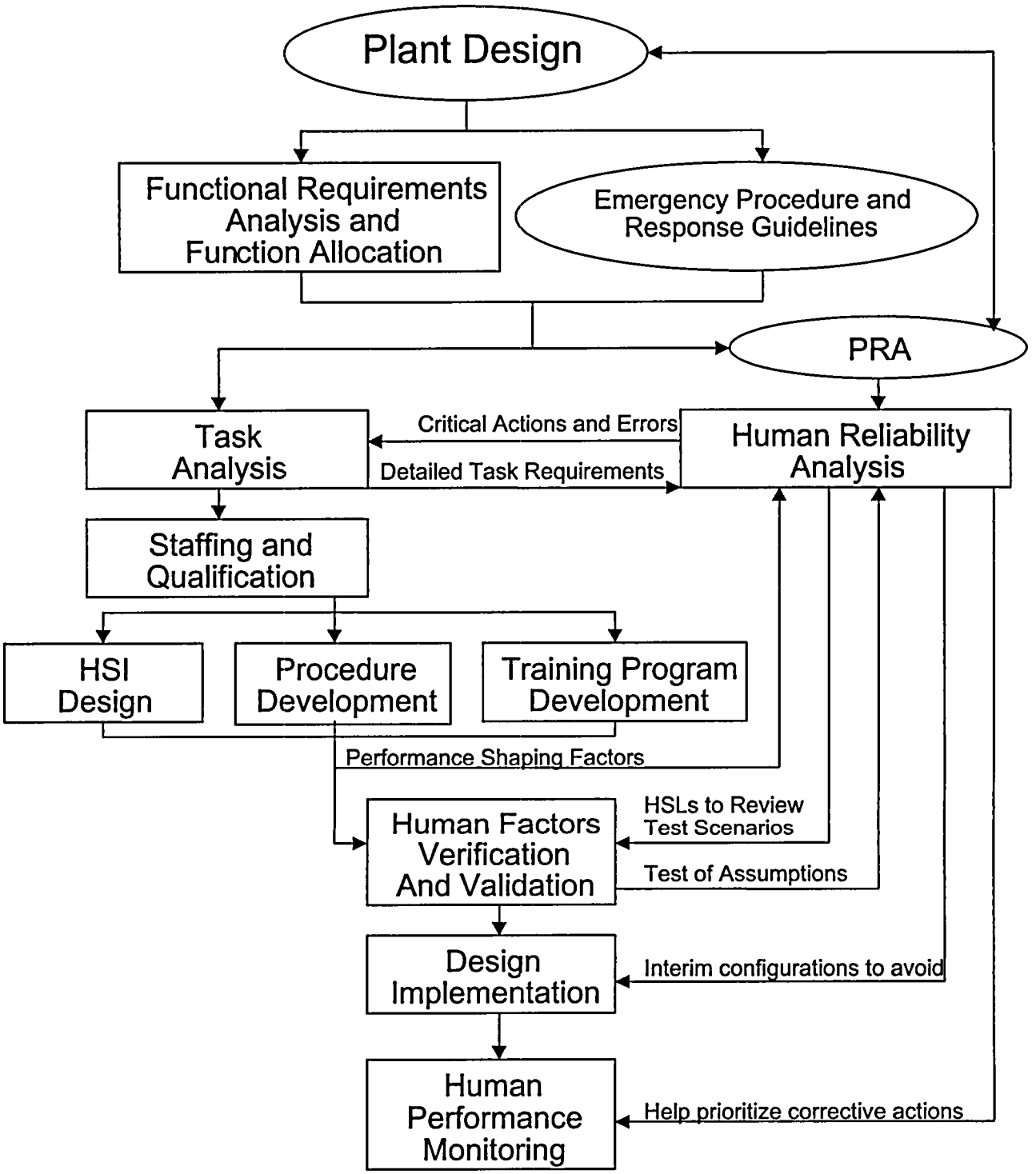

Figure 1 HRA task interactions with other HFE tasks

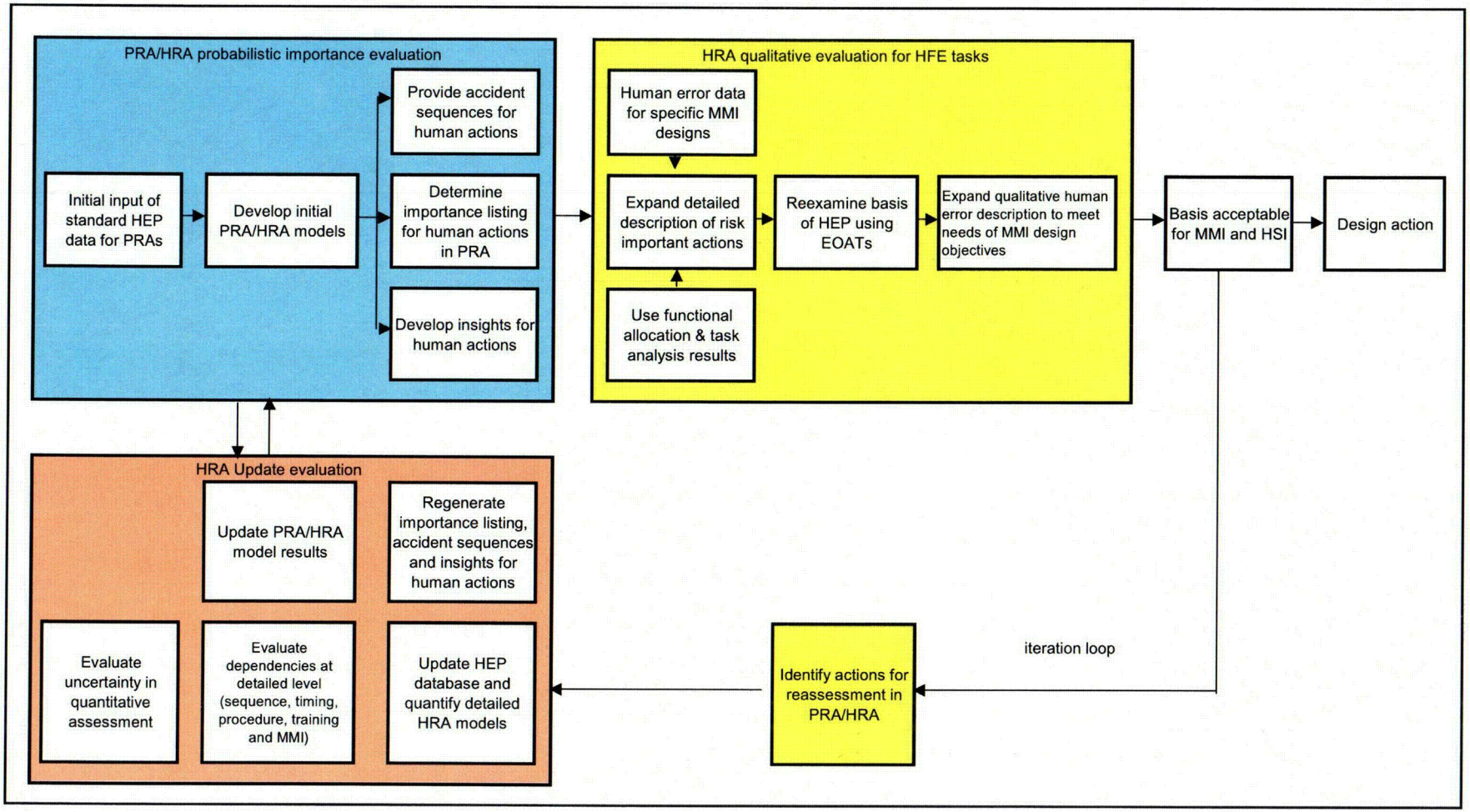

Figure 2 Link between the PRA/HRA and HFE input for HSI design

C01

Table 1 Summary of multiple element HRA models

Approach	Data/Models	Advantage	Weakness	Total HEP Formulation	Treatment of timing
One Element Model	Uses conservative trial data or simple models for initial PSA quantification. Can be applied by PRA team members	Simple for initial screening to help determine the important human actions, time is implicit	Does not account for plant specific conditions. Very conservative (not best estimate model)	HEP= Ps	qualitative assessment
One Plus Model	Considers performance factor adjustments to basic HEP qualitatively applied by HRA analyst	Provides for Performance Shaping Factors on a direct screening HEP value. Focuses on key performance factors	Misallocation of the PSF to broad failure modes.	HEP = Pb*PSFs	qualitative assessment
Two Element Model	Combines data base from NUREG/CR-1278 and EPRI-TR-100259 with rules to help HRA analyst select HEPs for specific context	Supports best estimate HRA based on error modes that can be described in the categories of cognitive and implementation. Provides generic data for a defined context set.	Analyst judgment and assumptions required to define context and time issues for each fixed error mode	HEP= P1+P3	qualitative assessment
Three Element Model	Uses models or simulator data to address time dependent HEP elements where the HRA analyst adjusts direct simulator measures	Uses basic models for P1 and P3 and explicit model for timing to match with simulator observations and data. Provides both a generic P2 model and permits use of plant specific simulator measures on time to success.	Behavior in a training simulator can be different than in the plant under real context and measures typically address timing only	HEP= P1+P2+P3	Solves for t2 from system time limt. Calibrates model with simulator measures
One element integration Time Model	Integrates all HEPs assessments into a HFE assessment using several parameters adjusted by HRA analyst to provide probabilities	Does not require explicit evaluations of P1 or P3. These are assumed to be included within the lumped model	Difficult to evaluate sensitivities on factors that relate to specific error modes, does not relate to specific error modes	HFE = f(m.σR,t)	Incorporates time as log normal function calibrated to early simulator measures
Four Element Model	Expands range of error modes for detailed examination and evaluation	Clear identification of specific error combinations for qualitative evaluation of situations also supports human factor assessments	Sparse data to support quantification. Quantification by expert judgment panel requires additional budget	HEP= P1a+P1b+ P2+P3	Solves for t2 time limit from a system time limt

Appendix A: Concepts for Quantifying Human Actions in PRAs

A.1 Introduction

The use of probabilistic risk models to evaluate the likelihood of accident scenarios in large complex plants requires reliability quantification of both equipment and human actions (and associated human errors) to properly estimate the total risk and relative importance of individual sequences. The human reliability quantification depends on data and models, after the qualitative description of the human action and its situation context in the accident scenario or system model have been defined and refined during the PRA modeling

Data for equipment failures can be collected under exacting laboratory or operational conditions and translated to failure rates for the basic events in the risk model. In the case of human errors the collection of data is much more difficult, because such errors are context specific, somewhat rare, and difficult to predict in advance. They are driven by numerous performance factors within the situation context. Any laboratory set up to measure human reliability must, to the degree possible, eliminate variability in performance factors and control the context to reduce observational feedback to the individual, which changes the error likelihood. Attempting to measure human actions and associated errors may be considered a multiple dimensional expansion of the Heisenberg uncertainty principle for physical elements. Therefore, the data used to support human reliability assessments must address the performance factors within the situation context of the action to be modeled. HRA analysts must also use judgment in selecting and applying the data as applicable factors when defining the context for a specific human action being analyzed.

A.1.1 HRA quantification goals

The ASME PRA standard [ASME, 2002] provides high-level goals for each element of the PRA. In the case of human reliability Analysis (HRA) the quantification requirement goals are:

- For pre - initiator actions it is to assess the probability of human failure events using a systematic process that addresses plant- and activity-specific influences on human performance.
- For post-initiator actions it is to use a systematic process that addresses plant-specific and scenario-specific influences on human performance to assess the probabilities, model plausible and feasible recovery actions, and address dependency on prior human failures in the scenario.

A.1.2 HRA basic questions

This paper illustrates basic models and methods that can be used to quantify human reliability for different levels of detail in a PRA and meet the systematic process requirements of the ASME PRA Standard. A systematic quantification of human reliability and errors in the context of a defined situation asks four basic questions which are answered by use of the basic methods. These are:

- Is the action feasible from the aspects of detection (e.g., HSI displays address accident context), timing and implementation (e.g., appropriate number of crew members available with control interface to the system)?
- What is the likelihood of success in a given time interval?
- What are the conditions within the context that increase or decrease the chance of cognitive errors?
- What are the conditions within the context that increase or decrease the chance of implementation errors?

If the answer to question 1 is "no," then the HEP associated with the defined action is 1.0. If the answer to question 1 is "yes," then the PRA team selects various methods and models to answer the remaining questions during different phases of the risk analysis process. For example, the quantitative HRA methods for screening may apply one probability number to cover questions 2 to 3. They are typically easy to use, and conservative enough to represent the analyst unknowns about event context, timing and types of errors. One element screening HRA models are very useful during initial evaluations. They support early prioritization of accident sequences and identification of risk important human actions.

During advanced phases of a PRA the context for risk contributing human actions is better defined, thus detailed modeling effort in terms of detailed questions and identification of performance factors can be focused on the analysis of the detailed error modes for key actions (ASME Category II level). Plant specific models can be calibrated to specific simulator measures as part of the basis for quantification to answer question 2 (Category III). More detailed evaluations can be used to support best estimate HEPs for important accident sequences in answering questions 3 and 4. The results identify those areas most likely to contribute to errors (e.g., procedures, communication, labeling, type of cue, lighting just to name a few). Detailed models can be used to characterize specific error causes and identify performance factors that exacerbate or ameliorate the error potential (Category III). Such detail is important, if the intent of the PRA is to reduce the likelihood of an error during hypothetical accident sequences through managed modification of the accident context factors. For example, providing written procedures where only on the job training is used. In the three element models timing to success can be combined with generic human error data to produce an overall estimate of an HEP.

When the accident descriptions are completed questions about dependency of human errors in the same sequence need to be addressed.

A.2 HRA model applications

This section describes five HRA modeling approaches that have been used to quantify the human reliability in PRA studies and meet the goals for analysis [Hannaman, PSA 2005]. They range from screening to very detailed methods.

The human actions for analysis are identified through the systematic process of performing the qualitative part of the HRA and through iterations with the PRA accident sequences to better define the context of the action. The PRA defined operator actions (OAs) can be quantified with various models and data, based on the qualitative information obtained and available to define the context of the action. The models described below provide results in various degrees of precision, based on the amount of effort used to define the context of the action.

A 2.1 Number of quantification elements in HRA models

The number of key probability elements used in the model to group and guide modeling assessment questions also provides a means for classifying HRA quantification approaches. They are:

- A one-element screening model is easy to use for screening in initial stages of PRA quantification when many human action boundary conditions have yet to be fully defined. The data needed can be found in screening tables developed from review of successful PRA applications. Application of the data requires only a general knowledge of the situation context and it carries conservative assumptions associated with the entries in Tables 1 and 2. The PRA team and the HRA analyst can use these values early in the modeling process to identify important sequences. *[Applies to ASME HR-D1 Category I, mostly Category I in all other areas*]

- An integrated one-element model typically includes explicit PSFs and timing at a single HEP level. Such a model can be used for detailed assessment, but requires considerable experience on the part of the analyst to apply the modification factors. The one element integrated model also includes timing as an input to the model, but requires HRA analyst judgment to apply. This model considers accident timing as an input to the quantification. *[Applies to HR-D2, Category I, F1, Category II G1 category II/III, HR-G3 Category I, HR-G4/G5 & HR-H1 Can apply to all Cat depends on data used]*

- Two-element models provide a basis for considering PSFs around two basic probability elements - cognitive and implementation errors. These models can be expanded to include explicit error modes and mechanisms associated with cognitive

and implementation errors. This approach provides a way of checking the accident context against the potential for key human error modes. Suggested databases have been supplied with these models, but timing is addressed as sufficient or not sufficient. *[Applies to HR-D2/D3/D4, Category II if applied to pre-initiators, F2, Category II or III, G1 category II/III, HR-G3 Category II/III, HR-G4/G5 & HR-H1 Can apply to all Categories depends on data used]*

- Three-element models provide a basis for detailed assessment by considering the impacts of PSFs on errors in cognitive processing, implementation, and response timing. In this case the PSFs can be applied at the level of each element or on sub level error modes. The three-element models can incorporate plant specific simulator measurement data to address the time to become successful following a cue for action. A timing equation is needed to address cognitive response errors in the three-element model. Both the systematic examination of human error modes and the plant specific measurement process provide insights on how to reduce the likelihood of human error. *[Applies to HR-D2/D3/D4, Category II if applied to pre-initiators, but this would not be done for P2. HR-F2, Category II or III, G1 category II/III, HR-G3 Category II/III, HR-G4/G5 & HR-H1 Can apply to all Categories depends on data used, and number of sequences analyzed]*

- Four-element models provide a more precise basis for detailed HEP by grouping the PSFs to address errors specific to detection, diagnosis, planning and implementation. The detection, diagnosis, and planning represent greater detail in the cognitive errors and the implementation errors are the same as the three and two-element models. The timing equation must be expanded to address response errors in the four-element model. The number of variables in the timing equation expands to areas, which are very difficult to measure. *[Applies to HR-D2/D3/D4, Category II if applied to pre-initiators, HR-F2, Category II or III, G1 category II/III, HR-G3 Category II/III, HR-G4/G5 & HR-H1 Can apply to all Categories depends on data used, and number of sequences analyzed]*

A 2.2 Common HRA model parameters

The types of HRA models can be qualitatively related to each other by using a common set of definitions [EPRI, 2002]. The symbols below are used in the following sections to describe relationships between various single and multiple-element models used to produce HEPs, which can be combined into an HFE by evaluating the dependences between actions in the same sequence.

- P1 errors in detection and diagnosis
- P2 delay in planning and organizing the response (e.g., non response)
- P3 errors in implementing a desired action
- ts time period until system changes state or fails the success criteria.

- t1 time allocated for completing the detection and diagnosis.
- t2 time allocated for completing planning and organizing
- t3 time allocated for implementing the task

A.3 Screening Assessments

The first quantitative objective that an HRA analyst typically faces is to provide initial values to the risk model for initial screening quantification. Thus, for quantitative screening purposes in system reliability or fault tree models it is useful to provide a traceable single value HEP that can be derived from simple systematic assessments. The second objective is to provide detailed quantifications using a quantification structure considering more detailed models that can be selected on the basis of the experience and knowledge of the analyst, the data available and the resources for the PRA project.

Since the PRA quantification process typically truncates low- probability sequences, this step economizes the PRA effort by focusing the detailed assessment on human errors that are likely to dominant the results. One example of a screening process is to assign probabilities by accounting for several elements that can be easily evaluated by an analyst.

A.3.1 Initial Screening level HEPs

The values for screening, based on Jens Rasmussen's [1986] qualitative process structure for skill, rule, and knowledge, were proposed in the SHARP report [1984] as fairly large ranges. As data were acquired from reviews of LERs, the ranges were refined to somewhat conservative values for pre-initiator actions as shown in Table A1.

- A skill-based action can be assigned if there is no significant cognitive involvement is required. This classification does not apply to pre-initiator actions outside the control room.

- Assumptions for assigning a rule-based action classification include a procedure is available that covers the case and there is no independent checking for non-routine actions. The procedure (e.g., an EOP or AOP) is assumed to be well written and easily understood by personnel, but only occasionally practiced (e.g., the training schedule for discussion walk through, or simulator training is less than once in 2 years).

- The knowledge-based cognitive process is assigned in cases where the procedure may not exist in written form or does not cover the case, or it is not well understood by the operator.

Crew redundancy in checking and verifying the task can reduce the values in Table A1 when good procedures exist, and in Table A2 for the short and long term cases by 0.3 to 0.1 following walk down and verification by the HRA analyst.

A.3.2 Screening level HEPs using Generic Simulator Results

As data were acquired from simulators, the ranges and central estimates were also refined for post –initiator actions to somewhat conservative values to address the importance of timing for actions in groups [EPRI 6560-L]. As starting point for initial screening quantification, several HRA analysts have suggested the probabilities in Table A2 [EPRI TR-100259, NUREG/CR-4772, EPRI-NP-3583].

There should be a high confidence that these probabilities will not be exceeded. The suggested time periods correspond to typical activities in a nuclear power plant, for example: (1) very short – actions to gain control of reactivity, (2) short – actions to reach transition to early decay heat removal systems, and (3) long term – actions that establish long term cooling. Implementation actions are assumed to require little time for opening and closing valves and breakers automatically from the control room. Caution must be used in cases where many actions are modeled in the same accident sequence with "AND" gates and the product of many 0.1 values makes the combination of actions go below PRA screening parameters. In this case a dependency assessment is needed to produce a combined HFE, which represents all the HEPs in one value applied to the specific accident sequence.

A 4 Detailed Analysis Quantification

Detailed analysis quantification focuses on the risk-significant human errors identified during the initial PRA quantification with screening HEP values, and sequence recovery actions. To reduce the uncertainty and refine the HEP estimate for those actions that are important to risk more information and knowledge is needed. Information is obtained from talk and walk- through procedures, walk-down of plant locations where the actions take place and simulator observations for control room actions.

The PRA team selects quantification models and data that depend on the specific goal of the PRA application, experience of the analyst, and the data and resources available. The resources for applying different HRA models can vary considerably. For example, use of a four-element model is more resource intensive than the two-element model. Simulator observations provide the time that an operating crew needs to do a task, and support a behavior model. Interviews with operators and walk downs of specific tasks provide information for assessing the impact of time and PSFs. Task analysis describes the operator action in terms of tasks and subtasks and includes the effects of PSFs. Engineering studies can be used to estimate the available time period for performing each element of the task. Engineering studies provide values for the overall system time (ts), simulator observations support timing estimates for T1/2, t1, and t2. Job performance measurements provide data for t3.

From the risk perspective it is important to focus on the most important actions. Consider that, if 1000 or 10,000 trained crews were in the same situation, how many

would be successful in completing the action or mission called for by the accident evolution. The focus of the models is on quantifying the impact of P1 (potential cognitive errors), P2 (time to success) and P3 (potential implementation errors).

To perform quantification and document results, it is necessary to have a set of models that can be applied as needed. The following descriptions are based on the number of elements in the model. Representative models following each type are used as examples.

A 4.1 Single-element HEP models

The simplest form for human reliability quantification [NUREG/CR-4772, NURE/CR-6350] is:

$$\Pr(OA) = 1\text{-}HEP_b(PSFs)$$

Where HEP_b is a basic human error probability for a single task[1] and the PSFs are modifiers between the base case task and context of the situation being evaluated[2,3]. The qualitative issues are identified during the qualitative analysis. Typical PSFs include factors such as event context (e.g. routine, or emergency actions), man-machine interface (e.g., strip chart, analog, digital, CRT figure), procedures (e.g., type and clarity), training (on the job, class room, or simulator), type of cue (e.g., active signal, instrument interpretation, etc.), personnel redundancy (e.g. backup checker with full attention or signoff). For emergency cases the added issues of detection, interpretation and planning for a response by the SRO should be considered. The list of modifiers can be very long depending on whether they explicitly focus on the error probability, error mode, error mechanism, cognitive processing, cognitive errors, detection, diagnosis, planning, and implementation. Thus, when using the simple model judgment is need to apply those

[1] The basic HEP, developed in the mid 1980's, considered a specific control room operator task required for plant start up. This baseline task of removing a source term before a protective trip provided statistical evidence and the effect of specific performance factors. The procedure for this task was handed down verbally during training. There was no written procedure or checklist. The cue for the action was read from a strip chart recorder of power level with multiple decade scales. There was no warning indicator before the trip point if the source had not been removed. Operators were told to remove the source and latch it to the bypass relay between 10 –50 % of trip level. At the appropriate time the licensed operator defines the task and asks the back up control room person to remove the source. The action takes less that 30 seconds to complete. If the operator fails to have the source removed before the trip level, the reactor trips and the restart takes about one hour to get back to that point. For an experienced operator with more than 10 starts the HEP is about .03 (e.g., 3.5 out trips of 120 starts for one operator). For new operators with less than 10 starts the HEP is about .1 (e.g., for 5 operators with 50 starts 4.5 trips). The case of 0.5 is due to a second person notifying the operator. These cases supported the development of the basic HEPs in NUREG/CR-4772 (.03 and .05). Thus, the introduction of written procedures or an annunicator alarm virtually eliminated this error type.

[2] EPRI NP-3583, Systematic Human Action Reliability Procedure (SHARP), Appendix A, 1984 uses a basic breakdown of skill, rule and knowledge for the basic HEPs (.001, .01 and .1).

[3] NUREG/CR-4772,"Accident Sequence Evaluation Program: Human Reliability Analysis Procedure", February 1987.

factors expected to significantly influence the results. These models are often very easy to apply and offer an easy basis for developing initial screening values.

A major drawback for this modeling process is that the relationship between PSFs is non-linear and a particular PSF may apply to only a part of the basic HEP. Therefore it is desirable in many cases to introduce a finer description of the HEP contributors as sub-elements where PSFs apply only to one element of the error cause, mechanism, or operator action processing phase. By extending the model structure beyond one-element a more accurate treatment of relationship between the performance factors and the basic HEP elements can be accomplished, because multiple-element quantification models address HEP modifiers explicitly by failure mode or cause.

A.4.2 One-element plus model (ASEP)

When time is not critical, and P1 and P3 can be lumped, a descriptive formulation is:

$HEP = P_{1+3} = BP * RF * MF * PSFs$

In this formulation BP is the Basic HEP Probability (e. g., 0.03 or 0.05 from ASEP), RF is the crew redundancy factor, MF is the multiple component dependency factor, and PSFs represent miscellaneous Performance Shaping Factors [NUREG/CR-4772].

Analyst judgment must be used to ensure that the HEP is not greater than 1.0, and that appropriate probabilities and uncertainties are obtained for each situation modeled in the accident sequences.

This model applies to both pre- and post-initiator actions when time is not critical. The cognitive and implementation failures modes are lumped into a single value where PSFs are used to adjust base values as described in NUREG/CR-4772. Verifying that the base HEP of 0.03 applies in the context of the accident requires a walk down. If no plant verification can be made use the base HEP of 0.05 should be used. In the case of pre-initiator actions these values are adjusted by PSFs to lower values, if there is a component status indication in the control room, there is a post-maintenance or calibration test, there is a backup checker, and periodic checks are documented in a written check off list. In the case of post initiator actions where time is short the HEP goes to 1.0 if the action is outside the control room, and there is no written procedure. If the analyst can classify the elements of skill rule and knowledge, based on interviews walk downs and procedure reviews, then the values in Tables 1 and 2 can be adjusted by factors of 0.3 and 0.1.

A 4.3 One-element lumped time based model

An integrated time reliability model from [Dougherty and Fragola, 1988] is used in some PRAs to represent P1, P2 & P3 in the case of post initiator human errors. It lumps all the failure modes for each element into a time integral equation by adjustment of the

equation parameters for t, σR, and m. The modeling equation is a lognormal distribution of the form

$$P_{1+2+3}(t) = \frac{1}{\sqrt{2\pi}\sigma_R} \int_{-\infty}^{t} \frac{1}{s} \exp\left\{-\left[\frac{\ln(s/m)}{\sigma_R}\right]^2\right\} ds$$

The HRA analyst accounts for the operational context by adjusting general factors such as the parameters t, m and σR:

- Rule-based versus knowledge-based
- No burden versus burden
- Other performance influencing factors

A typical result of the TRC model is shown in Figure A1.

A4.4 Two-element HEP models

Two-element models typically focus on the cognitive and implementation error modes for each action when timing is not critical. The probability of cognitive failure modes are lumped into a P1+2 and implementation errors into P3 values and then summed for the HEP as shown in Figure A2. The main difference between the two- and three-element models is that P1 and P2 are combined in the cognitive element with the assumption that timing is not a significant contributor [NUREG/CR-4772, EPRI, 1984].

Note that the probability equation is written in the algebraic rather than the Boolean

$$HEP(t) = P_{1+2} + P_3$$

form.

This equation for the two element model induces cognitive and implementation error modes. In this case timing is addressed qualitatively by noting that there is sufficient time for success.

A4.4.1 P1 Cognitive error quantification

EPRI TR-100259 presents structured questions whereby important PSFs can be evaluated for their impact on the probability of each error mode. The results are P_{1+2} probabilities in the ranges shown in Table A3. The process of evaluating the error mechanisms in this way gives ideas for improving the context of the human action to reduce the error probability.

A4.4.2 P3 Implementation Error quantification

Example of data for implementation errors can be found in [NUREG/CR-1278 20-7]. Table A4 shows implementation error probabilities that come from the work of Swain at Sandia Labs from the 1960s to the 1990's. The basis of the data is not open to evaluation, but it is published and has been used by many in PRA studies. It provides a variation in HEP depending on the type of procedures used.

A4.5 Three-element HEP models

Among many lessons, the TMI accident demonstrated the importance of timing of operator actions in managing accident sequences. For example, if the crew had thought to restart the safety injection pumps within about 1 hour, the accident would not have developed into core damage. The three-element model addresses the timing to success issue by explicitly considering P2 in the HEP equation [EPRI-NP6560-L]. Figure A3 addresses the Logic for a three- element model. The main new elements are evaluation of P2 for time to success and determination of elements for the time equation. Note the three-element equation is a Boolean equation.

The probability and time equations for a three-element model become:

$$HEP = P_1(t) + P_2(t) + P_3(t), \text{ and}$$

$$t_2 = t_s - (t_1 + t_3)$$

The assessment processes for P1 and P3 in the two element models can apply here. It remains to quantify P2 the probability of not being successful in a specific time. Evaluations of simulator data using previous models and data provide insights for improvement in the areas of training, procedures, control room interface, communications, cue types, and etc. The following sections describe the models and data obtained from previous testing.

A4.5.1 P2 HCR model hypothesis

The shape of the non-response curve was found to be dependent on somewhat observable conditions for individuals and possibly for crews. Hypotheses were developed to test this idea [EPRI 6560-L]. They were:

- Time dependent behavior of operator-crew actions is a function of skill, rule, and knowledge (S, R, & K) and can be measured in simulations.
- A time dependent equation can be constructed to represent S, R, & K timing for use in HRA quantification.

After initial small-scale experiments on individuals, an initial form of this equation was selected as shown below [NUS-4531, 1984].

$$P_2(t) = \exp\{-[(t/T_{0.5} - \gamma)/\eta]^{\beta}\}$$

It is a complementary form of the three-parameter Weibull distribution, which was selected because (1) it could handle timing delay (γ), 2 it has a characteristic factor for the situation (η), and a change in rate (β). Through the initial tests discrete combinations of β,γ, and η were found to represent SRK behavior in individuals. Discrete changes from K to R to S could be observed as specific rules were developed and practice resulted in further improvement.

It was also postulated that the impact of PSFs could be addressed as functions impacting $T_{0.5}$, which is the median time for crew actions measured in a simulator.

$$T_{0.5} = T_{0.5/\text{nominal}}\ \Pi[(1+K_i)\ldots(1+K_n)]$$

Where Ki are coefficients for operator experience, stress level, quality of operator/plant interface, and other PSFs.

To demonstrate this hypothesis it is necessary to obtain data to support the SRK concept if it is to be useful in HRA and PRA assessments. Obtaining time dependent data from simulators on simple tasks showed that people's success probability increased with time from the triggering cue. EPRI proposed the Human Cognitive Reliability hypothesis and sponsored experiments in power plant simulators to see if skill, rule, and knowledge-based actions could be differentiated. It was difficult to classify actions of a crew made up of individuals as purely S, R, or K, because of the difficulty in separating the different processes for each crewmember, and the linked impact of PSFs on $T_{0.5}$. However, the process provided some remarkably interesting results, which can be used to compare with new simulator measures.

A4.5.2 P2 HCR/ORE simulator data

The initial success of the HCR hypothesis lead EPRI and EdF to sponsor additional simulator experiments to see what else could be learned from simulator observations that could benefit PRA, operator training, and operating procedures [EPRI-6560-L]. Following numerous measurements in simulators, it was found that the general normalized curves were valid for events with clearly defined cues, and experienced operating crews using scrubbed procedures. Lognormal distributions could also fit the data categorized by initiating event, by cue type, etc. Available statistical analysis tools did not support a simple evaluation of the three-parameter Weibull models. The way that the cues presented themselves was found to be very important in the evaluation of the simulator observation data.

The resulting normalized non-response times which measure the time to success are not the same as time reliability curves which group all error modes into one probability calculation. As such the set of normalized non-response curves can be used as building blocks to construct time reliability curves for use in PRAs by combining them with probabilities of cognitive and implementation errors.

Analysis of more than 200 crew-scenario accident simulations found that a two parameter lognormal distribution provided an adequate statistical fit to observed times, normalized to $T_{0.5}$. The following formulation [EPRI 6560-L and EPRI TR-000259] represents the non-response probability at time t2.

$$P_2(t@t_2) = Pr(T > t@t_2) = 1 - \Phi\left(\frac{ln(t@t_2 / T_{0.5})}{\sigma}\right)$$

Where: $T_{0.5}$ = Measured planning or diagnosis median time;

t_2 = maximum time available for planning or diagnosis time; and

σ = standard deviation of the measure $\ln(T_{0.5})$ which can be quantified from a series of simulator observations. Sigma changes for different cue conditions.

$\Phi(..)$= distribution function of the standard normal distribution; and

@ = at.

A4.5.3 Comparison of HCR 1 & 2

Figure 4 compares the three parameter Weibull fits to early experiments with the two parameter Lognormal fits to simulator data collected from experiments of more than 200 crew scenarios. With the appropriate parameters in both equations the Weibull and Lognormal versions of the HCR model appear to be very close as far as the normalized non-response curves are concerned. This provides HRA analysts with a basic tool for evaluating the impact of timing on the HEP. A few simulator observations can help calibrate plant specific measures to the base case models. If no plant specific simulator data are available, then the generic models and data can be used to support HRA assessments.

The CP1, 2 and 3 relate to the type of cue that stimulates the response. In a generic assessment, the analyst needs to compare the definitions for CP1, 2, and 3 in Table A5 with the type of cue expected in the situation being analyzed, or select the dominant type of cognitive behavior to select the most appropriate curve as summarized below (from TR-100259). This sets the base formulation. Since the statistical values for CP1, 2, and 3 came from experimental simulator measures, the analyst may need to adjust the sigma values to account for the difference between the unexpected accidents in the control room versus expected events in the simulator. The amount of the adjustment for simulator measures versus real plant actions is currently based on judgment. The curves for HCR model and the HCR/ORE models are compared in Figure A4.

A4.5.4 Timeline analysis

The time equation is also important for the assessment. The time required for each element of the HEP equation (t2 = ts – (t1 + t3)) is needed. Plant-specific thermal hydraulic analyses are used to estimate system time periods (ts). In lieu of T/H models, the simulator may be used. A figure noting the cues, and values for ts can be used to evaluate the time periods for t1, t2, and t3.

This process documents that the time is sufficient for the action and produces a contribution to the total error probability.

A4.5.5 Engineering estimate of ts

Analysis of operator actions in the context of an accident sequence requires knowledge of event timing and cue presentation. Such data can be obtained from thermal-hydraulic calculations and/or engineering judgment. If thermal hydraulic assessments are not available, then engineering estimates can be used to account for specific cases that include initial cooling following a reactor trip and failure of a heat removal system. Simple model timing benchmarks are very useful for evaluating cases with system run failures after initially running.

An example of the combined HEP = P1(t) + P2(t) + P3(t) is shown in the figure 5 below. In this case, t is the time from the initial cue, and the HEP is the Boolean combination of each P. Within the evaluation, t2 is established by t2 = ts – (t1 + t3) leading to a maximum fixed value for t2 of 210 minutes where the HEP is 0.1. This applies to recovery of an air pressure system during station black out events. The process of considering timing changes the basic probabilities in an accident description into a time dependent relationship.

A4.6 Four-element HEP model

The driving force for a four-element model is that it can produce a more realistic description of the error modes, causes and identification of possible barriers to failure. As noted in Attachment A of EPRI-TR-100259, the HCR curves are conditional on the crew selecting an appropriate set of procedures or accident response path and then if not making the correct selection recognizing it as inappropriate and taking corrective actions within the time limit. The four-element model addresses the potential for not identifying that the wrongly selected path through the procedures is inappropriate and continuing with an uncorrected condition. Such errors have been labeled as errors of commission (EOC). These actions can be triggered by a false signal, a misinterpreted cue, etc. Thus, the evaluation for P1 is divided into P1a and P1b to account for crews' missing the cue, selecting an inappropriate path and failing to recognize the mistake. ATHEANA [NUREG/CR-6350] uses this modeling concept to identify detailed error causes for each element. The logic model for the four-element model is shown in Figure A6.

A4.6.1 P1 division to P1a and P1b in four-element HEP quantification

An advantage of using the four-element model is that it focuses on errors of commission in the decision making process so that causes that can be linked to corrective actions. A disadvantage of using a greater number of elements in HRAs for PRA quantifications is the lack of statistical data to support them. However, antidotal information has been identified linking errors of commission to causes in some very significant accidents. Use of expert judgment elicitation is currently the accepted way for quantifying the HEPs in ATHEANA. Calibration databases based on correlations could be used to evaluate the impact of different PSFs on the base HEP values.

Note that Performance Shaping Factors are controlled by both management actions and the day-to-day variability of individual crewmembers. The equations for probability and timing for the four-element model are shown below.

HEP (t) = P1a(t) + P1b(t) + P2(t) + P3(t)

t2 = ts -t1a- t1b -t3.

The timing elements in this equation are more difficult to measure, because t1a and t1b are difficult to separate during observations.

A4.6.2 Performance factors in four-element models

These examples of PSFs provide some consideration for evaluation. Reference 9, ATHEANA, uses systematic evaluation of a list of PSFs for each operator decision-making element. The PSFs listed in the table 5 illustrate how specific PSFs apply to specific phases of a human action. The ATHEANA process is constantly looking for new structures to describe PSFs that enhance the potential for errors of commission. Alternate descriptions for PSFs and Dependencies between PSFs have been proposed, and can be found in the CREAM modeling process [Hollnagel, 1998].

P1b is the area where errors leading to the selection of a wrong path through the procedures are addressed. Trainers provide defense against these error modes by helping crews practice communication and making sure that the operators can recognize the symptoms and take corrective actions. Even so, some events might present themselves in a confusing way leading to the wrong model of the plant (e. g., TMI). For P3, the control room actions are generally very clear, but actions outside the control room might require more time to gather tools if they are not available at the location. Use of this method provides additional insights on how to reduce the potential for specific human errors described as errors of commission.

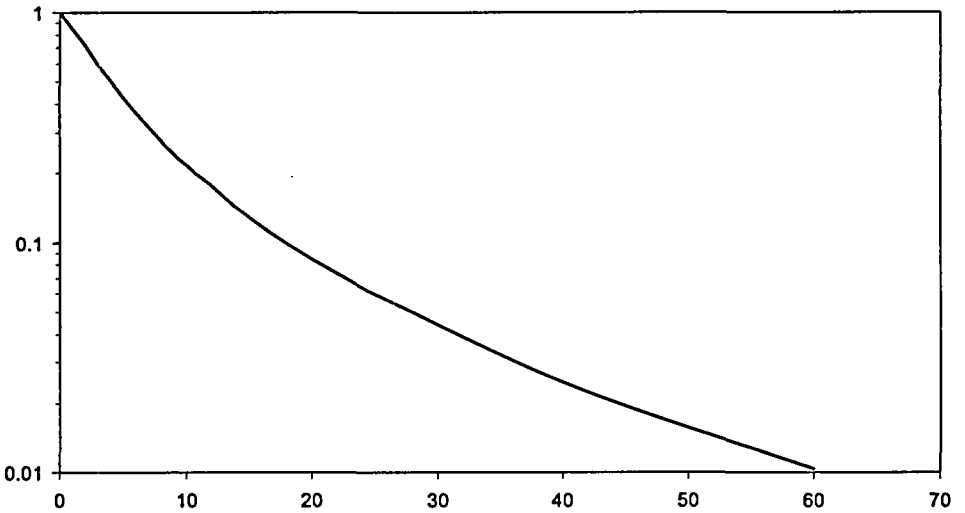

Figure A1 Time reliability correlation for one-element lumped model[4]

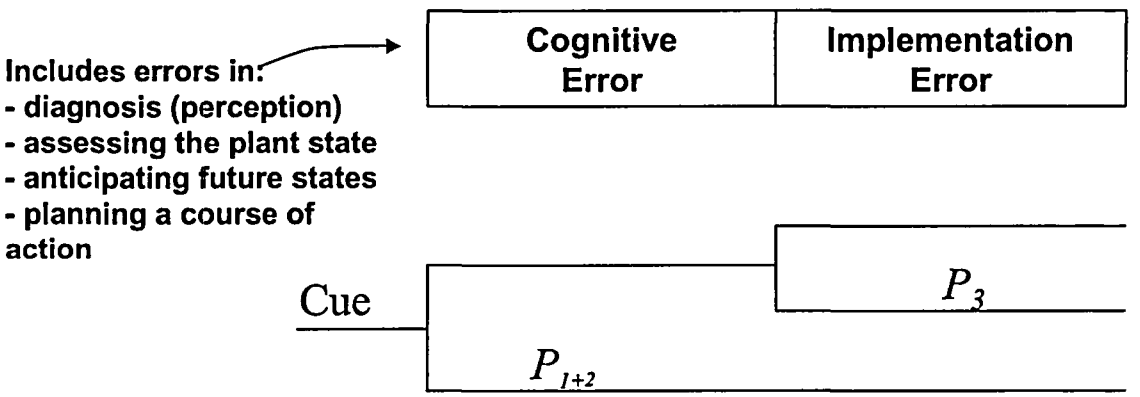

Figure A2 Operator Action Tree logic diagram for two-element HRA model[5]

[4] Dougherty and Fragola 1988
[5] EPRI-NP-3583

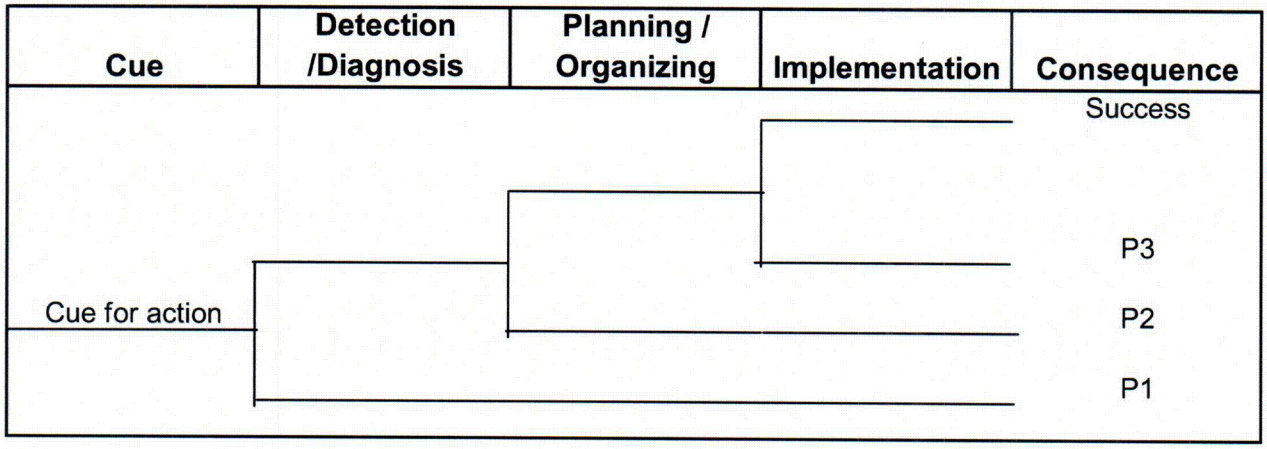

Figure A3 Operator Action Tree logic diagram for three-element models[6]

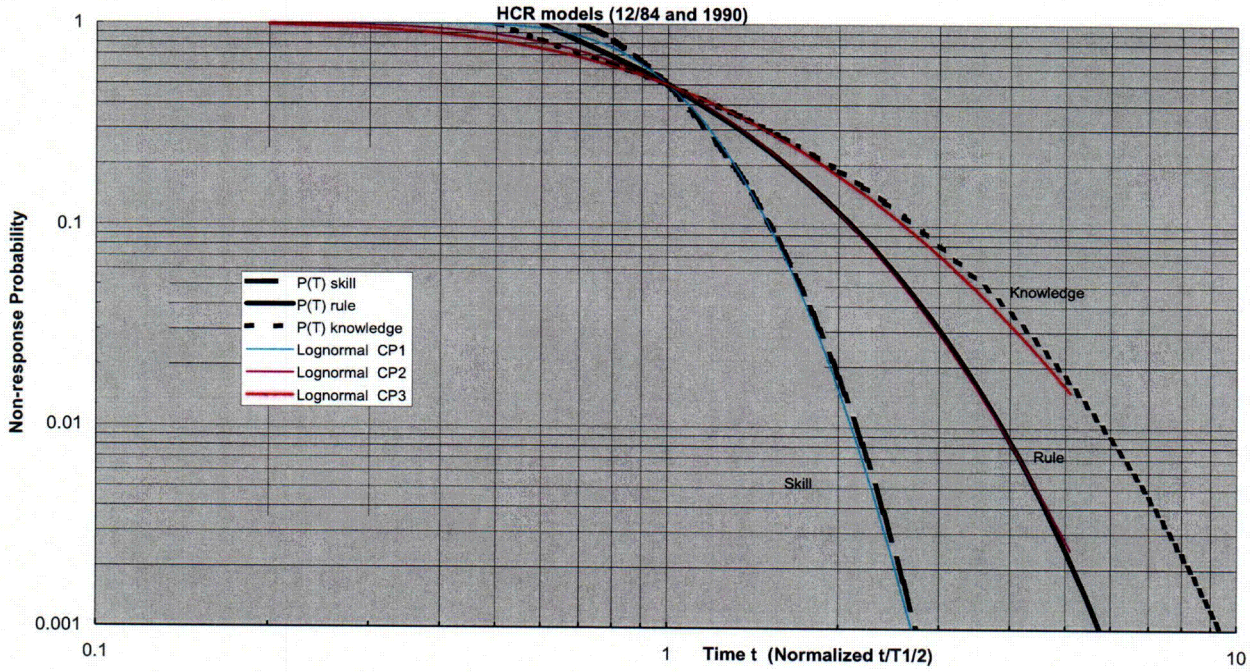

Figure A4 Comparison of HCR hypothesis and simulator data collection results[7]

[6] EPRI NP-3583, and NUS –4531, 12/84

[7] EPRI NP-6560-L, and NUS–4531, 12/84

C02

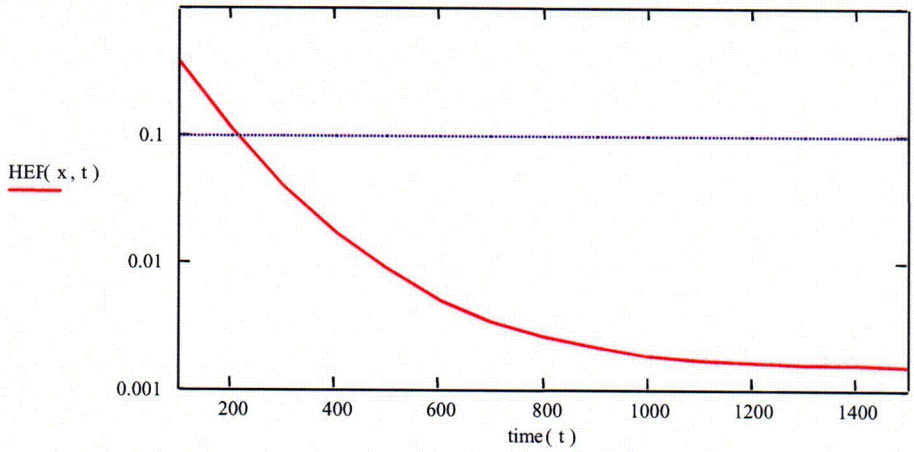

Figure A5 Example three-element model result

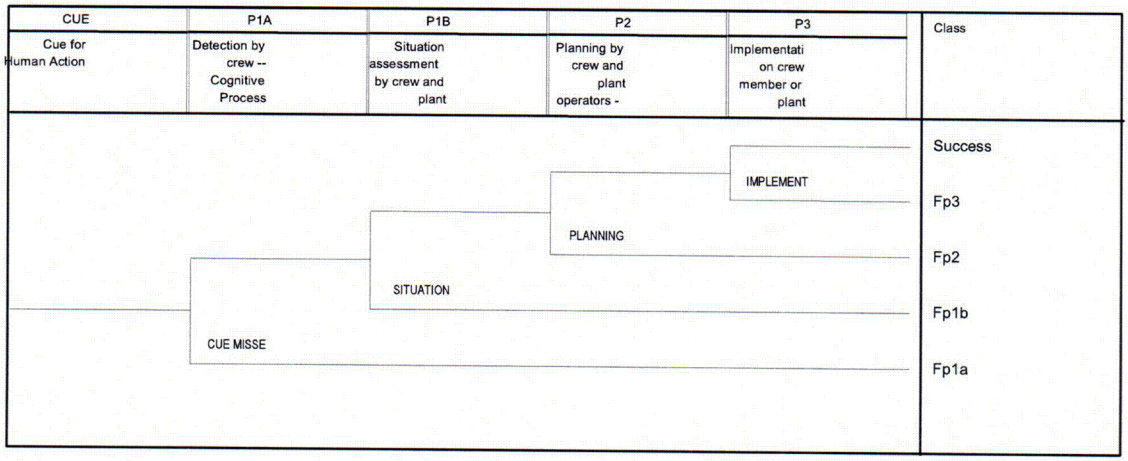

Figure A6 Operator Action Tree logic for a Four-element

Table A1 Conservative HEPb median values for an initial screening quantification[8]

Pre-Initiator Human Error Probabilities			
	Behavioral Type		
Action Type	Skill-Based	Rule-Based	Knowledge-Based
Calibration	NA	3E-2	-
Test	NA	2E-2	-
Maintenance	NA	1E-2	5E-2
Operational Realignment	NA	3E-2	1E-1

[8] EPRI 1003329, 2002

TableA2 Conservative HEPb median for post initiator actions[9]

Post-Initiator Human Error Probabilities			
	Behavioral Type		
Available Time	Skill-Based	Rule-Based	Knowledge-Based
Diagnosis			
Very Short (< 5m)	1E-1	5E-1	1
Short (5-60m)	1E-2	3E-2	3E-1
Long (> 60m)	1E-3	1E-2	5E-2
Implementation			
Realignment	3E-3	3E-2	1E-1

[9] EPRI 100332, 2002

Table A3 Probability ranges for cognitive errors in two-element model[10]

Error Mechanism	Range of failure probabilities
Availability of information	Neg to .5
Failure of attention	Neg to .03
Misread/miscommunicate data	Neg to .007
Information misleading	Neg to 1.
Skip a step in procedure	Neg to .1
Misinterpret instruction	Neg to .06
Misinterpret decision logic	Neg to .049
Deliberate violation	Neg to .95

[10] EPRI TR-100259

Table A4 Example assessments for implementation errors[11]

Tbl No.	Item	Text	Median	EF
20-7		**Estimated probabilities of errors of omission per item of instruction when use of written procedure is specified (from Table 15-3)**		
	1	Omission of item when procedures with checkoff provisions are correctly used. Short list, <= 10 items.	0.0010	3
	2	Omission of item when procedures with checkoff provisions are correctly used. Long list, > 10 items.	0.0030	3
	3	Omission of item when procedures without checkoff provisions are used, or when available checkoff provisions are incorrectly used. Short list, <= 10 items.	0.0030	3
	4	Omission of item when procedures without checkoff provisions are used, or when available checkoff provisions are incorrectly used. Long list, > 10 items.	0.0100	3
	5	Omission of item when written procedures are available and should be used but are not used.	0.0500	5

[11] NURE/CR-1278 1983

Table A5 Cue response timeline for simulator based HCR/ORE [12]

Cue type	Cue response structure
CP1	Disturbance occurs then one alarm occurs causing operators to detect, plan and implement the response. Success is completing the action within the desired time window established with some margin before an irreversible damage.
CP2	Disturbance occurs then first alarm occurs causing operators to detect, and plan. A second alarm indicating a plant limit is reached occurs causing additional planning and new priorities for the implementation response. Success is completing the action within the desired time window established with some margin before an irreversible damage.
CP3	Disturbance occurs then first alarm occurs causing operators to detect, plan and implement a response, however a new plant limit is reached after the operators implement the first action. Success is completing additional actions within the desired time window established with some margin before an irreversible damage.

[12] EPRI NP-6560-L 1990 and EPRI TR-100259, 1992

Table A6 Example PSFs for use in four-element models[13]

P1a Detection PSFs
Indications available CR
Indications available local
Clarity of Cue-CR
Feedback for monitoring change
Availability of CR personnel
Distraction through event
P1b Situational Assessment PSFs
CR operators develop appropriate mental model
Human errors before or during event mask symptoms
CR Procedure Applies
CR wrong mental model strengthened by inappropriate information
CR wrong mental model persist in face of contradictory information
P2 Develop Plans PSFs
Procedure Applicability for local action (restart and control)
Using plans not applicable to situation
Priority of Action/Give higher priority other plant function
Local operator availability
No plans exist therefore knowledge based training
Practice/Exp
Local operators don't follow plans
P3 Implementation PSFs
Procedure addresses local failure mode recovery
Location access easy
Equipment failures hinder operation
Tools available for complex repairs
Practice directly on recovering failure mode
Unfamiliar conditions increase stress
Local control feedback available
Miscommunication CR local

[13] Derived from NURE/CR-6350, Hollnagel, 1998