GE Energy
Nuclear

3901 Castle Hayne Rd
Wilmington, NC 28401

NEDO-33267
Revision 2
Class I
March 2007

LICENSING TOPICAL REPORT

ESBWR HUMAN FACTORS ENGINEERING
HUMAN RELIABILITY ANALYSIS
IMPLEMENTATION PLAN

INFORMATION NOTICE

This document NEDO-33267, Revision 2, 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 Economic Simplified BWR (ESBWR), the NRC expects that vendors address severe accidents during the design stage using Probabilistic Risk Analysis (PRA) tools. This allows 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 PRA 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.

HRA is a required activity of a probabilistic risk assessment (PRA) for both pre- and post-initiator human actions [ASME-RA-S-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.

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

1. Ability of the Human System Interface (HSI) to detect and present abnormal conditions to the operators,

2. Selection of personnel with abilities for plant and main control room (MCR) operations,

3. General training of operators,

4. Level of operator training for specific actions and contingency planning,

5. Robustness of the procedures for a wide range of accident conditions, and

6. Availability of HSI for monitoring, controlling, and providing feedback on actions taken in response to specific events.

HRA information is incorporated into the ESBWR human factor engineering (HFE) process as shown in Figure 1. 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 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 gives 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 is used to support the HSI HFE design goals. This occurs when use of the HSI impacts a significant accident sequence defined in the PRA. The initial “design level” ESBWR PRA/HRA is submitted in support of NRC licensing requirements using an HSI reference design with many system features from predecessor 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 HSI reflects these design features as well as technology advances in indication displays, control and instrumentation approaches (e.g., analog to digital).

Risk-informed decision-making is used to justify the specific design features for the ESBWR. Changes from the predecessor BWR licensing basis meets 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. The following bullets from RG 1.174 provide a framework for interpreting and evaluating changes in risk when design choices are made for the HSI during the design process.

- 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 update iterations with the PRA addresses the impact of human-error mechanisms on the ESBWR HSI design. Through these updates, the impact of HSI changes on core damage frequency and large early release frequency evaluations can be assessed. The update assessment permits evaluations of margins to safety over established safety goals (e.g., RG 1.174) based on the inherent design features in the ESBWR and the HSI.

Human errors identified and quantified in the PRA are 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 both qualitatively and quantitatively links the HFE program into the PRA and risk analysis. In addition, the results become design inputs to the software development activities.

Operator requirements for maintaining plant safety and availability goals over the complete range of transient event conditions are 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 are provided in revisions to S&Q Results Summary Report document. The recommended staffing level is reflected in procedures and training program design.

1.2 Scope

This plan establishes a HRA process in conformance with the NEDO-33217 ESBWR Man-Machine Interface System (MMIS) and Human Factors Engineering Implementation Plan , and NUREG-0711r2, Human Factors Engineering Program Review Model. The interaction of the HRA tasks with other HFE tasks is shown in Figure 2.

The scope of this plan includes the following:

- Using a multidisciplinary team as described in Section 3 to analyze human actions within the context of the PRA.

- Developing a process for using PRA/HRA (e.g., level 1, level 2, internal and external events) to support the design of the ESBWR HSI. An initial working process is shown in Figure 3.

- Identifying and selecting HRA elements and key actions that impact the quantitative risk estimates.
- Clarifying the role of operators, through applicability of the HSI to support key operator tasks, emergency procedures and training, and to protect the plant from accident challenges.
- Clarifying the role of operators by obtaining design information related to factors that affect human performance.
- Iterating with the probabilistic 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 (PSFs) 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 and Acronyms

1.3.1 Definitions

The terms below are defined to provide a definitions for specific terms used in this report and to support interactions between the PRA/HRA and the Task Analysis.

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-RA-S-2002).

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-RA-S-2002).

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.

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

Action type: the actions considered in PRAs are classified as pre-initiator, initiator and post-initiator actions by designating them as A, B, and C, respectively, to prepare for different types of HRA analyses (EPRI TP-101711).

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 MCR operators. This involves monitoring the plant state or identifying a cue for action, 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.

Component: an individual piece of equipment such as a pump, valve, or vessel; usually part of a plant system.

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

Contingency plans: 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).

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 MCR, RSS panels, and LCSs with a safety related function or as defined by high level task analysis.

Core Damage Frequency (CDF): expected number of core damage events per unit of time.

Core damage (CD): uncovery and heatup of the reactor core to the point at which prolonged oxidation and severe fuel damage involving a large fraction of the core is anticipated.

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.

Cutset: the route through a logic tree represented as a collection of basic events whose occurrence guarantees that a top event in a fault tree or sequence end state in an event tree occurs. The cutset is minimal if the non-occurrence of one basic event in the collection prevents the top event or sequence from occurring.

Dependency: requirement external to an item and upon which its function depends and is associated with dependent events that are determined by, influenced by, or correlated to other events or occurrences.

Diagnosis: examination and evaluation of data from the HSI to determine either the condition of the system structures and components (SSC) or the cause of the condition (ASME-RA-S-2002).

Emergency Procedure Guidelines (EPGs): 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.

Error of Commission (EOC): an error that occurs as a result of an action taken. In the context of PRA/HRA quantification an operational failure event resulting from an overt, unsafe human action that when taken leads to a change in plant configuration with the consequence of an undesired degraded plant state. Examples are inappropriate blocking of depressurization leading to lack of heat removal and premature depressurization leading to over cooling and possible vessel damage due to pressurized thermal shock. The classification of an error of commission depends on the context of the situation.

Expanded Operator Action Tree (EOAT): a logic tree that combines two or more operator action trees (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 in this document).

Failure mechanism: any of the processes that results in failure modes, including chemical, electrical, mechanical, physical, thermal, and human error (ASME-RA-S-2002).

Failure mode: a condition or degradation mechanism that precludes the successful operation of a piece of equipment, a component, or a system (ASME-RA-S-2002).

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-RA-S-2002).

Function: an activity or role performed by a human, structure, or automated system to fulfill an objective (NEDO-33219).

HFE design team: a multi-disciplinary team of engineers, as defined in NEDO-33217, who are responsible for the design of the HSI systems.

HSI design team: a team of engineers, as defined in NEDO-33217, who are responsible for the design of the HSI systems.

Human Action (HA): a manual response to a cue involving one person to achieve one task or objective. Potentially risk-important HAs 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 an error of commission performs the wrong action. In other words HEP is the probability of the operational failure event (ASME-RA-S-2002).

Human error recovery: the human ability to recognize and correct an error before the error results in conditions that become irreversible.

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

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 a basic 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-RA-S-2002).

Human System Interface (HSI): in general the HSI 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, at power operation, and refueling) as well as off-normal, emergency, and accident conditions. Specifically, the HSI is the organization of inputs and outputs used by personnel at a location to interact with the plant, including the using of alarms, displays, controls, and job performance aids. Generically, this includes interfaces that support actions for monitoring, controlling, maintaining protection functions, responding to events, and performing maintenance, calibration, inspection and testing activities. The details of the HSI systems are defined in ESBWR DCD, Tier 2, Chapter 7.

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 faults in a system (i. e., Type B human actions leading to errors).

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.

Large Early Release Frequency (LERF): the expected number of large early releases per unit time (ASME-RA-S-2002).

Large early release: the rapid unmitigated release of airborne fission products from the containment to the environment occurring before the effective implementation of off-site emergency response and protective actions, such that there is a potential for early health effects (adapted from ASME-RA-S-2002).

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.

Main Control Room (MCR): room that provides the location from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents.

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

Operating time: total time during which components or systems are performing their designed function (ASME-RA-S-2002).

Operating Experience Review (OER): a systematic review, analysis and evaluation of lessons learned from operating experience that can apply to the development of the man machine interface design.

Operational Failure Events (OFEs): an integrated logic description of multiple HEPs based on the error modes, PSF assessment, and other qualitative information needed to justify a single input to the risk model (adapted from ASME-RA-S-2002 from definition of Human Failure Events).

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 in this document).

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, use of electric power external to the component, 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-RA-S-2002).

Plant-specific data: data consisting of observed sample data from the plant being analyzed (ASME-RA-S-2002).

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 and 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 actions with 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-RA-S-2002).

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 human actions with 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-RA-S-2002).

Primary tasks: those tasks performed by the operator to supervise the plant; i.e., monitoring, detection, situation assessment, response planning, and response implementation (NUREG-1764).

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-RA-S-2002).

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-RA-S-2002).

Remote Shutdown System (RSS): panels, and applicable Local Control Stations located outside the MCR.

Response: a reaction 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).

Risk: probability and consequences of an event, as expressed by the risk triplet that is the answer to the following three questions: (1) What can go wrong? (2) How likely is it? and (3) What are the consequences if it occurs?

Risk-important human actions: actions that must be performed successfully by plant personnel in the context of a PRA to prevent core damage or large early releases. Both absolute and relative criteria are used to define risk-important HAs. From an absolute standpoint, a risk-important HA is one whose successful performance is needed to ensure that predefined risk criteria are met. From a relative standpoint, the risk- important actions constitute the most risk-significant human action identified. Actions may be made up of one or more tasks. The identification can be done quantitatively from risk analysis and qualitatively from various criteria such as task performance concerns based on the consideration of PSFs (adapted from NUREG-1764).

Safety functions: those functions that serve to ensure higher-level objectives and are often defined in terms of a design basis event (a boundary or entity that is important to plant integrity and the prevention of the release of radioactive materials) (adapted from NUREG-1764).

Safety related task: a task that is required to be performed to achieve a safety function defined in the design basis events. Safety related operator tasks qualitatively include those required to start, control and stop equipment in order to meet the design basis event radiological limits. The use of automated systems for starting, controlling and stopping systems in design basis events limits the need for a safety related operator task.

Safety systems: those systems that are designed to prevent or mitigate a design-basis accident (adapted from ASME-RA-S-2002).

Safety-related operator action: a manual action required by plant emergency procedures that is necessary to cause a safety-related system to perform its safety-related function during the course of any Design Basis Event. The successful performance of a safety-related operator action might require that discrete manipulations be performed in a specific order (NUREG-1764). Use of passive and automated systems removes the need for safety related operator actions.

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-RA-S-2002).

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-RA-S-2002).

Secondary tasks: those tasks that the operator must perform when interfacing with the plant, but are not directed to the primary task. Secondary tasks may include: navigating through and paging displays, searching for data, choosing between multiple ways of accomplishing the same task, and making decisions regarding how to configure the interface (NUREG-1764).

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-RA-S-2002).

Simulator: a computer driven system that physically represents the human-system interface configuration of the main control room or other control interface and that dynamically represents the operating characteristics and responses of the plant in real time. Simulators include both part-task models that represent specific aspects of one or more systems and full scope models that integrate the dynamic behavior of all plant systems and HSIs working together to match the real world performance of the control room.

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.

Standard interface: the HSI based on rules provided in the ESWBR HFE style guide that will be used by the designers (NEDO-33266 Table 2).

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-RA-S-2002).

Support system: a system that provides a support function (e.g., electric power, control power, or cooling) for one or more other systems (ASME-RA-S-2002).

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-RA-S-2002).

System: an integrated collection of plant components and control elements that operate alone or with other plant systems to perform a function (NUREG-1764).

Task Analysis (TA): a method for describing what plant personnel must do to achieve the purposes or goal of their tasks. The description can be in terms of cognitive activities, actions, and supporting equipment.

Task: a collection of activities with a common purpose, often occurring in temporal proximity, with an identifiable start and end point for which human actions are performed using displays and controls.

Time available: the time period from the presentation of a cue for human action or equipment response to the time of adverse consequences if no action is taken (ASME-RA-S-2002).

Transients: in the context of a PRA/HRA, initiating events or system faults that perturb the normal steady state condition. If exceeded during the event, protective set points automatically trigger plant mode changes requiring backup systems to function. Failures in the backup systems can result in emergency conditions, where prompt operator actions might be required to avoid plant damage, or to prevent accidents from damaging structures, systems or components.

Unavailability: the fraction of time that a system or component is not capable of performing its function, including but not limited to the time it is disabled for test or maintenance (adapted from ASME-RA-S-2002).

Uncertainty: a representation of the confidence in the state of knowledge about the parameter values and models used in constructing the PRA (ASME-RA-S-2002).

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 actions involving errors).

Workload: the physical and cognitive demands placed on plant personnel (NUREG-1764).

1.3.2 *Acronyms*

The following is a list of acronyms used in this plan:

Acronym	Description/Name
ANS	American Nuclear Society
ANSI	American National Standards Institute
AOF	Allocation of Function
AOP	Abnormal Operating Procedure
ASEP	Accident Sequence Evaluation Program
ASME	American Society of Mechanical Engineers
ATHEANA	A Technique For Human Error Analysis
BRR	Baseline Review Record
BWR	Boiling Water Reactor
CCDP	Conditional Core Damage Probability
CD	Core Damage
CDF	Core Damage Frequency
CFR	Code of Federal Regulations
CRDT	Control Room Design Team
CREAM	Cognitive Reliability and Error Analysis Method
CRT	Cathode Ray Tube

Acronym	Description/Name
DCD	Design Control Document
DOE	Department of Energy (formerly ERDA)
EF	Error Factor (measure of uncertainty)
EOAT	Expanded Operator Action Tree
EOC	Errors of Commission
EOP	Emergency Operating Procedure
EPG	Emergency Procedure Guideline
EPRI	Electric Power Research Institute
ESBWR	Economic Simplified Boiling Water Reactor
FV	Fussell Vesely (Importance measure)
HA	Human Actions
HCR	Human Cognitive Reliability
HEP	Human Error Probability
HFE	Human Factors Engineering
HFEITS	Human Factors Engineering Issue Tracking System
HI	Human Interaction
HRA	Human Reliability Analysis/Assessment
HSI	Human System Interface
IAEA	International Atomic Energy Agency
IEEE	Institute of Electrical and Electronics Engineers
LERF	Large Early Release Fraction
LOCA	Loss of Coolant Accident
MCR	Main Control Room
MMIS	Man Machine Interface System
NPEC	Nuclear Power Engineering Committee
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NUREG	Nuclear Regulatory Commission technical report designation
OA	Operator Action
OAT	Operator Action Tree
OER	Operating Experience Review
OFEs	Operational Failure Events
ORE	Operator Reliability Experiments
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factor
RAW	Risk Achievement Worth
RG	Regulatory Guide

Acronym	Description/Name
RRW	Risk Reduction Worth
RSS	Remote Shutdown System
S&Q	Staffing and Qualifications
SFRA	System Functional Requirements Analysis
SHARP	Systematic Human Action Reliability Procedure
SPAR	Simplified Plant Analysis Risk
SRK	Skill, Rule, Knowledge
SRO	Senior Reactor Operator
SSC	Structure, System and Component
STD	Standard
TA	Task Analysis
TMI	Three Mile Island
TP	Technical Position
TR	Technical Review
TRC	Technical Review Committee
V&V	Verification and Validation

2 REFERENCES

Applicable documents include supporting documents, supplemental documents, codes and standards and are given in this section. Supporting documents provide the input requirements to this plan. Supplemental documents are used in conjunction with this plan. Codes and standards are applicable to this plan to the extent specified herein. For references listed below, the revision number if not listed is the current reference.

2.1 Supporting and Supplemental Documents

2.1.1 Supporting Documents

The following supporting documents were used as the controlling documents in the production of this plan. These documents form the design basis traceability for the requirements outlined in this plan.

1. ESBWR DCD Tier 2, Chapter 18, Revision 03, (GE 26A6642BX)
2. ESBWR DCD Tier 2, Chapter 19, Revision 01, (GE 26A6642BY)
3. NEDO-33217, Rev. 2, ESBWR Man Machine Interface System and Human Factors Engineering Implementation Plan

2.1.2 Supplemental Documents

The following supplemental documents are used in conjunction with this document plan.

1. NEDO-33219, Rev. 1, ESBWR Functional Requirements Analysis Implementation Plan
2. NEDO-33220, Rev. 1, ESBWR Allocation of Functions Implementation Plan
3. NEDO-33221, Rev. 1, ESBWR Task Analysis Implementation Plan
4. NEDO-33262, Rev. 1, ESBWR Operating Experience Review Implementation Plan
5. NEDO-33266, Rev. 1, ESBWR HFE Staffing And Qualifications Plan
6. NEDO-33268, Rev. 2, ESBWR Human System Interface Design Implementation Plan
7. NEDO-33274, Rev. 2, ESBWR Procedure Development Implementation Plan
8. NEDO-33275, Rev. 1, ESBWR Training Development Implementation Plan
9. NEDO-33276, Rev. 1, ESBWR HFE Verification & Validation Implementation Plan
10. NEDO-33277, Rev. 2, ESBWR Human Performance Monitoring Implementation Plan

2.2 Codes and Standards

The following codes and standards are applicable to the HFE program to the extent specified herein.

1. ANSI/ANS 58.8, Time Response Design Criteria for Safety-Related Operator Actions, 1994
2. ASME-RA-S-2002, Standard for Probabilistic Risk Assessment For Nuclear Power Plant Applications, 2002
3. IEEE 1082, Guide for Incorporating Human Action Reliability Analysis for Nuclear Power Generating Stations, 1997
4. ANSI/IEEE 1023, IEEE Guide to the Application of Human Factors Engineering to Systems, Equipment and Facilities of Nuclear Power Generating Stations, 2004

2.3 Regulatory Guidelines

1. NUREG-0654 Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants, 1980, (FEMA-REP-1, Rev.1 addenda, 2002)
2. NUREG-0700, Rev 2, Human -System Interface Design Review Guidelines, 2002
3. NUREG-0711, Rev.2, Human Factors Engineering Program Review Model, 2004
4. 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"), 1980
5. NUREG-0800, Standard Review Plan, Chapter 18, Human Factors Engineering. Rev 1, 2004
6. NUREG-0800, Standard Review Plan: Chapter 19, Use of Probabilistic Risk Assessment in Plant-Specific, Risk-Informed Decision Making: General Guidance, Rev. 1, 2002
7. NUREG-0933, A Prioritization of Generic Safety Issues, Supplements HF, 2004
8. NUREG-1123, "Knowledge and Abilities Catalog for Nuclear Power Plant Operators: Boiling Water Reactors, 1995
9. NUREG-1624, Rev. 1, Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA), 2000
10. NUREG-1649, Reactor Oversight Process, 2000
11. NUREG-1764, Rev. 0, Guidance for Review of Changes to Human Actions, 2004

12. NUREG-1792, Good Practices for Implementing Human Reliability Analysis (HRA), 2005

13. Regulatory Guide 1.174 , An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, Rev. 1, 2002

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), 1990

2. DOE Order 5480.19, Conduct of Operations Requirements for DOE Facilities; Change 2, 2001

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

4. MIL-STD 1472D, Human Engineering Design Criteria for Military Systems, Equipment and Facilities, Dept of Defense, 1989

2.5 Industry and Other Documents

Additional reference documents or those that have been removed may be re-added to the next revision, as they become available to the HFE design team.

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

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

9. IAEA-TECDOC-632, ASSET Guidelines: Revised Edition, Vienna 1991

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

11. NUREG/CR-1278, Handbook of human reliability analysis with emphasis on nuclear power plant applications, 1983

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

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

14. Hannaman, Spurgin and Lukic, A Model for Assessing Human Cognitive Reliability in PRA studies, Conference record for IEEE Third Conference on Human Factors and Nuclear Safety, Monterey, California / editor, Edward W. Hagen, June 23-27, 1985

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

3 HRA METHODOLOGY

The specific methodology for HRA is developed by the PRA team and supported by the GE HFE design team following the iterative links with the HFE program shown in Figure 2, leading to an "as designed PRA/HRA" at the completion of design. To show that the ESBWR meets the risk goals during the design, it may not be necessary to develop detailed HRA models for more than a few actions. Development of a more comprehensive PRA model suitable for risk monitoring from the MCR requires additional detailed PRA/HRA modeling. The development of this HSI feature is considered as a possible MCR feature for the ESBWR that has not been included in the base design scope of the previous ABWRs and BWRs.

Plant owners working with consultants after plant start up developed and installed risk monitors in many currently operating plants. Licensed operators use the risk monitors as a tool to evaluate the risk impact of scheduling new equipment to be out of service when other equipment is already out of service. If the risk of the proposed action is found to be too high for the combination of equipment out for service, a new schedule is developed with a lower risk value.

3.1 Requirements

The requirements to achieve a PRA/HRA model suitable for risk monitoring are:

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

  The PRA and HRA will be performed during the design process to provide insights and guidance both for systems design and for HFE purposes. Accordingly, the HRA will be updated as the design progresses and the early versions of the PRA/HRA will be finalized when the plant design and HFE are complete. The PRA includes the identification of human actions that are required to start and stop systems, and special actions needed to initiate passive cooling features (e.g., manual depressurization, and back up to automatic triggering of the squib valves for gravity feed) and quantification via HRA screening methods.

- 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 GE HFE design team incorporates sufficient expertise to accomplish this detailed HRA process by including NRC licensed SROs, and engineers/analysts who have performed or managed maintenance activities, reviewed events, classified human errors, observed simulated accidents, and developed procedures.

- 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 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 gives special attention to those plant scenarios with risk- important human actions, and the HSIs that have been identified by PRA/HRA as being important to plant safety and reliability.

- The HRA task interacts with the HFE verification and validation program to provide test scenarios and updating quantitative evaluations based on data from the validation process.

- The HRA model establishes a listing of key tasks for future human performance monitoring, and helps prioritize corrective actions.

3.2 General Approach

The requirements for a PRA call for, and support the use of, a systematic process for HRA evaluations. RG 1.174 provides a map of absolute risk regions for deciding when to take actions to reduce risk through design upgrades for currently operating plants. This risk informed approach supports the use of resources to address the highest risk items first. This concept is used for the ESBWR even though the initial PRA results show that the over all risk measures are far below the NRC risk regions in RG 1.174. This is due to the passive design features and the use of automation.

3.2.1 Risk Measures for Human Interactions

PRAs take advantage of the specialized ranking tools that can be systematically used to rank basis event inputs to the PRA model relative to their risk importance. For example, the following three processes are used within the PRA models to determine the importance of human interaction tasks that are modeled as basic events. Three of the ranking processes are:

- The Fussell-Vesely (FV) Importance evaluation is the relative contribution to the system failure probability, core damage frequency (CDF), large early release frequency (LERF), or conditional core damage probability (CCDP) from a basic event failure at its estimated failure probability,

- The Risk Achievement Worth (RAW) evaluation is the factor increase in the system failure probability, CDF, LERF, or CCDP when a basic event (or group of basic events) is assumed to be failed, and
- The Risk Reduction Worth (RRW) evaluation is the factor decrease in the system failure probability, CDF, LERF, or CCDP when a basic event (or group of basic events) is assumed to succeed.

These importance evaluation processes provide the keys for determining the risk impact of human errors that are represented in the PRA model as basic events. For example, NUREG-1764 provides a process for ranking HIs by their importance to various measures within the operating plant PRA models such as system failure probability, CDF, LERF, or CCDP. This process maps the FV and RAW importance measures to the risk regions in RG 1.174 so that human actions can be treated with the same risk criteria as equipment when evaluating their risk importance and taking actions to manage the risk.

In the case of the ESBWR the passive features and automation virtually eliminate the need for the safety related human actions required for design basis events (e.g., manually start a safety system). These design features reduce the CDF to a mean value much lower than the plants used as the basis for the NRC risk regions in RG 1.174. As a result, the risk boundaries associated with the risk regions in RG 1.174 are far above the ESBWR baseline risk. Hence, the ESBWR basic events representing HIs do not become important contributors to plant risk on an absolute basis.

To evaluate the risk impact of the HIs for the beyond design basis events a relative risk approach is used. First, risk sensitive actions that support ESBWR safety for beyond design basis events are identified in both the PRA and through the top down HFE operational analysis. Sensitivity analyses using the FV, RAW and RRW described above on the basic events related to HIs are used to create a listing of top risk contributors on a relative basis. This listing is generated in the PRA and is compared with the top down operational analysis to identify gaps and support requantification for the PRA. On a relative scale, the HIs with a FV greater than 0.1 and RAW of 2.0 for CDF and LERF are subjected to the greatest detail in the HFE tasks, even though the absolute risk values are far below regions I and II described in NUREG-1764.

3.2.2 HRA quantification

There are a number of HRA modeling approaches that can be used to produce the basic event quantifications that are modeled in the PRA. Table 1 provides a classification of

HRA quantification approaches based on the number of key probability elements (Px) in the HRA models. Currently available HRA models contain from one to four probability elements or nodes that can be used for quantification for a task. These elements are classified in Table 1 based on descriptions of the cognitive and implementation steps required to carry out an action task. Examples of the method for each Px are provided in Appendix A. The examples are not expected to cover all modeling approaches because within the community of HRA analysts there are varying viewpoints on the depth of HRA needed for PRAs. The consideration of Px permits the development of new methods for quantification. HRA 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.

3.2.3 *Data for Human Interactions*

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 to address cognitive and implementation errors 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 PRA for the conceptual ESBWR design in DCD Tier 2 Chapter 19, includes the human error contribution as part of each basic event input data. The impact of the human error modes on the basic event such as errors of commission (EOC), while not explicitly modeled in the level of detail, are expected to produce consequences no greater than modeled in the end states of CD and large early release. Error mode data such as EOC for explicitly modeled actions that are not mitigated by the design are identified through the top down HFE operational analysis, review of OER events, experienced operator interviews and observations using the part-task simulator during the design. These activities provide both design-specific human errors and operator response data.

3.3 Application to the ESBWR

The GE HFE design team will select specific methodology and modeling approaches for the ESBWR by using information from HRA reports on data, models and methods [e.g., from sources such as NUREG/CR-1278, EPRI NP-3583, NUREG/CR-4772, EPRI NP-6560-L, EPRI TR-100259, NUREG-1624, Hollnagel, 1998, NUREG-1764, NUREG-1792, and NUREG/CR-6883]. Standards include ASME-RA-S-2002, and IEEE 1082.

The HRA inputs include descriptions and analyses of operator functions and task requirements, previous PRA identified action tasks 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 relative 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 demonstrates how these human action tasks 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 action tasks within the context of the PRA.

  For human action tasks that are required to satisfy a safety function, as identified through the operational analysis (i.e., SFRA, AOF and TA), the level III requirements in ASME-RA-S-2002 shall be applied to support quantification of these risk-important HAs in dominant accident sequences. The HRA assumptions involving diagnosis, decision-making, and planning and implementation strategies during accident responses will be validated by event simulations using experienced crews, and by walkthrough analyses using personnel with operating experience to apply emergency operating procedures (EOPs) and other procedures. The validation process does not exclude the use of a plant-specific control room mockup or simulator to simulate conditions that trigger operator actions. Selected validations are conducted to support as designed quantification of the PRA.

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

  These include: accident analyses from design basis events, operating 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 procedures, EOPs or other specific written procedures. These items are referred to as PSFs that are managed through the design of the HSI.

- Evaluating the effects of HSI advanced technology on human performance and the potential to change the human error mechanisms due to the advanced technology. The evaluation of advanced 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 new HSI design features,
  - 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 updated 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 action tasks with an emphasis on human error mechanisms.

  The likelihood of operator error is minimized for risk-important HIs by identifying key human 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 action tasks and associated error mechanisms that are modeled including human to human dependencies and dependencies between human action tasks and hardware failures.

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

  These analyses use a variety of importance measures, HRA sensitivity analyses, and top down operational analyses to ensure that risk-important HAs are not overlooked.
- Integrating the PRA and HRA activities into plant design activities by defining safety important action tasks, 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 documents support a basis for providing risk-monitoring tools.

4 HRA IMPLEMENTATION FRAMEWORK

The specific HRA systematic processing framework for supporting the HFE HSI design requirements, obtaining input information and for selecting modeling approaches are established by the HSI design team. The HRA brings 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 2.

4.1 HRA Interactions with HFE tasks

Figure 2 indicates that the HRA task receives from the baseline PRA a listing of human interactions modeled in the PRA. The HIs are ranked by their level of importance using several different important measures. These risk-important human interactions from the PRA/HRA are 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 demonstrates how these human action tasks 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 interacts with the Task Analysis by providing critical human action tasks and errors to the Task Analysis and receives from the Task Analysis detailed definitions of tasks defined through the Function Allocation process.

The HRA interacts 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 establish a basis for future human performance monitoring and help prioritize corrective actions. The HRA task permits examination of assumptions used in designing the HSI with regard to the ability of licensed operators to perform needed tasks.

The HRA task enhances PRA based information to help prioritize maintenance actions and identify plant configurations to avoid during plant operation.

4.2 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 priority of display elements.

The initial baseline ESBWR PRA study, which is described in the ESBWR DCD Chapter 19, is used as the starting point for defining risk-important HA tasks. An ESBWR design objective is to avoid the need for operator actions for the first 72 hours following an initiating event for the design basis events. However, HAs that involve monitoring, planning and scheduling of system operation and asset management may contribute to a system or component basic event failure probability via the failure rate and outage time. Furthermore, risk sensitive HAs that backup automated systems that are part of the plant defense-in-depth features may be identified in some PRA sequences that are beyond the design basis events. The details of how these HAs, which support defense-in-depth risk-important hardware and systems, are defined during the HFE operational analysis of each system. Results of the operational analyses identify details about how these HAs interact with the systems and plant prior to and following initiating events to reduce risk in the beyond design basis events.

From the ESBWR PRA model as described in DCD Tier 2 Chapter 19, Tables 19.1-3, 19.2-1 and 19.2-3 list important components, systems functions, tasks and event initiators considered in the ESBWR PRA model and PRA models of previous BWR designs. The basis for mitigating or eliminating the previously defined important BWR human actions in the ESBWR design is provided. Table 19.1-3 lists hardware elements that are important. The human interactions for these hardware elements involving maintenance, repair, and backup to automatic functions are defined during the operational analysis by the HFE team. This process produces a clear listing of human actions that contribute to operation of plant and system functions. The process provides a structure for identifying potential EOC associated with defined actions. Additional human actions are defined during simulator training, procedure development and plant operation.

The HRA/PRA follows ASME-RA-S-2002, principles as applied to a conceptual design, and continues to meet more detailed objectives as the design progresses. The HRA development follows IEEE 1082. The PRA includes both internal and external events to the extent possible during the design phase. The input to the PRA/HRA is a description of the functions in terms of the machine human roles in achieving the function or task. The main output from the PRA/HRA is a listing of potentially risk-important human interactions.

As the design progresses the HRA analyst updates the human error probability (HEP) models and data based on design features that are projected to impact performance influence factors, which in turn reduce or increase the error probability of the basic HEP model. These new HEPs become inputs to the PRA, in terms of logic structure and data changes, for reunification of the CDF and LERF models. The changes consider the scope of the human action, including factors that influence the quantification such as PSFs that reflect the HSI, procedure development, and the training program.

These changes to HAs, when incorporated into the PRA as HIs, refine evaluations for the reliability of core and containment heat removal systems (e.g., quantification of CD frequency for level 1 PRA changes and LERF for level 2 PRA updates which include internal and external events). The PRA provides refined importance quantifications that include both HAs and HIs which represent HSI interface improvements and other changes that increase margins to the quantitative safety goals.

The basic elements for interaction between the PRA model and HFE HRA task are shown in Figure 3. 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 action tasks for reassessment in the PRA/HRA, and updating the HRA for input to the PRA.

4.2.1 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 by 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.

The timing of transients, based on water volumes planned for the design, can be better estimated than other PSFs that depend on the details of the HSI. If operators make errors during an event, the time available to perform the action gives operators the resource of time for making corrective actions. Thus, time available for action is an important influence on the HEP. This influence is evaluated during initial screening analysis when details of the HSI that are modeled as PSFs such as cues for action, written procedures, training, implementation process and feedback on actions taken are yet to be established. As the allocation of the functions and HSI details become available for each system and the plant as a whole, the HRA models are refined to explicitly address other PSFs. These more detailed models may show that time available becomes less important and the HRA model becomes dominated by lack of a cue, poor procedures, lack of training, difficult to implement procedures or no feedback on the action taken. Thus, time is not always the most important PSF and this is determined during the detailed HRA modeling. HIs that are performed during plant operation and identified for evaluation of HEPs consist of three types.

First, Type a human interactions take place before an initiating event. Type A errors leave systems in an unrevealed state of unavailability (e.g., fail to restore equipment to their normal condition following a test and/or maintenance) are evaluated. The HEP for an unrevealed fault depends on the HSI, the crew checking process, and feedback from systems. In cases with good feedback Type A human errors can be detected as a revealed fault and be corrected before it either triggers an initiating event in a front line system or becomes an unrevealed fault in a support system.

Second, Type B human interactions are those whose errors can cause a revealed fault that triggers an initiating event. The HEP for Type B actions depends on the HSI, the control interface navigation process, and ability to make sure that actions taken are appropriate in the context of the system configuration. The HEP modeling for Type B human actions is typically included as part of a statistical analysis of the initiating event frequency in most PRAs.

Third, Type C human interactions address successes and errors in responses to initiating events. Type C HIs are the most time sensitive for nuclear power plants (NPPs). For the Type C HIs, HEPs are conservatively selected based on the time available to perform the action task. The time available for an action task is based on water volumes available to remove heat under the specific scenario conditions. Sources of water that contribute to time for action are contained in the reactor vessel, the suppression pool, gravity driven cooling supply pool, reactor water cleanup and shutdown cooling, and the auxiliary fuel pool. Until ESBWR design details are established screening criteria are used to estimate the initial HEPs. Initial screening HEPs is updated when special features of the HSI, additional training or development of written procedures and instructions that include the EOPs are provided for the HRA (e. g., a lower HEP value reflects clarified procedures or an improved HSI).

Initial screening criteria are based on four general time period categories for HI tasks that must occur to prevent CD or a large early release 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 the HRA screening process takes no credit for HIs in the first category (e.g., a HEP of 1.0 is used). In general, the failure probability for the other categories is approximately one order of magnitude below the previous (e.g., HEP ~ 0.1, 0.01 and 0.001 for time periods 2, 3, and 4).

The output of the initial PRA model is a set of accident sequences that contribute to CDF and LERF. The, described as basic events, are included in the accident sequence descriptions. The importance ranking tools are then used to determine important systems, structures components, and supporting HIs that are modeled as basic events. Through the review and evaluation of these 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 initial 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 a HA, and the applicability of general or specific written procedures to the combination of HAs represented as a HI in the PRA model. Additional HRA support comes from accident analyses of design basis events, operating 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 are used to upgrade the PRA model to include design-specific HSI issues. When the "as designed elements" from the other plant systems are incorporated into the ESBWR PRA, it becomes an "as designed PRA/HRA." This PRA/HRA provides a stating point for the MCR risk monitor.

4.2.2 HRA qualitative evaluation for HFE tasks

The first HFE HRA sub-task is to expand the detailed description of risk-important HAs currently identified in the ESBWR PRA. The function 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 Table 1 and the guidelines from Appendix A to link HSI specific PSFs to an HRA quantification 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 on operator error mechanisms such as slips and mistakes.

The third HFE HRA sub task is to expand the qualitative human error description to meet the needs of HSI design objectives. This provides qualitative assumptions about procedures and training, and other PSFs. Information from HRA reports on data, models and methods from sources such as [NUREG/CR-1278, EPRI NP-3583, NUREG/CR-

4772, EPRI NP-6560-L, EPRI TR-100259, NUREG-1624, Hollnagel, 1998, NUREG-1792, and NUREG/CR-6883] provide structures, data and documentation tools.

4.2.3 Identify actions for reassessment in PRA/HRA

The operational analysis consisting of the SFRA, the AOF and TA provides an independent process for allocating machine tasks and identifying key human action tasks. HRA inputs include descriptions and analyses of operator functions and task requirements, previous PRA identified actions and errors, performance factors associated with the operating characteristics of HSI design, procedures for normal, startup, shutdown, and emergency operations as well as training programs.

For some of the risk-important HA tasks in dominant accident sequences the GE HFE design team considers the use of level III requirements in ASME-RA-S-2002 (e.g., use of simulator data collection) to guide the HRA quantification process. HRA assumptions in risk-important HAs involving diagnosis, decision-making, planning and implementation strategies during accident responses are validated by techniques such as event simulations using experienced crews, or walkthrough analyses using personnel with operating experience to apply procedures for specific scenario conditions. The walk through validation process does not exclude the use of a plant-specific MCR mockup or simulator. Such reviews and validations also support quantification of the as built PRA/HRA.

4.2.4 HRA Update evaluation

The goal of this sub task which is shared by the GE HFE design 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 3 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 HSI)
- 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.

4.3 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 operating staff to passive safety functions that rely primarily on inherent features of the design. These inherent design features shift the fundamental operator tasks from manual back up for active systems that protect against CDF and LERF, to monitoring and supporting operation of the natural circulation systems during transient events that inherently protect against CDF and LERF.

The items listed as assumptions for HRA quantification are based on elements in ASME-RA-S-2002 for PRAs on completed plants. The assumptions remain as assumptions during the PRA of the plant conceptual design. The assumptions are confirmed during initial part-task simulations and during the V&V. Refined assumptions resulting from the PRA become rules and commitments, which are reflected, in technical specifications, procedures and training when the plant becomes operational.

4.3.1 Design impacts

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

- The cognitive tasks for operators that manage reactor safety in the ESBWR are expected to concentrate more on monitoring long-term needs and less on shorter-term manual control functions when compared with the current BWRs. For conservative HRA evaluations at the accident sequence level, it is assumed that the operators manage the event sequence using a knowledge based cognitive approach. When the relevant displays, procedures and charts, which operators use to manage the sequence specific event, are available for review by the HFE team other cognitive processing categories are assigned. The assumption of cognitive processing type is also confirmed during simulator testing.

- A licensed operator remains in control of plant operation through the HSI during all states of operation. During normal operations the operator monitors the automated control functions, performs semi-automated calibration, inspection, testing and maintenance tasks allowed with the 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 is able to assume manual control of those functions that have been assigned to automation during the function allocation. Operator training includes 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 uses 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). The initial assumption is adjusted during simulator training with operating crews.

- 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 observes 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 supports manual interventions better than predecessor designs do. This minimizes the potential for human factor problems that negatively affect plant safety and performance, for example,

  (1) knowledge, skills and ability of 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, calibration, inspection and testing 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. 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 HEPs to identify overall HEP-related changes to the HRA inputs to the PRA/HRA model.

4.3.2 *Pre-initiator HRA*

The process for developing Pre-initiator actions include:

- A systematic process is used to identify those specific routine calibration, inspection, testing and maintenance activities which, if not completed correctly, may impact the availability of equipment necessary to perform system functions modeled in the PRA. In many cases the failure rate of equipment includes contributions from human actions.

- An element of the systematic process is to further identify via review of operating experience, concept of design, procedures, and work practices those calibration, inspection, testing and maintenance activities that if performed incorrectly can have an adverse impact on the automatic initiation of standby safety equipment.

- The pre-initiator HRA and the V&V process helps identify work practices that could introduce a mechanism which simultaneously affects equipment in 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 MCR. The standby safety systems must provide adequate instrumentation and alarms in the MCR and local control stations for operators to be effective in supporting detection and recovery of unavailable systems before resuming normal plant operations. The ESBWR is designed to prevent inadvertent isolation of a standby system. For example, plant startup can't proceed until opening the closed isolation valve clears alarms that indicate a maintenance isolation valve in the Gravity Driven Cooling System is closed.

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

Calibration, inspection, testing and maintenance activities can be screened from the PRA model 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, or

3. Equipment position is indicated in the control room, status is routinely checked, and realignment can be effected from the control room, or local control stations including the remote shutdown system.

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

For each activity that is not screened, an appropriate set of operating failure events (OFEs) are defined to characterize the impact of the failure mode or mechanism as an unavailability of a component, system, or function modeled in the PRA. Consideration the following issues is addressed when quantifying pre-initiator actions.

1. Assess the joint probability of the OFEs for dependency with other OFEs (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. Where applicable operating experience is used to support quantification of the impact that calibration, inspection, testing and maintenance activities have on overall system unavailability.

The HEP evaluations for pre-initiator human failure events are 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.

4.3.3 Post Initiator HRA

The processes for developing post-initiator actions are:

A systematic review of relevant functions, task definitions and procedures is used to identify the set of operator responses required 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, alarm response procedures) to define human actions in the context of the accident scenarios, and

2. Review system operation to develop how the system(s) functions and the human interfaces with the system are modeled in the evaluation the HEPs.

3. Verify that actions required to initiate (for those systems not automatically initiated), operate, control, isolate, or terminate systems and components used in preventing or mitigating CD or a large early release as defined by the success criteria (e.g., operator initiates shutdown cooling) are included in the PRA model.

4. Verify that 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) are included in the HRA evaluation and PRA model.

Human failure events are 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) the procedures and sequence of events with plant operators and training personnel to confirm that the operator's interpretation of the procedures is consistent with training objectives and plant observations.

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

A set of OFEs can appear in a PRA accident sequence or cutset as an unavailability of functions, systems or components as appropriate to the level of detail in the accident sequence and system models. Failures to correctly perform multiple responses for each OFE may be grouped into one OFE basic event if the impact of the failures is similar or can be conservatively bounded. Supporting information for grouping is available in the Task Analysis. To complete the qualitative definition of a grouped OFE, 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 to correct detection and evaluation errors, and

- The specific detailed tasks (e.g., component level) required to achieve the goal of the HAs, or HIs required for a successful response.

The assessment of the HEP for the post-initiator OFE is 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 for different types of OFEs are shown in Appendix A. The models shown in Appendix A provide a basis for quantifying basic event HEP estimates at different stages of the design, for different action types (e.g., pre-, post-, and initiator triggers), and for different levels of detail (i.e., some of the detailed models are very expensive to use on a action by action basis). The process is to select a model that does not exceed the amount of the information available at the time of the update. If the simple model is sufficient, it can remain in place (for actions that are not risk-important) even as the more detailed models are applied to the high risk-contributor human actions. If necessary, all modeled HIs and OFEs can be calibrated to each other based on their relative complexity and the accident context.

The models should address failure in cognition as well as failure to execute tasks. When estimating HEPs the impact of PSFs on the following plant and scenario specific examples can be considered in the evaluation. The evaluation 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 HIs in dominant scenarios can be based 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 explicitly, if it can be demonstrated that the action is plausible and feasible for those scenarios to which they are applied. Estimates of probabilities of failure addresses dependency on prior human failures in the scenario. The relative consistency of the post-initiator HEP quantifications is evaluated by the following:

1. Review the OFEs 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 with multiplying OFEs 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.

4.4 HRA Risk Importance for HSI Design Updates

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

1. Whether the HRA evaluations used for previous BWR designs remain valid for the ESBWR design,

2. Whether the human errors analyzed in the previous LWR 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 new errors may be introduced by ESBWR HSI design features that are not modeled by previous designs HRA and PRA, and

5. Whether the consequences of errors, established in the previous plant HRAs, may change for the ESBWR.

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

5 HRA DOCUMENTATION

5.1 Results summary report

A HRA results summary report discusses how the Human Reliability Analysis is applied in the HFE process. The report provides a list of risk-important HAs, HIs and OFEs and summarizes how the risk-important basic events and their associated tasks and scenarios are addressed during the various phases of the design process (e. g., in allocation of functions analyses, task analyses, HSI design, procedure development, and training). The summary results report also discusses validation of the HRA assumptions.

5.2 Periodic Reports

Progress on the iterations of the HRA with the PRA is kept as files that document and link HRA evaluation updates to the list of HIs modeled in the PRA.

5.3 Technical Information in Report

The HRA for both Pre- and Post- initiators are documented in a manner that facilitates PRA applications, upgrades to the model and peer review. An example HRA is 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 includes:

1. Generic and plant specific assumptions that were made in the HRA, include:

   - The bases for the assumptions, and

- Their impact on the CDF and LERF results.

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

3. Source(s) of data used to quantify human actions, include:

    - 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, and
    - A listing of all HEPs for each post-initiator human action and significant dependency effects.

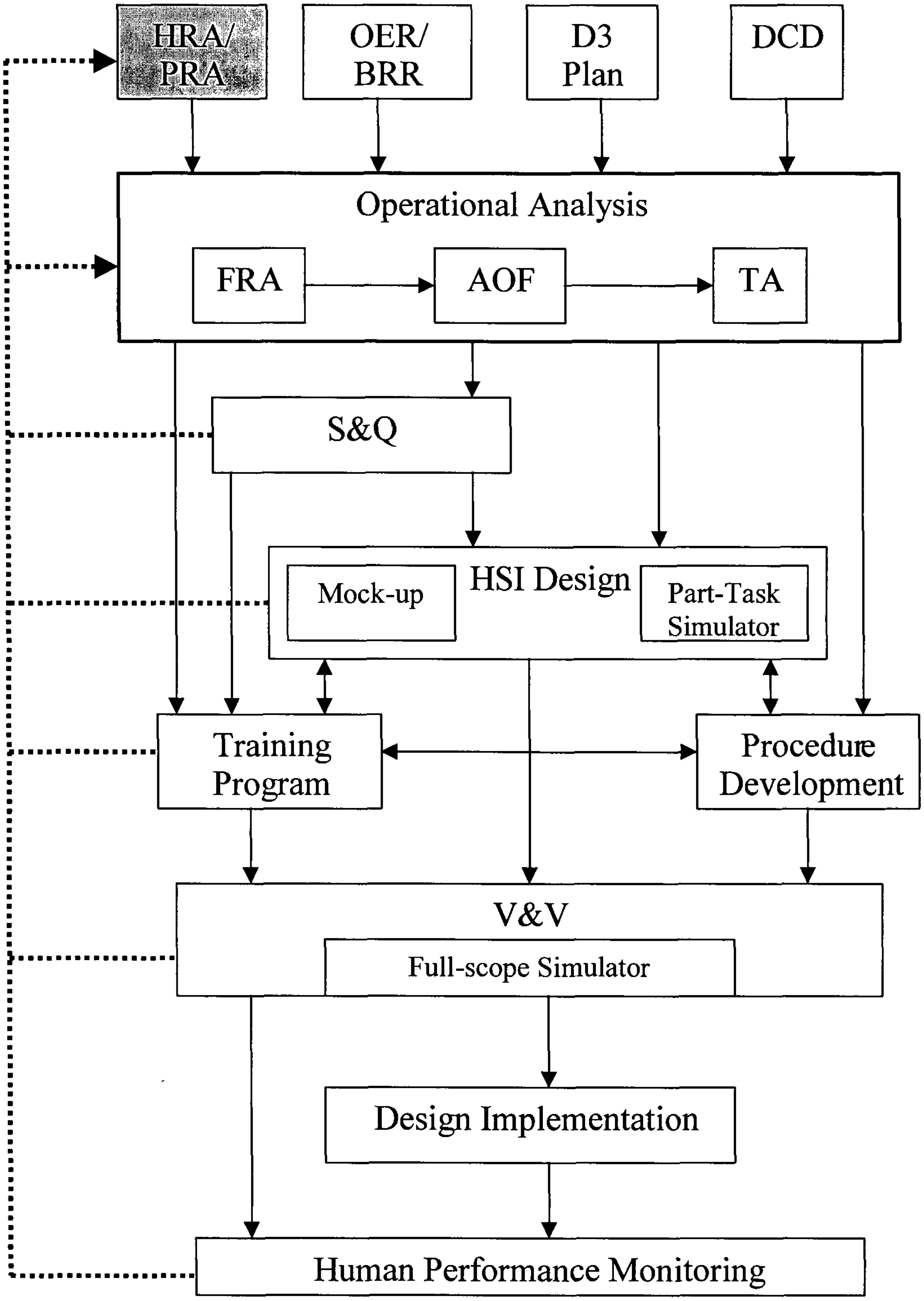

Figure 1 Overview of the human factors engineering process

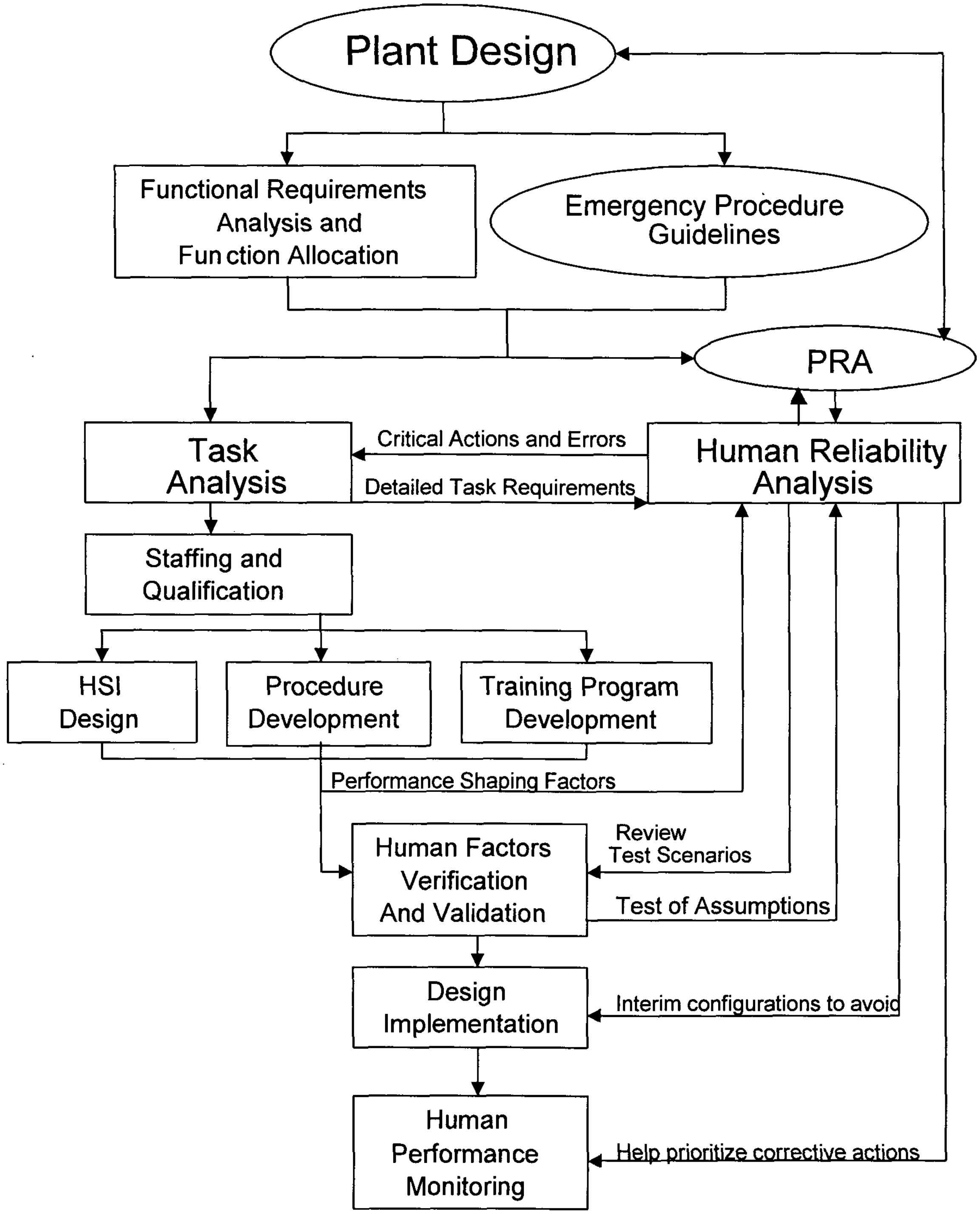
Plant Design
Functional Requirements Analysis and Fun ction Allocation
Emergency Procedure Guidelines
PRA
Task Analysis
Critical Actions and Errors
Detailed Task Requirements
Human Reliability Analysis
Staffing and Qualification
HSI Design
Procedure Development
Training Program Development
Performance Shaping Factors
Human Factors Verification And Validation
Review Test Scenarios
Test of Assumptions
Design Implementation
Interim configurations to avoid
Human Performance Monitoring
Help prioritize corrective actions

Figure 2 HRA task interactions with other HFE tasks

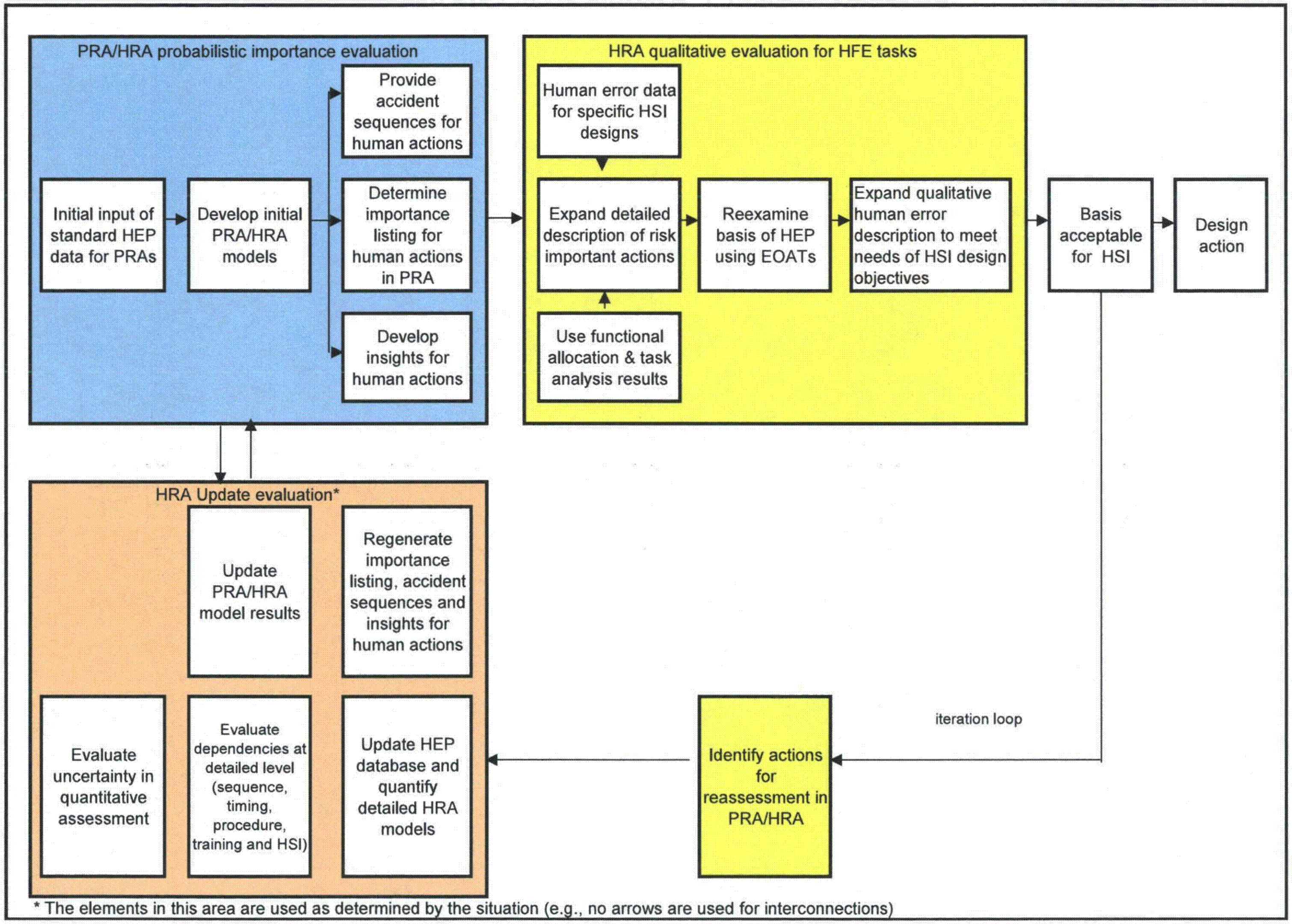
PRA/HRA probabilistic importance evaluation
Initial input of standard HEP data for PRAs
Develop initial PRA/HRA models
Provide accident sequences for human actions
Determine importance listing for human actions in PRA
Develop insights for human actions
HRA qualitative evaluation for HFE tasks
Human error data for specific HSI designs
Expand detailed description of risk important actions
Use functional allocation & task analysis results
Reexamine basis of HEP using EOATs
Expand qualitative human error description to meet needs of HSI design objectives
Basis acceptable for HSI
Design action
HRA Update evaluation*
Update PRA/HRA model results
Regenerate importance listing, accident sequences and insights for human actions
Evaluate uncertainty in quantitative assessment
Evaluate dependencies at detailed level (sequence, timing, procedure, training and HSI)
Update HEP database and quantify detailed HRA models
Identify actions for reassessment in PRA/HRA
iteration loop
* The elements in this area are used as determined by the situation (e.g., no arrows are used for interconnections)

Figure 3 Link between the PRA/HRA and HFE input for HSI design

Table 1 Summary of multiple element HRA models

Approach	Purpose	Data/Models	Total HEP Formulation	Treatment of timing
One Element Model	Screening	Uses conservative trial data or simple models for initial PSA quantification. Can be applied by PRA team members	HEP= Ps	qualitative assessment
One Plus Model	Considers performance influencing factors	Considers performance factor adjustments to basic HEP qualitatively applied by HRA analyst	HEP = Pb*PSFs	qualitative assessment
Two Element Model	Provides basis for cognitive and implementation errors	Combines data base from NUREG/CR-1278 and EPRI-TR-100259 with rules to help HRA analyst select HEPs for specific context	HEP= P1+P3	qualitative assessment
Three Element Model	Provides basis for cognitive, implementation, and timing limitation errors	Uses models or simulator data to address time dependent HEP elements where the HRA analyst adjusts direct simulator measures	HEP= P1+P2+P3	Solves for t2 from system time limt. Calibrates model with simulator measures
One element integration Time Model	Provide an integrated error model for use by an HRA analyst	Integrates all HEPs assessments into a HFE assessment using several parameters adjusted by HRA analyst to provide probabilities	HFE = f(m.σR,t)	Incorporates time as log normal function calibrated to early simulator measures
Four Element Model	Provides basis for errors in detection, diagnosis, planning and implementation	Expands range of error modes for detailed examination and evaluation	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 operating 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 compared with 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-RA-S-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 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 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 for both hardware failures and human error, and address dependency on prior human errors in the scenario.

A.1.2 HRA basic questions

This appendix 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 ASME-RA-S-2002. 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:

1. 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)?
2. What is the likelihood of success in a given time interval?
3. What are the conditions within the context that increase or decrease the chance of cognitive task errors?
4. 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 HAs.

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-RA-S-2002 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-RA-S-2002 HR-D1 Category I, mostly Category I in all other areas*]

- The one-element plus models are used for detailed quantification in PRAs when the HSI and protocols for procedure use are defined. Typical PSFs include level of training, quality/availability of procedural guidance, time available to perform an action, the level of crew redundancy, the use of checking by a second operator, clarity of the cue for action, and other PSFs as defined in NURE/CR-1278 and clarified with typical HEP estimates in NUREG/CR-4772. The PRA team and the HRA analyst can use judgment to apply these values in revisions of the PRA as supporting concepts and details are defined in the design. These one element plus applications are used to justify improved HEP assessments during the PRA development process. They are typically used in pre-initiator applications to represent unrevealed errors in backup systems following calibration, inspection, testing, maintenance and repair. *[Applies to ASME-RA-S-2002 HR-C2, C3, D2, D3, D4, and D6 Category II and III for pre-initiators depending on the level of detail available and rigor of the application. Supports ASME HR-G1 for implementation tasks, G3 for category I and supports G9 when long time periods are available]*

- 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 ASME-RA-S-2002 HR-D2, Category I, F1, Category II G1 category II/III, HR-G3 Category I, HR-G4/G5 & HR-H1. Can apply to all Categories depending on data used]*

- Two-element models provide a basis for considering PSFs around two basic probability elements - cognitive and implementation task errors. These models can be expanded to include explicit error modes and mechanisms associated with cognitive and implementation task 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 ASME-RA-S-2002 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 depending on data used]*

- Three-element models provide a basis for detailed assessment by considering the impacts of PSFs on errors in cognitive task 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 ASME-RA-S-2002 HR-D2/D3/D4, Category II if applied to pre-initiators, but this would not be done for P_2. 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 depending 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 task errors and the implementation task 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 ASME-RA-S-2002 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 depending 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 1003329]. 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 a basic event set of OFEs by evaluating the dependences between actions in the same sequence.

- P_1 errors in detection and diagnosis
- P_2 delay in planning and organizing the response (e.g., non response)
- P_3 errors in implementing a desired action
- t_s time period until system changes state or fails the success criteria.
- t_1 time allocated for completing the detection and diagnosis.
- t_2 time allocated for completing planning and organizing
- t_3 time allocated for implementing the task
- $T_{0.5}$ median response time (can be measured from simulations).

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 HEP screening, based on a qualitative process structure for identifying skill, rule, and knowledge cognitive behavior [Rasmussen, 1986], are provided in EPRI NP-3583 with order of magnitude 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 task involvement is required. This classification does not apply to pre-initiator actions outside the control room using local control stations.

- Criteria 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 task process is assigned in cases where the procedure such as a contingency plan 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 NP-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 from front line systems to early decay heat removal support systems, and (3) long term – actions that establish long term cooling using support or passive systems. 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 OFEs basic event, 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 MCR 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 $T_{0.5}$, t_1, and t_2. Job performance measurements provide data for t_3.

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 P_1 (potential cognitive errors), P_2 (time to success) and P_3 (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, NUREG-1624] is:

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

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

[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 neutron 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 0.03 (e.g., 3.5 out trips of 120 starts for one operator). For new operators with less than 10 starts the HEP is about 0.1 (e.g., for 5 operators with 50 starts and 4.5 trips). The case of 0.5 of a trip is due to a second person notifying the operator. These cases supported 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.) and 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 apply those factors expected to significantly influence the results. These models are often very easy to apply and offer a simple 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 P_1 and P_3 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), RF is the crew redundancy factor, MF is the multiple component dependency factor, and PSFs represent miscellaneous PSFs [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.

development of the basic HEPs in NUREG/CR-4772 (0.03 and 0.05). 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 (0.001, 0.01 and 0.1).

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

This model applies to both pre- and post-initiator actions when time is not critical. The cognitive and implementation tasks failure 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, 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 P_1, P_2 & P_3 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

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

of the form

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. Applications of this model to evaluate dependency between multiple human actions within the same sequence are expected to produce the probability for post-initiator human failure events.

A.4.4 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 P_{1+2} and implementation errors into P_3 values and then summed for the HEP as shown in Figure A2. The main difference between the two- and three-element models is that P_1 and P_2 are combined in the cognitive element with the assumption that timing is not a significant contributor [NUREG/CR-4772, and EPRI NP-3583].

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

$$HEP = P_{1+2} + P_3,$$

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.

A.4.4.1 P_1 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.

A.4.4.2 P_3 Implementation Error quantification

Example of data for implementation errors can be found in [NUREG/CR-1278, Table 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. Applications of this two-element model to evaluate dependency between multiple human actions within the same sequence are expected to produce the probability for post-initiator human failure events.

A.4.5 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 P_2 in the HEP equation [EPRI NP-6560-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 P_1 and P_3 in the two element models can apply here. It remains to quantify P_2 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, MCR interface, communications, cue types, and etc. The following sections describe the models and data obtained from previous testing.

A.4.5.1 P_2 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 NP-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 [Hannaman, et.al. 1985].

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

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 K_i are coefficients for operator experience, stress level, quality of the 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.

A.4.5.2 P_2 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 NP-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 NP-6560-L and EPRI TR-100259] 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.

A.4.5.3 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 [EPRI 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 MCR 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.

A.4.5.4 *Timeline analysis*

The time equation is also important for the assessment. The time required for each element of the HEP equation ($t_2 = t_S - (t_1 + t_3)$) is needed. Plant-specific thermal hydraulic analyses are used to estimate system time periods (t_S). In lieu of scenario specific T/H models, the simulator may be used to estimate periods. A figure noting the cues, and values for ts can be used to evaluate the time periods for t_1, t_2, and t_3.

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

A.4.5.5 *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 due to failure of a front line system and failure of a heat removal standby support system. The operating time for the standby system also becomes important in estimating the overall reliability of the supporting system used to remove heat and maintain core temperatures within safety margins. Simple model timing benchmarks are very useful for evaluating cases with supporting system run failures after initially running, and operator recovery of the system or switch to another heat removal system.

An example of the combined HEP = $P_1(t) + P_2(t) + P_3(t)$ is shown in figure A5. In this case, t is the time from the initial cue, and the HEP is the Boolean combination of each P. Within the evaluation, t_2 is established by $t_2 = t_S - (t_1 + t_3)$ leading to a maximum fixed value for t_2 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. Applications of this three element model to evaluate dependency between multiple human actions within the same sequence are expected to produce the probability for post-initiator human failure events.

A.4.6 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 P_{1a} is divided into P_{1a} and P_{1b} to account for crews' missing the cue, selecting an inappropriate path and failing to recognize the mistake. ATHEANA [NUREG-1624] 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.

A.4.6.1 P_1 division to P_{1a} and P_{1b} in four-element HEP quantification

An advantage of using the four-element model is that it focuses on EOC 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 EOC 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 PSFs 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.

$$\text{HEP}(t) = P_{1a}(t) + P_{1b}(t) + P_2(t) + P_3(t)$$

$$t_2 = t_s - (t_{1a} + t_{1b} + t_3)$$

The timing elements in this equation are more difficult to measure, because t_{1a} and t_{1b} are difficult to separate during observations.

A.4.6.2 Performance factors in four-element models

These examples of PSFs provide some consideration for evaluation. ATHEANA uses systematic evaluation of a list of PSFs for each operator decision-making element. The PSFs listed in the table A6 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 reveal the potential for EOC. Alternate descriptions for PSFs and dependencies between PSFs have been proposed, and can be found in the CREAM modeling process [Hollnagel, 1998].

P_{1b} 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 a wrong mental model of the plant in the mind of the operators (e. g., TMI). For P_3, the actions are generally very clear, but actions outside the MCR 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 EOC. Applications of this four element model to evaluate dependency between multiple human actions within the same sequence are expected to produce the probability for post-initiator human failure events.

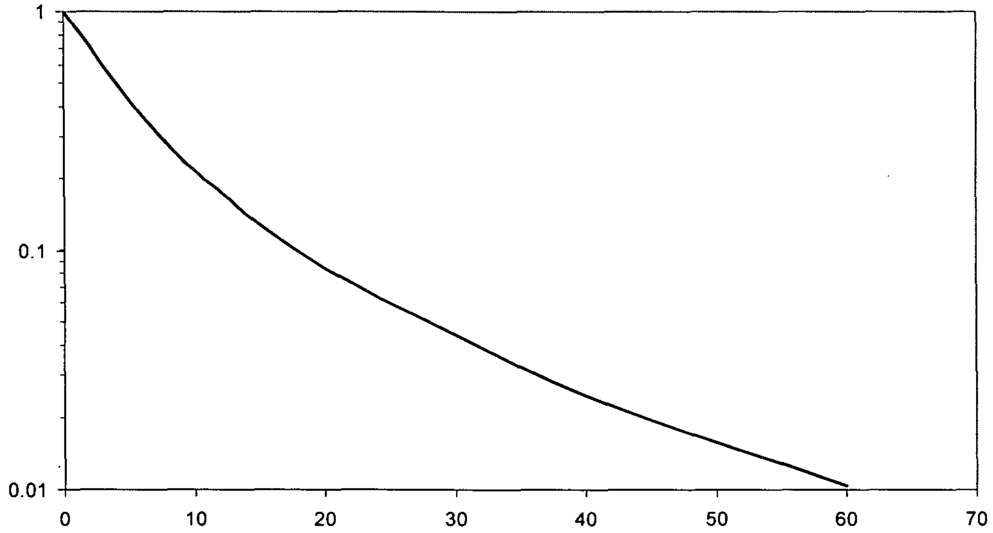

Figure A1 Time reliability correlation for one-element lumped model[4]

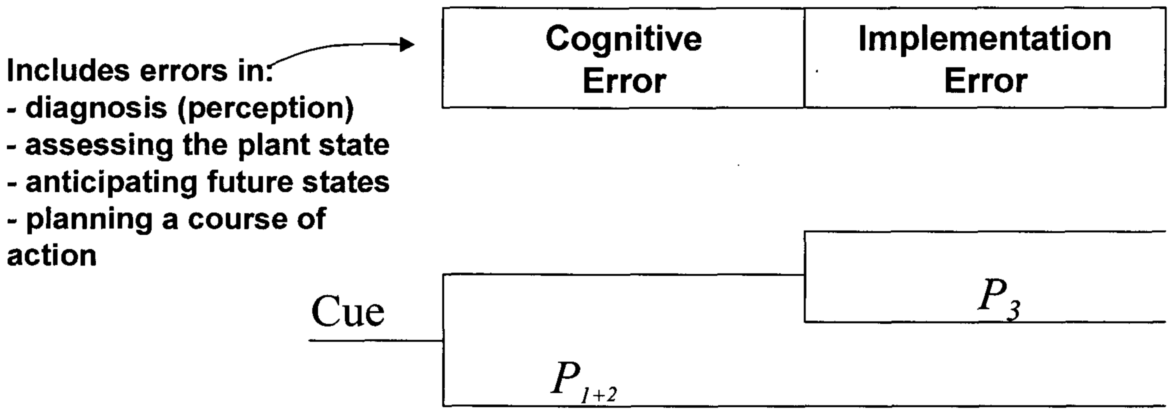

Figure A2 Operator Action Tree logic diagram for two-element HRA model[5]

[4] Dougherty and Fragola, 1988

[5] EPRI NP-3583

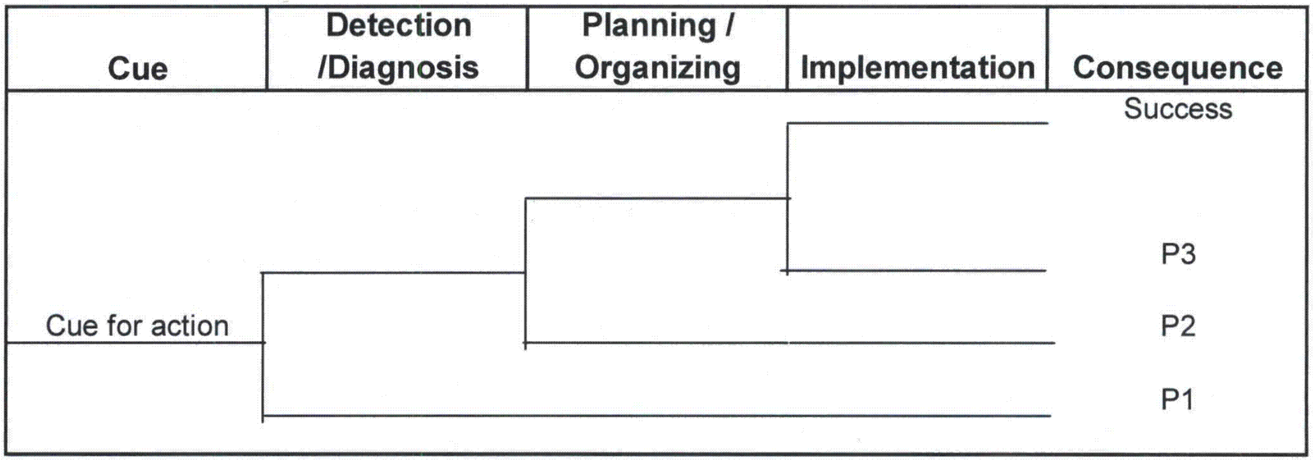

Figure A3 Operator Action Tree logic diagram for three-element models[6]

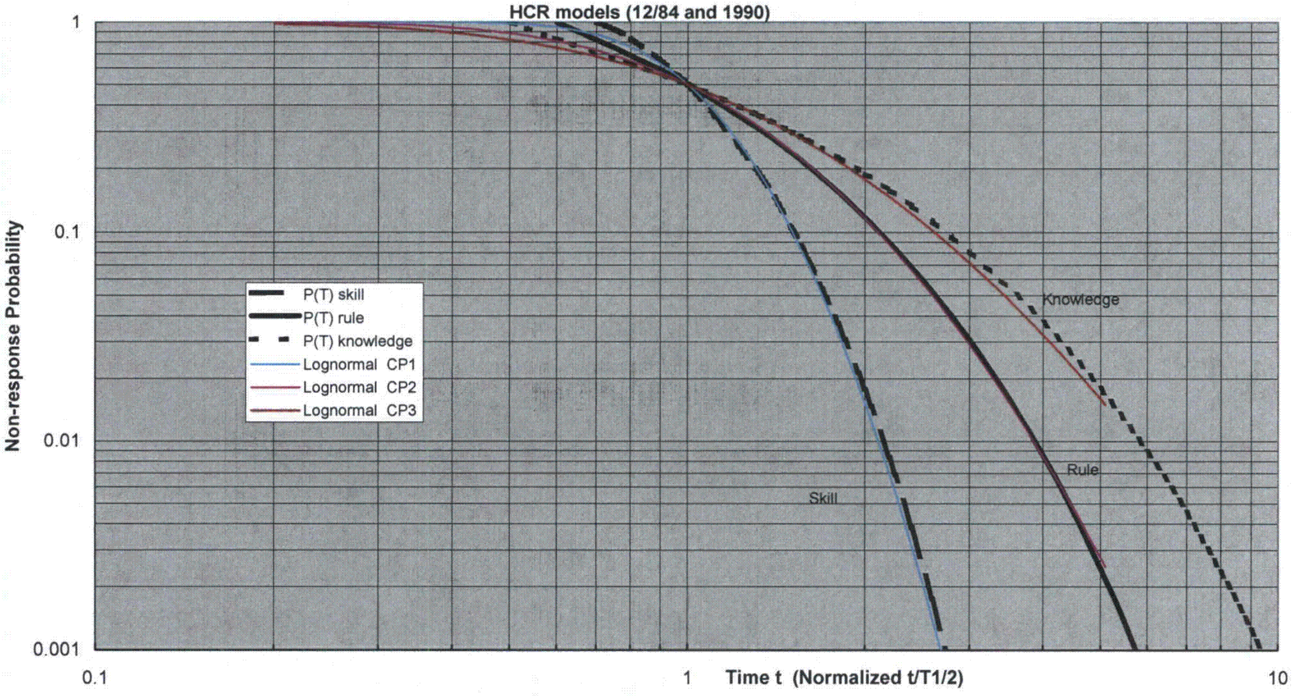

Figure A4 Comparison of HCR hypothesis and simulator data collection results[7]

[6] EPRI NP-3583, 1984 and Hannaman, et. al., 1985

[7] EPRI NP-6560-L, 1990 and Hannaman et. al., 1985

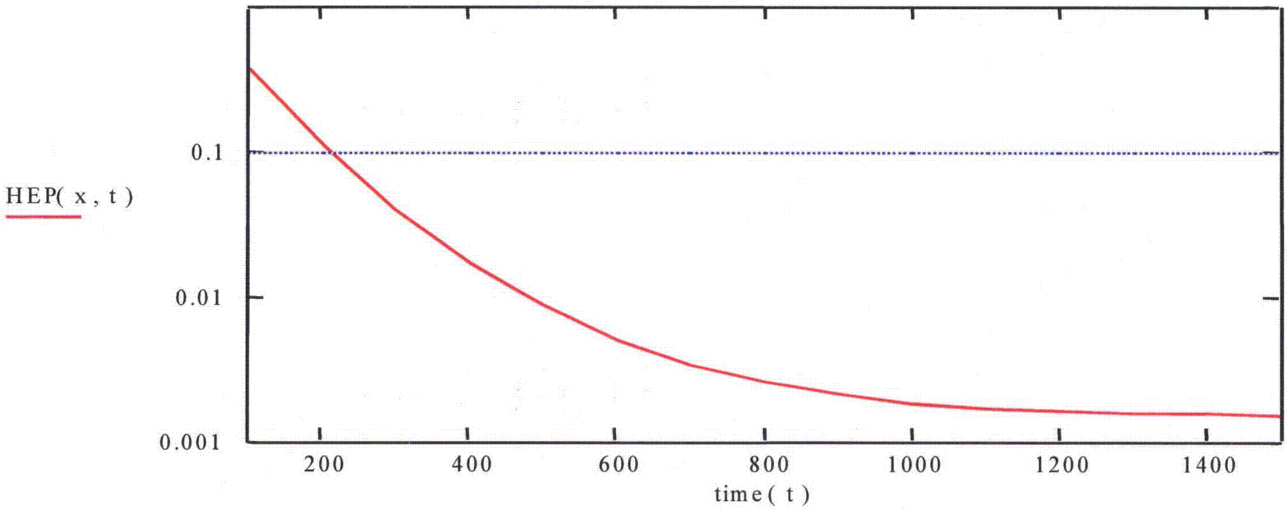

Figure A5 Example three-element model result

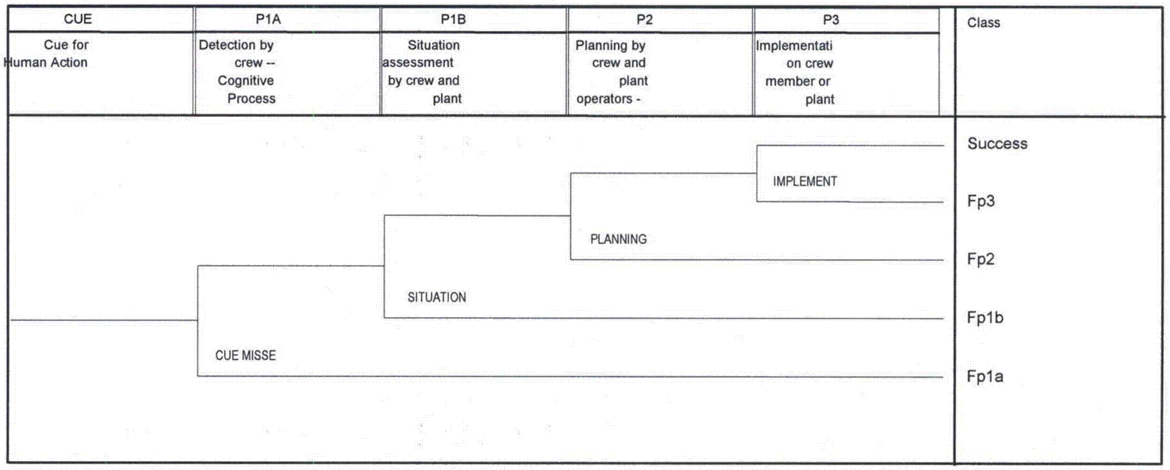
CUE
Cue for Human Action
P1A
Detection by crew -- Cognitive Process
P1B
Situation assessment by crew and plant
P2
Planning by crew and plant operators -
P3
Implementati on crew member or plant
Class
Success
IMPLEMENT
Fp3
PLANNING
Fp2
SITUATION
Fp1b
CUE MISSE
Fp1a

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			
Action Type	Behavioral 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

Table A2 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 1003329, 2002

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

Error Mechanism	Range of failure probabilities
Availability of information	Neg to 0.5
Failure of attention	Neg to 0.03
Misread/miscommunicate data	Neg to 0.007
Information misleading	Neg to 1.0
Skip a step in procedure	Neg to 0.1
Misinterpret instruction	Neg to 006
Misinterpret decision logic	Neg to 0.049
Deliberate violation	Neg to 0.95

[10] EPRI TR-100259, 1992

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] NUREG/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]

P_{1a} Detection PSFs
Indications available CR
Indications available local
Clarity of Cue-CR
Feedback for monitoring change
Availability of CR personnel
Distraction through event
P_{1b} 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
P_2 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
P_3 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 NUREG-1624, 2000, and Hollnagel, 1998.