NUREG/CR-2254
SAND81-1655
RX, AN
Printed May 1983

A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants

Final Report

Barbara Jean Bell, Alan D. Swain

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-76DP00789

Prepared for
U. S. NUCLEAR REGULATORY COMMISSION

Available from

GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

and

National Technical Information Service
Springfield, Virginia 22161

NUREG/CR-2254
SAND81-1655
RX, AN

A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants

Final Report

Manuscript Completed: April 1983
Date Published: May 1983

Prepared by
B.J. Bell, A.D. Swain

Sandia National Laboratories
Albuquerque, NM 87185

Prepared for
Division of Facility Operations
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN A1188

ABSTRACT

This document describes in detail a procedure to be followed in conducting a human reliability analysis as part of a probabilistic risk assessment when such an analysis is performed according to the methods described in NUREG/CR-1278, "Handbook for Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications." An overview of the procedure describing the major elements of a human reliability analysis is presented along with a detailed description of each element and an example of an actual analysis. An appendix consists of some sample human reliability analysis problems for further study.

ACKNOWLEDGMENTS

NUREG/CR-2254 was issued in December 1981 as a draft for interim use and comment. The document has benefitted from comments made October 26-28, 1981, by members of the Human Reliability Review Committee (Chairman: Dr. Randall W. Pack, General Physics Corporation) of the NRC/IEEE Review Conference on the Probabilistic Risk Assessment Procedures Guide for Nuclear Power Plants. This committee's comments were directed to Chapter 4, "Human Reliability Analysis," of NUREG/CR-2300, "PRA Procedures Guide," Review Draft September 28, 1981. NUREG/CR-2254 differs from Chapter 4 in that the former is a companion document to NUREG/CR-1278, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," while the latter is intended to be a more general document. In addition, NUREG/CR-2254 includes an appendix of sample human reliability analysis problems. (Some of the problems presented in the appendix are based on examples prepared by Mr. H. E. Guttmann of Sandia National Laboratories and the authors, as modified by Drs. M. Weinstein and M. Fitzwater of Human Performance Technologies.) Nevertheless, there is about a 90 percent overlap in the main bodies of the two documents.

Thanks are due to Mr. Ed M. Dougherty, Jr., Technology for Energy Corporation, who made suggestions for dealing with the incorporation of human reliability analysis into the overall probabilistic risk assessment. The authors' additional thanks go to Mr. Joseph R. Fragola, Science Applications Incorporated, who contributed a large number of technical comments. We also wish to thank Mr. James R. Jenkins, the original NRC program manager, Mr. James W. Pittman, the interim NRC program manager, and Dr. Thomas G. Ryan, the current NRC program manager, for their support and encouragement. Finally, we appreciate the reviews and comments received from Dr. D. P. Miller of Sandia National Laboratories.

The senior author, Barbara Jean Bell, is currently a Principal Research Scientist in the Risk and Safety Analysis Section, Battelle's Columbus Laboratories, 505 King Avenue, Columbus, OH 43201.

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF FIGURES

A PROCEDURE FOR CONDUCTING A HUMAN RELIABILITY ANALYSIS FOR NUCLEAR POWER PLANTS

1.0 INTRODUCTION

1.1 Objective

The purpose of this document on human reliability analysis (HRA)* is to provide a procedure for estimating the probabilities of human errors in the operation of nuclear power plants (NPPs). This introductory section defines the scope, assumptions, limitations and uncertainties, and product of a human reliability analysis. An overview of the procedure for conducting an HRA is then outlined, highlighting the major tasks involved. The methodology is described in the next section, followed by a listing of the information requirements. Next, a detailed procedure is given, along with an example of an HRA, each stage of which is presented in parallel with the description of each step of the procedure. For greater understanding of HRA methodology, the reader is urged to study the practice exercises presented in the appendix. Additional examples, human performance models, and estimates of generic human error probabilities (HEPs) for NPP tasks are found in NUREG/CR-1278[1] (short title, the Handbook), which serves as the source document for this procedure. The procedure is keyed to the 1983 version of the Handbook. (The December 1981 draft of NUREG/CR-2254 was keyed to the October 1980 draft of the Handbook.)

1.2 Scope

The HRA methodology in this document is intended to support full programs of probabilistic risk assessment (PRA) of NPPs, as exemplified by WASH-1400,[2] the Interim Reliability Evaluation Program (IREP), the Zion PRA, the Oconee PRA, the Big Rock Point PRA, and future PRAs that may be conducted as part of the National Reliability Evaluation Program (NREP). The manners in which the HRAs have been conducted in each of the current and past PRA programs have varied, but certain essentials were addressed in each and are described here. In an NPP PRA, the first effort toward identifying those human-related events affecting system reliability is made by the system analysts. The human reliability analysts then determine the human errors associated with these events that are to be defined and analyzed. Drawing from the data in the Handbook, on expert judgment, or on better sources of data if available, probabilities for these system-important errors are estimated, and their effects on system success probability will be investigated. Criteria for system success and failure are determined by the system analysts.

---

*All abbreviations used in this document are defined in the list at the end of this document.

In an NPP PRA, human tasks performed under normal operating conditions and in post-accident or post-transient situations must be considered. In the former situation, errors might be made during or following maintenance, calibration, or testing tasks or in the normal operation of the plant. These errors may occur in or out of the control room. In the post-accident situation, most but not all of the system safety-related errors occur in the control room.

In either situation, most of the errors to be identified and analyzed are made in following directives (written or oral procedures, or standard shop practice). Only occasionally are extraneous acts, operations outside the scope of the procedures, considered. That is, in most cases, whether a given directive is followed correctly is determined, while the identification of which uncalled-for elements are manipulated is not made. At times, it will be necessary to estimate the types and probabilities of errors made in interpreting plant conditions (diagnosis errors) or in deciding what actions are appropriate for a given plant condition (decision-making errors). These types of errors can have considerable impact in a PRA, so it is necessary to treat them as fully as possible.

1.3 Assumptions

We deal only with human errors--mistakes made in the performance of assigned tasks. Malevolent behavior (deliberate acts of sabotage and the like) is not considered for discussion. It is assumed that all NPP personnel act in a manner they believe to be in the best interests of the plant. Any intentional deviation from standard operating procedure is made because the employee believes his method of operation to be safer, more economical, or more efficient or because he believes performance as stated in the procedure to be unnecessary or inappropriate.

An important aspect of an HRA is the qualitative assessment of the sources of human error. This calls for identifying and understanding the underlying contributors to each error and for assessing the relative importance of each of these contributors to the system failure events being analyzed. Appropriate points in the procedure for the performance of qualitative analyses will be identified. For more information on the qualitative application of HRA to NPP operations, see the Handbook.

1.4 Limitations and Uncertainties

For a complete HRA, the PRA team should include a person who is, by professional training and experience, competent in applying human performance technology to complex systems. Such a person is usually known as a human factors specialist, an engineering psychologist, or an ergonomist. For a more detailed description of the qualifications of a human factors specialist, see pp. 8-9 of NUREG-0801.[3] This person must also be proficient in using HRA methodology as set forth in the Handbook. To carry out this procedure, he must be thoroughly familiar with and have a good understanding of this document as well as of the Handbook on which it is based. For a less complete HRA, e.g., a qualitative analysis, the only requirement in this respect is that the person performing the HRA be familiar with this document and the Handbook; he need not necessarily be a human factors specialist.

In all cases, it is presumed that the HRA will be performed as an integral part of the PRA. There will be considerable and continuing interaction between

those responsible for the HRA and those working in the area of system reliability analysis. The HRA should in no case be performed by the human reliability analyst in isolation from the rest of the PRA team. The structure of the team should in itself facilitate the interaction necessary among the several analysts.

Sources of uncertainty in HRA include the dearth of actuarial data on human error probabilities and the shortage of human performance models that have been verified in NPP situations. For the most part, the Handbook presents the best available data on human performance in carrying out NPP tasks. Most of the estimates of HEPs in the Handbook represent extrapolations from human error data based on tasks performed outside of but behaviorally similar to those performed in NPPs. In other words, tasks performed in situations other than NPPs may involve the same types of cues, interpretations, response requirements, and responsibilities as those performed in the NPPs themselves--the only significant difference may be that of the names of the facilities. Therefore, in those cases for which an analyst can find better data on human performance than are presented in the Handbook, he should use them.

In the future, it is expected that the uncertainty and subjectivity involved in estimating HEPs for NPP tasks will be reduced considerably. Under the sponsorship of the Office of Nuclear Regulatory Research, Nuclear Regulatory Commission (NRC), a program plan for a human performance data bank is being developed, and active efforts are underway to collect HEP data from realistic simulator exercises for control room tasks and from maintenance and other tasks taking place outside the control room.

As explained in the Handbook, most of the tabled HEPs relate to rule-based human actions. For some NPP operations, cognitive errors are critical, e.g., errors in evaluating the display indications resulting from a transient. There is relatively little information on errors of interpretation or decision-making, i.e., errors in the thought process. However, new models for estimating the probability of correct diagnosis are presented in Chapter 12 of the Handbook and are referenced in Section 5.7.1 of this document.

The nominal value for a specific HEP for a given human action that reflects the best estimate (based on available data and on judgment) of the probability of a particular error in a generic sense is presented in the Handbook along with uncertainty bounds. The latter are considered to approximate the 5th to 95th percentile range of the HEPs to be expected under all possible scenarios for a particular action. These uncertainty bounds are based on subjective judgment rather than on actuarial data and are not meant to represent statistical confidence limits.

As discussed in the Handbook, there are several sources of uncertainty in the generic HEPs provided. The variability of human performance is reflected in the individual differences in skill, experience, and other personal characteristics of NPP personnel. There can be wide variation in specific environmental situations and other physical aspects of the NPP tasks to be performed. Only some of this variation in performance shaping factors (PSFs) is accounted for in the Handbook data by providing different estimates of HEPs for different sets of influencing factors. The width of the uncertainty bounds surrounding each estimated nominal HEP represents an attempt to account for the residual uncertainty.

Unless specifically stated otherwise, all of the HEP estimates in the Handbook are based on a set of common assumptions that limit or restrict use of the data as stated. Exceptions to these assumptions are clearly indicated. These data apply to situations in which the following hold true:

- The plant is in a state of normal operating conditions. Also, there exists no emergency or other state that would produce in the operators a level of stress other than the optimal.
- The operations are considered to be performed without the necessity of the operator's wearing protective clothing.
- A level of administrative control roughly equal to the average of those employed industry-wide is in effect.
- The tasks are performed by licensed, qualified plant personnel such as operators, maintainers, or technicians. They are assumed to be experienced--to have functioned in their present positions for at least six months.
- The environment in an NPP control room is not adverse. The levels of illumination and sound and the provisions for physical comfort are adequate even if not optimum.

The above-mentioned factors must be evaluated qualitatively for each situation being analyzed. The determination of a situation's being similar to or significantly different from these assumed scenarios is highly subjective. There are no absolute guidelines for establishing a plant's conformance to what is "normal" for the rest of the industry. Only with experience and exposure to several operating plants can a human reliability analyst develop the skills necessary to perform these discriminations successfully and reliably.

It is mainly the level of detail that will differ for HRAs performed at different stages in the life cycle of an NPP. The level of detail of the methodology presented in this procedure is predicated on the application of HRA to NPPs that are already providing power. For earlier applications, e.g., at the construction permit stage, some of the information necessary for a detailed task analysis of that particular NPP will not be available. Nevertheless, the methodology can still be applied, as discussed in Part II of the Handbook. For very early applications of HRA to an NPP, much of the information needed to determine the potential for human error in that plant will have to be derived from HRAs of similar, operating plants.

1.5 Product

The main result of the HRA effort in a PRA for NPPs is, for each iteration of the HRA, a set of estimated plant- and situation-specific human error probabilities. During quantification of the risk-significant events, these estimated HEPs can be grouped into sets for incorporation into the total PRA on the basis of their affecting the reliability of a component, a whole system, or the entire response scenario required by an initiating event. The assumptions on which these sets of estimates are based are also presented to the systems analysis team.

2.0 OVERVIEW

The four phases of HRA (familiarization, qualitative assessment, quantitative assessment, and incorporation) are shown in Figure 1. Most HRA methods follow

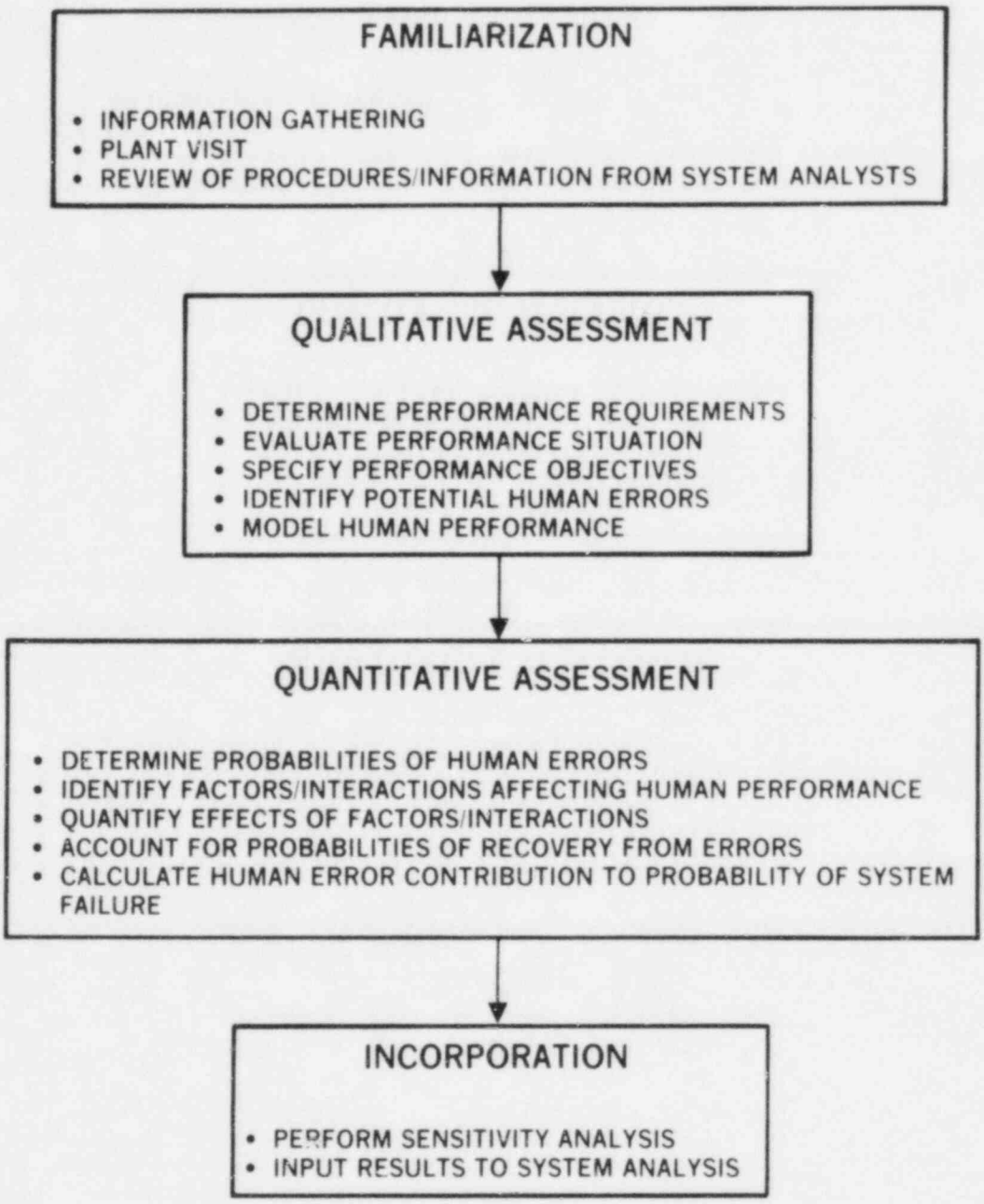


Figure 1 Four phases of a human reliability analysis.

this general format. A block diagram illustrating the application of these phases to the procedure followed in performing an HRA using Handbook methods is shown in Figure 2. The sequence of activities shown in this figure may, however, be different from that of an analysis performed in another context. Also, since this is a block diagram and not a flow chart of actual activities, the interactions between the human reliability analyst and the rest of the PRA team are largely left off. This is not to suggest that they do not exist, but simply to provide a schematic of the major tasks to be performed by the human reliability analyst himself. In reading the description of these activities, it is necessary to keep in mind that the order of the various HRA activities is not a fixed one in which the activities are accomplished only once. In fact, the entire process is highly iterative and its parts recursive.

It is necessary to begin preparation for the HRA concurrently with the rest of the PRA. Otherwise, there will not be sufficient time to perform all the activities required for an accurate assessment of the effects of human errors.

As mentioned, the HRA is an iterative process. Various stages of the HRA, as diagrammed in Figure 2, will be repeated as additional plant-specific or other information becomes available. A complete HRA is assumed in Figure 2; for less detailed analyses such as (in some cases) a bounding analysis, the performance of the activities represented by some of the blocks can be modified to reflect the level of detail of the analysis, while some of the blocks can be eliminated. Obviously, the less plant-specific the information analyst has, the more uncertain his estimates. In a sense, the degree of uncertainty drives the level of analysis that is possible. The more uncertain an analyst's estimates, the closer his analysis is to being qualitative in nature. A bounding analysis is more appropriate than a strictly quantitative assessment of the likelihood of any set of human errors when the information leading to the estimation of such errors is suspect.

2.1 Plant Visit

A survey of the control room performed in conjunction with a general plant visit is an essential preliminary to the performance of a plant-specific HRA. The purpose of such a survey is to allow the analyst to familiarize himself with the operations-relevant characteristics of the plant. No assessment of the control room in terms of design recommendations is made. The intention of such a visit is to identify the aspects of the control room, the general plant layout, and the plant's administrative control system that affect generic human performance. No evaluation of any individual's performance is to be done. This point must be clearly understood by plant personnel if accurate and complete information is to be obtained.

2.2 Review Information from System Analysts

For a given scenario or sequence of events, the system analysts pinpoint human actions that directly affect the system-critical components they have previously identified. In the light of the information obtained from the plant visit, the human reliability analyst must review these actions in the context of their actual performance to determine whether any factors exist that influence behavior on these system-critical actions that may have been overlooked by the system analysts. For example, if performance on a noncritical element subsequently affects performance on a system-critical element, this

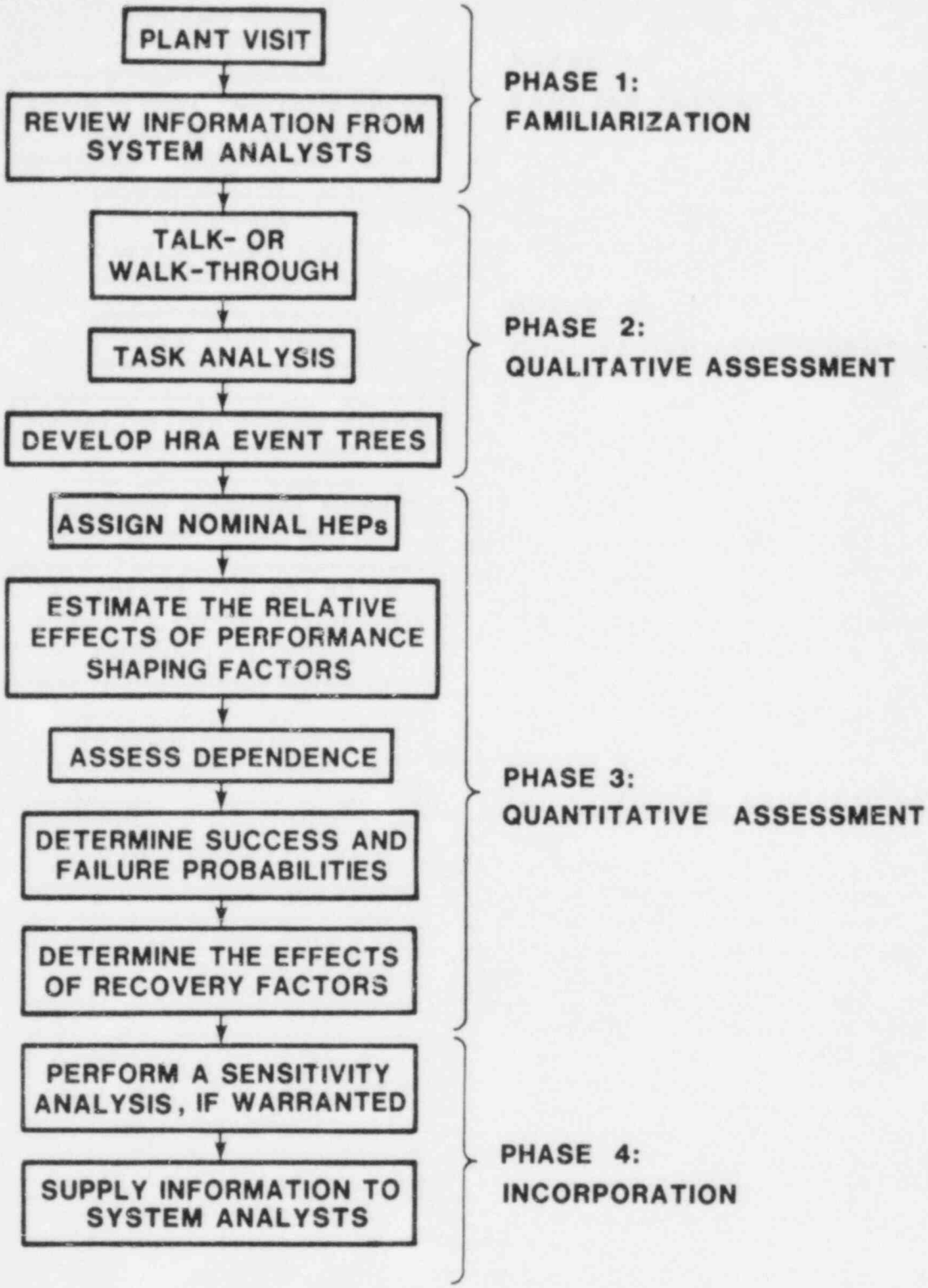


Figure 2 An overview of a human reliability analysis. (Note: The iterative nature of the analysis is not shown in the block diagram.)

effect must be considered in the HRA even though the first task in itself is not important to the reliability of the system as defined by the system analysts.

2.3 Talk- or Walk-Through

Sometimes performed in conjunction with the survey of the control room and sometimes at a later date during interviews with operations personnel, talk- or walk-throughs of the task sequences in question form a necessary part of any HRA. The terms talk-through and walk-through are synonymous. They are conducted by the human reliability analyst and performed by plant operations personnel. In this activity, the analyst questions the operator on points of the task performance until his understanding of the task is such that he could perform it himself or at least be able to understand fully the performance of an operator. Performance specifics are identified along with any time requirements, personnel assignments, skill-of-the-craft requirements, alerting cues, and recovery factors. (Performance talk-through for activities not defined by a specific plant procedure can be done, but the level of effort required by the human reliability analyst for such an analysis is greatly increased.)

The information obtained in a talk- or walk-through should enable the analyst to estimate the effects of a situation's PSFs. (See Chapter 3 of the Handbook for a discussion of these factors.) Modifications made to the nominal estimates of HEPs that are found in the Handbook will be based on information gathered at this point.

2.4 Task Analysis

Next, a task analysis should be performed, as described in Chapter 4 of the Handbook. (The discussion in Chapter 4 considers the gathering of information during the plant visit and the performance of the talk-through to be components of the task analysis.) We define a task as a quantity of activity or performance that the operator sees as a unit either because of its performance characteristics or because that activity unit is required as a whole to accomplish some part of the system goal. Only safety-relevant tasks are considered in the PRA. A task analysis involves breaking down each task into individual units of behavior. Usually, this breakdown of tasks is accomplished by entering information relative to each specific human action into a table. Format requirements for such a table are not rigid--any style that contains information in such a manner that it can be retrieved easily can be used. These formats will reflect the level of detail as well as the type of task analysis to be performed. The analysis itself and the information obtained from it can be either qualitative or quantitative. Examples of task analysis formats are presented later.

Specific potential errors should now be identified for each unit of behavior shown in the task analysis. As defined in the Handbook, a human action (or its absence) constitutes an error only if it has at least the potential for reducing the probability of some desired system event or condition. The existence of this potential should be identified in conjunction with the system analysts. For every human action appearing in the task analysis table, likely errors of omission and commission should be pinpointed. As mentioned earlier, extraneous acts are seldom considered. For example, the analyst may

determine that because of the control panel layout, a selection error is possible during the manipulation of a specific switch, but his analysis will not usually predict which other element will be chosen, nor will it deal with the system effects of the operator's selecting a specific incorrect switch. An exception to this statement is illustrated in the second case study in Chapter 21 of the Handbook.

The situation must be evaluated for other errors affecting system success and failure probabilities that do not appear in the task analysis. Some of these can be disregarded by assuming for the entire analysis that a certain condition does or does not exist. For example, in the case of a post-maintenance test, if we are interested in the conduct of the test itself, we may assume that the supervisor has already ordered the test. In determining which of these assumptions may be made, great care must be taken by the analyst. In analyzing actual plant conditions, it is inappropriate to assume that something that should be done will always be done.

2.5 Develop HRA Event Trees

Each of the errors defined above should be entered as binary branches on an HRA event tree, as described in Chapter 5 of the Handbook. The possible error events should appear on the tree in the chronological order in which they might potentially occur if such order is relevant. The suggested format for HRA event tree diagramming will be presented later. The product of the HRA event tree is a probabilistic statement as to the likelihood of occurrence of a given sequence of events. Some PRAs deal only with the probability of successful completion of all human actions, while others take a more global approach, considering all system interactions and reactions that may contribute to the probability of system success. In either case, recovery factors usually are not included at this time. This is simply a time-saving feature of this HRA procedure. If, in a preliminary system analysis, the probability of an unrecovered human error is found not to impact system safety significantly, there is no need to expend additional time and effort identifying and quantifying the effects of recovery factors acting on the situation.

2.6 Assign Nominal Human Error Probabilities (HEPs)

An estimate of the probability of each human error event appearing on the HRA event tree must be derived from the data tables in the Handbook, other data sources, or expert judgment. Tables of HEPs (and their associated uncertainty bounds) for generic task descriptions are found in Chapter 20 of the Handbook. One of the reasons for recommending the analyst's familiarity with the Handbook is that he must have a thorough understanding of the assumptions and limitations underlying each of these tables. If there is no exact match between the descriptions of a task found in the Handbook and that defined by the task analysis, the estimated HEP for a similar task may be used as is or may be used for extrapolation for that situation, depending on the degree of similarity between the descriptions. Similarity in this context refers to the likeness of required operator behaviors. There can be a high degree of similarity between the performance of two tasks even though the equipment be dissimilar. In our experience, a person skilled in human performance technology is required for these kinds of judgments.

2.7 Estimate the Relative Effects of Performance Shaping Factors

HEPs assigned for a given task must now be modified to reflect the actual performance situation. For example, if the labeling scheme at a particular plant is very poor compared to those described in MIL STD-1472C[4] or NUREG-0700,[5] the HEP should be increased toward the upper of its uncertainty bounds. If the tagging control system at a plant is particularly good, perhaps the HEPs for certain errors should be decreased.

Some of the PSFs have an effect on the performance of a whole task or on that of the whole procedure, while others have an effect on certain types of errors regardless of the types of tasks on which they might occur. Still other PSFs have an overriding influence on the probability of occurrence of all types of errors in all conditions. Familiarity with those sections of the Handbook that deal with the effects of PSFs is absolutely necessary in order to perform an accurate HRA.

2.8 Assess Dependence

For any given situation, different levels of dependence may exist between an operator's performance on one task and on another because of the characteristics of the tasks themselves or because of the manner in which the operator was cued to perform the tasks. Dependence levels between the performances of two (or more) operators may differ, also. The analyst should keep in mind that the effects of dependence on human error probabilities is always highly situation-specific. The concepts presented in the chapter on dependence in the Handbook must be followed precisely. The analyst should also remember that the Handbook dependence model deals only with positive dependence. If negative dependence is assessed, some basis other than this dependence model must be employed for estimating conditional probabilities of success or failure. Chapter 10 of the Handbook includes a sample HRA using negative dependence.

2.9 Determine Success and Failure Probabilities

Based on the criteria for system success and failure supplied by the system analysts, the end point of each path through an HRA event tree can be labeled as a success or failure. Multiplying the probabilities assigned to each limb in a success or failure path through the HRA event tree provides a set of success and failure probabilities that can then be combined to determine the total system success and failure probabilities.

2.10 Determine the Effects of Recovery Factors

It is often convenient to postpone consideration of the effects of recovery factors in the sequence of activities in the HRA until after the total system success and failure probabilities have been determined. These estimated probabilities for a given task sequence may be sufficiently low without considering the effects of recovery factors so that the sequence does not appear as a potentially dominant failure mode. In this case, it can be dropped from further consideration.

2.11 Perform a Sensitivity Analysis, If Warranted

To determine the effect of a single parameter or assumption on the total system success probability, a sensitivity analysis can be performed. In this

exercise, the value of a given parameter is manipulated or an assumption is changed and the resulting system success probabilities are compared to judge the impacts of different magnitudes of change. This is not a necessary part of all HRAs, but is extremely helpful in identifying those elements of the system that have relatively large or small effects on system safety.

2.12 Supply Information to System Analysts

A copy of each HRA event tree along with a synopsis of the results, a copy of the task analysis table, and a list of the assumptions made should be presented to the system analysts. They and the human reliability analyst should then go over the HRA event tree and its associated assumptions very carefully. This ensures that the human reliability analyst has correctly defined system success and that the system analysts do not apply the results of the HRA event tree outside the scope of its stated limitations.

3.0 METHODOLOGY

The theory, models, and data presented in this document are taken from the Handbook. Original sources for some of the methods (such as task analysis) can be found there.

The basic components of the HRA described in this document are task analysis and the Technique for Human Error Rate Prediction (THERP). Task analysis involves breaking down system-required human actions (or tasks) into small units of physical or mental performance (steps) as well as identifying to the extent possible likely human actions not required by the system but having the potential for degrading certain system functions. These small units are then fully described and analyzed in terms of the PSFs that affect each of and combinations of them. The performance models and theories from the Handbook are then applied to these steps using the THERP approach. Possible human errors are identified and estimates of the probability of occurrence of each error are derived. The end product of an HRA for a PRA is a set of system success and failure probabilities that reflects the probable effects of human errors. These system-based probabilities are in a form such that they can be entered on a sequence, task performance, or component availability basis on the system fault trees.

For cases in which it is necessary to use expert judgment to derive estimates of the probabilities of human errors in NPPs, there are a number of psychological scaling methods available. For a recent review, see Stillwell et al (1982).[6] Seaver and Stillwell (1983)[7] provide recommendations and procedures for the use of expert judgment to derive estimates of HEPs and performance times in NPP tasks. A review of these two documents is found in Chapter 8 of the Handbook.

4.0 INFORMATION REQUIREMENTS

The PRA team members involved in system analysis should supply the human reliability analysts with system-critical events or components to be evaluated. The human reliability analyst should double-check to ensure that no human events affecting these system-critical events have been overlooked. Procedures for the performances of each of the tasks involved in these events must be evaluated. These procedures can be written, oral, or in the form of

known standard shop practice or skill-of-the-craft. In the case of written procedures, a copy of the procedure itself should be supplied to the human reliability analyst. In the other two cases, the specifics required of the performance must be determined in the course of interviews with and observation of plant personnel.

For the human reliability analyst, familiarity with the plant, especially with the layout of the control room, the characteristics of its test and maintenance activities, the plant environmental conditions, and the plant's general operating standards and administrative controls, is necessary. For the analyst who is not familiar with these aspects of a particular plant, at least one visit (and preferably several) to the site is recommended. Blueprints, drawings, or photographs of the consoles and control boards should be available for later reference. Personnel familiar with all phases of plant operations should be on call to provide information relative to control room specifics and other aspects peculiar to the plant.

A thorough understanding of NPP systems and functions is not necessary for the human reliability analyst--he need not have the same degree of understanding of these systems and functions as other specialists on the PRA team. The human reliability analyst should concern himself only with actual human performance--system causes and effects are not of interest to him except in that they may influence an operator's perception of the urgency of a particular task. The system analysts and plant representatives are chiefly responsible for defining the impacts of human errors on the plant systems and functions. Their close interaction with the human reliability analyst will ensure the correct modeling of the effects of human errors. In quantifying these effects, the underlying assumptions and limitations that apply to the models and data presented in the Handbook must be understood and not contradicted in their applications to PRA.

5.0 PROCEDURE

5.1 Introduction

The purpose of performing an HRA as a part of the PRA described in this document is to determine the contribution of human errors to predetermined significant system failures. The object of such an analysis is to treat the relevant human actions as components in system operation and to identify error probabilities that could significantly affect system status. This section outlines an approach to be used in deriving relevant human error probabilities. Frequent reference to the Handbook will be necessary to increase the consistency of the estimates made and the similarity of the approach utilized.

As stated previously, the HRA should be performed by a human factors specialist who is familiar with the theory and techniques presented in the Handbook. For a complete HRA, he must have an understanding of the plant's administrative control network, some familiarity with the layout and operating characteristics of the control room, and frequent access to plant personnel who can provide information on specific aspects of performance situations. Without sufficient plant-specific information, he will be unable to perform an HRA that models the actual plant situation adequately in that he will not have defined all the potential human errors nor will he have accounted for all the likely recovery factors.

In this section, each of the major tasks of an HRA (outlined in Section 2.0, Overview) is discussed. An example of an HRA is presented in tandem with these discussions. For each task described, an example of its application to an actual HRA is given.

There are several possible sequences for the elements of an HRA. The sequence outlined in this procedure is by no means absolute, but it does reflect an order that served well for the IREP and other programs. The elements themselves were derived from THERP and should be included in all complete HRAs. The recording and reporting formats described in this document can be modified for the convenience of the analyst, but he should keep in mind the type and level of detail of information necessary for reference to his analysis. The HRA can be used for qualitative as well as quantitative assessments, with the level of detail of the information collected reflecting that of the analysis itself. The state-of-the-art of HRA is such that it depends largely on data sources that are extrapolations from tasks not directly related to NPPs and on models that have not been validated in the strictest sense of the word. Nevertheless, this application of the theory, data, and models presented in the Handbook represents an attempt at standardizing the approach to applying HRA to PRAs of NPPs.

5.2 Plant Visit

5.2.1 Discussion

At least one plant visit specifically including a detailed survey of the control room should be made at the onset of an HRA. Arrangements with the plant as to the areas of the facility to be visited, the plant's requirements for access, and the types of personnel to be made available for interviews during the visit need to be made. Impact on the plant and on the utility should be minimized. As little disruption of plant operations as is possible should be effected.

When possible, a meeting between the human reliability analyst and representatives of the plant and/or utility should be held in advance of the actual plant visit. The purpose of this visit is to assure the plant and utility representatives that the purpose of this portion of the PRA is not a regulatory one. More cooperation at all levels of involvement will be afforded if the concerned parties do not see the role of the human reliability analysts as a condemnatory or judgmental one. The main purpose of the visit should be stressed: plant conditions are to be observed so that in the analysis accurate descriptions of actual performance can be predicted. These observations are to be only descriptive in nature. No "solutions" to plant problems or inadequacies are to be offered. (If the PRA is performed by or for the utility, it can be used as a design or evaluative tool. In such a case, the information from the HRA can be used to recommend changes to layout, procedures, or administrative control. PRA provides a powerful input to the plant's analysis of its own operating efficiency and safety through the employment of sensitivity analysis. However, when the PRA is performed for government agencies such as NRC, the information collected will be relevant to the operating plant in most cases, and not usually to the safety implication of proposed changes.)

In this section, each of the major tasks of an HRA (outlined in Section 2.0, Overview) is discussed. An example of an HRA is presented in tandem with these discussions. For each task described, an example of its application to an actual HRA is given.

There are several possible sequences for the elements of an HRA. The sequence outlined in this procedure is by no means absolute, but it does reflect an order that served well for the IREP and other programs. The elements themselves were derived from THERP and should be included in all complete HRAs. The recording and reporting formats described in this document can be modified for the convenience of the analyst, but he should keep in mind the type and level of detail of information necessary for reference to his analysis. The HRA can be used for qualitative as well as quantitative assessments, with the level of detail of the information collected reflecting that of the analysis itself. The state-of-the-art of HRA is such that it depends largely on data sources that are extrapolations from tasks not directly related to NPPs and on models that have not been validated in the strictest sense of the word. Nevertheless, this application of the theory, data, and models presented in the Handbook represents an attempt at standardizing the approach to applying HRA to PRAs of NPPs.

5.2 Plant Visit

5.2.1 Discussion

At least one plant visit specifically including a detailed survey of the control room should be made at the onset of an HRA. Arrangements with the plant as to the areas of the facility to be visited, the plant's requirements for access, and the types of personnel to be made available for interviews during the visit need to be made. Impact on the plant and on the utility should be minimized. As little disruption of plant operations as is possible should be effected.

When possible, a meeting between the human reliability analyst and representatives of the plant and/or utility should be held in advance of the actual plant visit. The purpose of this visit is to assure the plant and utility representatives that the purpose of this portion of the PRA is not a regulatory one. More cooperation at all levels of involvement will be afforded if the concerned parties do not see the role of the human reliability analysts as a condemnatory or judgmental one. The main purpose of the visit should be stressed: plant conditions are to be observed so that in the analysis accurate descriptions of actual performance can be predicted. These observations are to be only descriptive in nature. No "solutions" to plant problems or inadequacies are to be offered. (If the PRA is performed by or for the utility, it can be used as a design or evaluative tool. In such a case, the information from the HRA can be used to recommend changes to layout, procedures, or administrative control. PRA provides a powerful input to the plant's analysis of its own operating efficiency and safety through the employment of sensitivity analysis. However, when the PRA is performed for government agencies such as NRC, the information collected will be relevant to the operating plant in most cases, and not usually to the safety implication of proposed changes.)

In the initial visit to the plant, the human reliability analysts will make notes on relevant PSFs, especially those dealing with the control room operations and the paperwork associated with equipment change and restoration activities. If the system analysts have already indicated plant subsystems or procedures that are of interest in the PRA, these can be examined closely at this time. General information about the plant's operating characteristics and a "feel" for the effectiveness of the plant's administrative control system are to be derived from this visit.

An evaluation of the various kinds of written procedures (maintenance, calibration, emergency, etc.) related to critical tasks for the PRA should be performed, using available checklists, e.g., Brune and Weinstein (1982, 1983)[8,9] and INPO.[10] If the written material at a plant deviates from the good practices specified in these checklists, the analyst may adjust the nominal HEPs from the Handbook accordingly.

In surveying the control room, note specifics relating to the layout of controls and displays. Take copious notes on the characteristics of critical controls and displays, noting any factors that would influence their use--anything that would aid or hinder the operators in either locating, manipulating, or interpreting them. Deviations from good human factors engineering practices, such as those noted in MIL STD-1472C[4] and NUREG-0700,[5] should be noted. Record any specifics relative to the operation of critical subsystems that have been pinpointed for observation by the system analysts. If they have already identified any plant procedure that will be examined, use the time at the plant to perform a talk-through of that procedure (see Section 5.4).

5.2.2 Example

Following is a set of notes similar to the type that would be collected during an actual plant visit.

- On some chart recorders, the indications are hazy because nonglare glass is used. The operations superintendent says they are all being changed to regular glass. (The nonglare glass was installed on a recommendation from the manufacturer.)
- Some labels for two-channel switches are sideways because of space restrictions. (Later note: When these sideways labels appear between displays, some confusion in relating a label to a display may result.)
- Each annunciator panel is numbered, with the numbers increasing from right to left rather than the conventional left to right (so do the numbers for control boards and panels).
- On the fronts of control boards CB1 and CB2, there are rows of J-handle switches, the first of which are turned inward to prevent their inadvertent manipulation. This is not true for CB4, but the J-handle switches there are not critical to plant operation. Those on CB1 and CB2 are for oil pumps and turbines, movement of which during normal power generation would cause a trip. The direction of manipulation for the reversed J-handles is the same as for the outward-facing ones.
- Some J-handles have arrows at their bases that indicate the direction of operation, some do not (note: different manufacturers?). Other-shape handles have arrows at their bases, especially round knurled or symmetrical handles. The size of these shape-coded handles is such

that the arrows cannot be seen easily, especially when viewed at eye level straight on.

- At the alarm cathode-ray tube (CRT), there are three display modes: a flashing dark green display indicates a new, unacknowledged alarm; a steady dark green display indicates an uncorrected but acknowledged alarm; and a steady light green display indicates a cleared alarm (it remains on for reference only).
- For the engineered safety feature (ESF) panels in the cabinets in the back (as well as other indications in the control room), display status and some parameter readings must be recorded at various intervals of time. (Note: Need to request a copy of "Procedures for Conducting Plant Operations" to review the checklist used versus the frequency of its use and the locations of all controls checked.)
- On the ESF panels in the control room, the color of the label for a particular item is the color of the indicator light during actuation of the automatic safety equipment. During system response to an emergency, the operator can scan the ESF panel quickly to see whether the lights that are on are the same color as the labels for those items. A disagreement between the colors indicates that some safety system has malfunctioned or has been overridden manually for some reason.
- Stubs from yellow tags for valve change operations are tossed into a drawer; no record of them is in evidence. (Note: Check this out.)
- The labels on locally operated valves are impression-printed on metal tags and, due to poor lighting, are difficult to read. No indication is present at these valves that designates their normal positions.
- The procedures for responding to a LOCA often have many actions per numbered step. (Note: Check the Complexity Index and Specificity Index using NUREG/CR-2005.[9])

Obviously, there are other observations that could be made during a survey, but they have been omitted here simply for the sake of brevity. The levels of detail of the control room survey and the inspection tour of the plant are at the discretion of the human reliability analyst and should reflect the level of detail required by the PRA being performed. Specific information relating to the conduct of certain procedures identified later in the program can be supplied by plant personnel during a talk-through, with the human reliability analyst interpreting that information in the light of knowledge gained during the plant visit.

5.3 Review Information from System Analysts

5.3.1 Discussion

The system analysts will have identified a set of scenarios to be analyzed. These will usually take the form of operator performance on a critical system element during the course of following a set of plant procedures. The system analysts will have identified system-critical components and the circumstances under which they will be manipulated. The human reliability analysts must then determine the probability that errors will be made in dealing with these components. They must also determine whether human performance on other elements or in the conduct of the plant's administrative control system will affect the probability of error in operating the system-critical components.

Often, the system analysts will present the human reliability analysts with a set of plant procedures from which they have pinpointed the steps that they

feel deal directly with the operation of system-critical components. In other cases, they may have identified entire systems for which human errors must be identified and quantified. In either case, the human reliability analysts must examine the entire set of plant procedures associated with these elements to determine whether they involve required performances on other elements that might affect the probability of error on the critical components or systems. At times, these determinations will have to be made in conjunction with the performances of the talk-throughs of the sets of procedures (see Section 5.4).

During this review of the information received, the critical task required of the human reliability analyst is that he ensure that all human performance is analyzed in the context of its actual performance. Human actions in an NPP should not be considered isolated entities, unaffected by other factors. There are many interactions in an NPP--between personnel and between tasks--that must be identified. Some of these interactions will affect the assessment of levels of dependence between certain behaviors (see Section 5.9). Some of them will have a global effect on the performance of all tasks in a given procedure. The system analysts will have identified the interfaces between critical equipment items and associated human tasks. However, the identification of the interactions between these and other system elements should be made by the human reliability analyst, who has been trained to spot them. This extra investigative effort on the part of the human reliability analyst ensures that the better part of them are identified.

Note that, in some cases, a single plant procedure will cover the performance of several sets of tasks involving critical components. For example, in restoring items of equipment after maintenance acts, the operators may follow a general plant procedure governing the application and removal of tags. This administrative control procedure may apply to all cases in which tags are used. In this case, it is the following of the administrative control procedure that is analyzed as well as the restoration act per se. The operator is actually following the administrative control procedure rather than a set restoration procedure for a specific component. Here the human reliability analyst can examine one procedure (the administrative control procedure) and apply the results to all cases involving restoration after maintenance. He must take care, however, to determine that the administrative control procedure applies to every case he analyzes.

As he reviews the information received from the system analysts, the human reliability analyst should search for deviations from or inconsistencies with respect to the assumptions of the theories and models in the Handbook. The HEP estimates in Chapter 20 of the Handbook are based on limitations on their use that must not be contradicted. The human reliability analyst must examine a given procedure in the context of its performance to assess its conformance to these limitations.

5.3.2 Example

A set of hypothetical plant procedures dealing with response to a small loss-of-coolant accident (LOCA) is reproduced in Figure 3. Only part of the procedure has been reproduced, and the steps identified by the system analysts as being critical are double-asterisked. In this case, the system analysts have made the assumption that the situation has been diagnosed correctly and that the operators have completed the immediate actions required by the situation

D. SUBSEQUENT ACTIVITIES

Note: Reverify asterisked parameters in all sections, using alternative indications if available. Select proper computer functions to monitor incore thermocouples.

*If FW and RCPs are available (manual HPI actuation, no automatic actuation), proceed through Section D.
*If no FW is available, proceed to Section E.
*If FW is available but RCPs are not, proceed to Section F.

D.1 Stop all but one RCP in each loop.

Note: If ES actuation occurs before HPI can be manually established and the RCS pressure recovers, do not reset ES analog channels, since this would delay restart of actuated equipment in the event of a loss of offsite power as pressure would have to fall again to the actuation setpoint.

**D.2 Monitor RCS pressures and temperatures; maintain at least 50°F margin to saturation by holding RCS pressure near the maximum allowable pressure within the cooldown pressure-temperature curve (Figure B).

Note: If RCS pressure is not restored before the pressurizer goes solid, or if the RCS relief valve alarm remains in, the leak may be in the pressurizer steam space, and the pressurizer must be taken solid to regain RCS pressure. If such is the case, reopen ERV block valve MOV-1300 to allow ERV operation before pressurizer code safeties.

**Caution: HPI components are not to be overridden unless the following criteria are met:

1. The HPI system has been in operation for 20 min, and all hot- and cold-leg temperatures are at least 50°F below saturation temperature for the existing RCS pressure, or

2. The RCS is >50°F subcooled, and throttling of HPI is necessary or

3. The RCS is 50°F subcooled, and HPI throttling is necessary to remain within the plant cooldown pressure-temperature curve limits, or

4. DH or LPI has been operating for >20 min with total flow rates of ≥2000 gpm.

If margin to saturation drops below 50°F after HPI override, reinitiate maximum HPI until >50°F subcooled. UNDER NO CIRCUMSTANCES IS HPI TO BE OVERRIDDEN IF RCS IS NOT SUBCOOLED.

D.3 Monitor RB pressure; if pressure reaches 4 psig, verify reactor building isolation and cooling actuation (ES channels 5 & 6) and HPI & LPI actuation (channels 1, 2, 3, and 4).

Note: Proper ES actuation is verified by noting that the colors of components' indicating lamps on the ES panels ES-16 and ES-18 and CB-26 correspond to the colors of the switch nameplates. Proper flow ranges for HPI, LPI, and RB spray are marked on the meter faces. Proper penetration room ventilation is verified by noting all room isolation damper lights out, flow indicated, and negative penetration room pressure indicated....

**D.4 If RCPs and FW are available, and RCS margin to saturation is >50°F, override and throttle HPI MOVs to control system pressure if pressurizer is solid or to hold pressurizer level at setpoint while using pressurizer heaters and spray for RCS pressure control; initiate plant cooldown per Plant Procedure 12 at a rate that allows RCS pressure to be maintained within the cooldown pressure-temperature envelope.

D.5 If RCS pressure falls to within 50°F of saturation or if low margin to saturation temperature alarms are received, maintain maximum HPI flow until 50°F margin is restored.

D.6 If RCS pressure falls below secondary pressure, reduce and maintain secondary pressure at 20 lb/in. less than primary pressure and maintain maximum HPI flow until subcooled, then initiate a cooldown by decreasing secondary pressure per Plant Procedure 23.

Figure 3 Part of the procedures for responding to a small LOCA, with the critical steps double-asterisked (**) p. 1 of 2.

**D.7 Prepare for LPI boost to MU pump suction and RB sump recirc as follows:

D.7.1 Verify MU tank outlet MU-13 closed.

D.7.2 Open DH-7A and DH-7B, LPI discharge to MU pumps suction, verify MU pump suction crossover valves MU-14, MU-15, MU-16, and MU-17 open, and verify MU pump discharge crossover valves MU-23, MU-24, MU-25, and MU-26 open.

D.7.3 Isolate the DH rooms by closing both DH room floor drain valves, ABS-13 and ABS-14, securing room purge dampers CV-7621, CV-7622, CV-7637, and CV-7638 from ventilation control panel (east wall of 404-foot ventilation room) and closing watertight doors.

D.7.4 Verify both DH pumps operating and both LPI MOVs open (MOV-1400 and MOV-1401).

D.8 Once a 50°F margin to saturation is attained.....

**D.9 Monitor BWST level; when BWST level has fallen to 6-foot indicated level or when the corresponding BWST lo-lo-level alarm is received, transfer suction to RB sump by verifying RB sump suction valves inside containment MOV-1414 and MOV-1415 open, opening RB sump suction valves outside containment MOV-1405 and MOV-1406 (a slight upward perturbation should be noted on pump flows indicating suction transfer) then close both BWST outlets MOV-1407 and MOV-1408 (refer to Plant Procedure 23 for RCS temperature control methods). Close NaOH tank outlets MOV-1616 and MOV-1617. MANUAL OVERRIDE PUSHBUTTONS MUST BE DEPRESSED FOR ALL VALVE MANIPULATIONS IF ES ACTUATION HAS OCCURRED.

Figure 3 (cont'd.) p. 2 of 2.

correctly. These assumptions limit the nature of the HRA since, given them, the human reliability analyst does not have to account for errors of diagnosis or for the fact that the operators' level of stress might be higher due to their having made mistakes in the immediate actions. However, those systems that have been judged to have the potential of being degraded by human errors are those involved in the "SUBSEQUENT ACTIVITIES" section of the procedure. These, therefore, are the only ones to be considered in this example. (The treatment of diagnosis errors will be discussed in a later section.)

Given the above assumptions and following a detailed reading of the procedures, everything seems to be in order for a straightforward use of the theories and models in the Handbook, with one exception: the performance of these tasks takes place about an hour after the onset of the small LOCA. Chapter 18, "Staffing and Skill Levels," in the Handbook states that there will be three reactor operators and a shift technical advisor in the control room at this time. In this example, for simplicity we assume that the shift technical advisor has aided in the initial diagnosis, but now he has no involvement in the procedure to be carried out by the operators. We will also make the very conservative assumption those actions required by the procedure which take place outside the control room must be performed by one of the licensed reactor operators, leaving only two qualified operators in the control room. Often such activities may be performed by auxiliary operators with no reduction in the number of qualified reactor operators in the control room. Furthermore, during an incident of this type, there will probably in actual fact be several people in the control room. However, the shift supervisor is still in charge of operations, and personnel working for him are likely to follow his instructions and line of thought. Therefore, we conservatively assume that the net effect of having several people present during response to a transient would be no more beneficial than that afforded by the presence of only three licensed operators.

5.4 Talk- or Walk-Through

5.4.1 Discussion

In a talk-through of a set of procedures for which safety-critical events have been identified, the human reliability analyst questions someone familiar with the performance of that procedure on specific points of the procedure until the analyst is so familiar with the tasks that he could perform them himself or at least be able to understand fully the performance of an operator. The talk-through can be performed on sets of written or oral plant procedures or standard shop practice or training methods. (These talk-throughs could take place at a simulator facility instead of at the plant itself, but, in these cases, the human reliability analyst must take great care in noting which of the characteristics of the simulator are unlike those to be found at the plant.) During the talk-through, the human reliability analyst must determine the PSFs that influence behavior, such as the location and the physical and operating characteristics of specific controls, the type and location of alarms and annunciated indicators, control room manning and task allocation, and time requirements and limits for alarm indications and responses. He must also "translate" the written procedures into English as he speaks it. That is, he is to determine the meaning or the specific instruction resulting from each command that is given in the language of that particular plant in the set of procedures. The analyst must specify in language he can understand the

exact interpretation the operators will make from the sometimes vague wording of plant procedures. At times, these interpretations are based on the operator's knowledge of system operation rather than on a standardized plant definition of the term in question. When this is the case, the human reliability analyst must discover whether all the operators define that term in the same way.

To perform a talk-through, the human reliability analyst conducts an interview with a plant employee who is familiar with the performance of the procedure in question. (In the case of a new plant, the person most familiar with the development of the procedures should be interviewed.) To afford himself more familiarity with the performance characteristics of the procedure, the human reliability analyst should ask general questions about the PSFs acting at the time of performance and specific questions about the PSFs affecting the performance of the critical steps.

A talk-through of control room operations can be performed as part of the survey of the control room. In this case, the operator and the analyst actually follow the path taken by the operators during the performance of the procedure. When the procedures call for the manipulation of a specific control or for the monitoring of a specific set of displays, the operator and the analyst approach them at the control panels, and the operator points out the controls and displays in question. The procedure is followed in sequence, and the analyst could generate a link analysis at this time. (Link analysis is discussed in Chapter 4 of the Handbook.)

Careful notes chronicling the outcome of the talk-through must be taken. Much of the information from these activities will be entered directly into the task analysis tables (see Section 5.5) for use later in the analysis.

5.4.2 Example

In the talk-through of the procedures in Figure 3, some general information was gathered that relates to the performance of all the steps in the procedure. They are listed below.

1. The plant is following an emergency procedure. (Note for later reference: There will be some level of stress for the operators.)
2. The SUBSEQUENT ACTIVITIES section of the procedures will be performed approximately 1 to 1-1/2 hours after the initiation of the transient.
3. At least three licensed operators will be available to deal with the situation. One of them will be the shift supervisor.
4. At this plant, "verify" means to check and, if necessary, to correct the status of a given item of equipment. For example, if the operator must verify that a valve is open and on checking its status finds it closed, he must open it manually.
5. The asterisked notation at the beginning of the section indicates that completion of the items in Section D is to be reverified (double-checked) after the section has been completed. This constitutes a recovery factor and, as such, will not be included in the HRA event tree at this time.
6. The Caution following Step D.2 in Figure 3 resulted from actions taken during the incident at Three Mile Island II in March 1979. Because of the special implications of performing these actions incorrectly, they will be considered in a separate analysis.

7. Steps D.2, D.4, D.9, and D.7.4 are performed in the control room. They will be diagrammed separately from steps D.7.1, D.7.2, and D.7.3, which take place outside the control room.

Specifics relating to the performance of individual steps will now be given in the order of the steps themselves.

Step D.2 -- RCS pressures are found on a chart recorder; RCS temperatures can be read from digital indicators; both are on a front control board. A copy of the pressure-temperature curve is taped to the side of the computer terminal, adjacent to these other indicators. To manipulate the pressure and temperature values, the heater switches found on the same front control board will be used.

Step D.4 -- Switches for four HPI MOVs are located on the vertical ESF panels. A sketch of the layout of the controls is shown in Figure 4. Cooldown is initiated by following another procedure. The operator says that this other procedure is so well known that he cannot think of any situation in which it would actually be necessary to refer to it.

Step D.7 --

D.7.1 -- MU-13 is a manual valve located in the stairwell outside the MU Pump Room. This is two levels down from the control room.

D.7.2 -- The layout of these valves is shown in Figure 5, with the channels they represent indicated. One channel should always be completely open so that the operator should only have to open one LPI discharge valve, two MU pump suction crossover valves, and two MU pump discharge crossover valves. The operators view this entire series of tasks as one unit task--in their interpretation, all these steps are performed to satisfy a major system function. These valves are located one level below the MU Pump Room.

D.7.3 -- ABS-13 and ABS-14 are large, locally operated valves located outside the DH rooms, one level below the DH pump rooms. They are large valves situated under the grating outside the watertight doors. There are no other valves under the grating. The Ventilation Room is two levels above the control room. The switches for CV-7621, 22, 37, and 38 are located on the wall there in the midst of dozens of other similar switches. They are grouped near each other and near other switches that control equipment in the same physical area of the plant, but there are no location cues on the wall to indicate where this grouping can be found among other groups.

D.7.4 -- Indicator lamps for the DH pumps and for the LPI MOVs are on the vertical ESF panels in the control room. See Figure 4 for the layout of the panels.

Step D.9 -- The level indicator, an analog meter, is on a panel adjacent to the vertical ESF panels in the control room. The lo-lo-level alarm sounds when the 6-foot level is reached. During a small LOCA, this should happen no sooner than 1-1/2 hours after initiation of the event. All the MOV switches are on the ESF panels.

5.5 Task Analysis

5.5.1 Discussion

At this point, a formal breakdown of the procedure into tasks or smaller units of behavior should be done; that is, for each step in the procedure that was

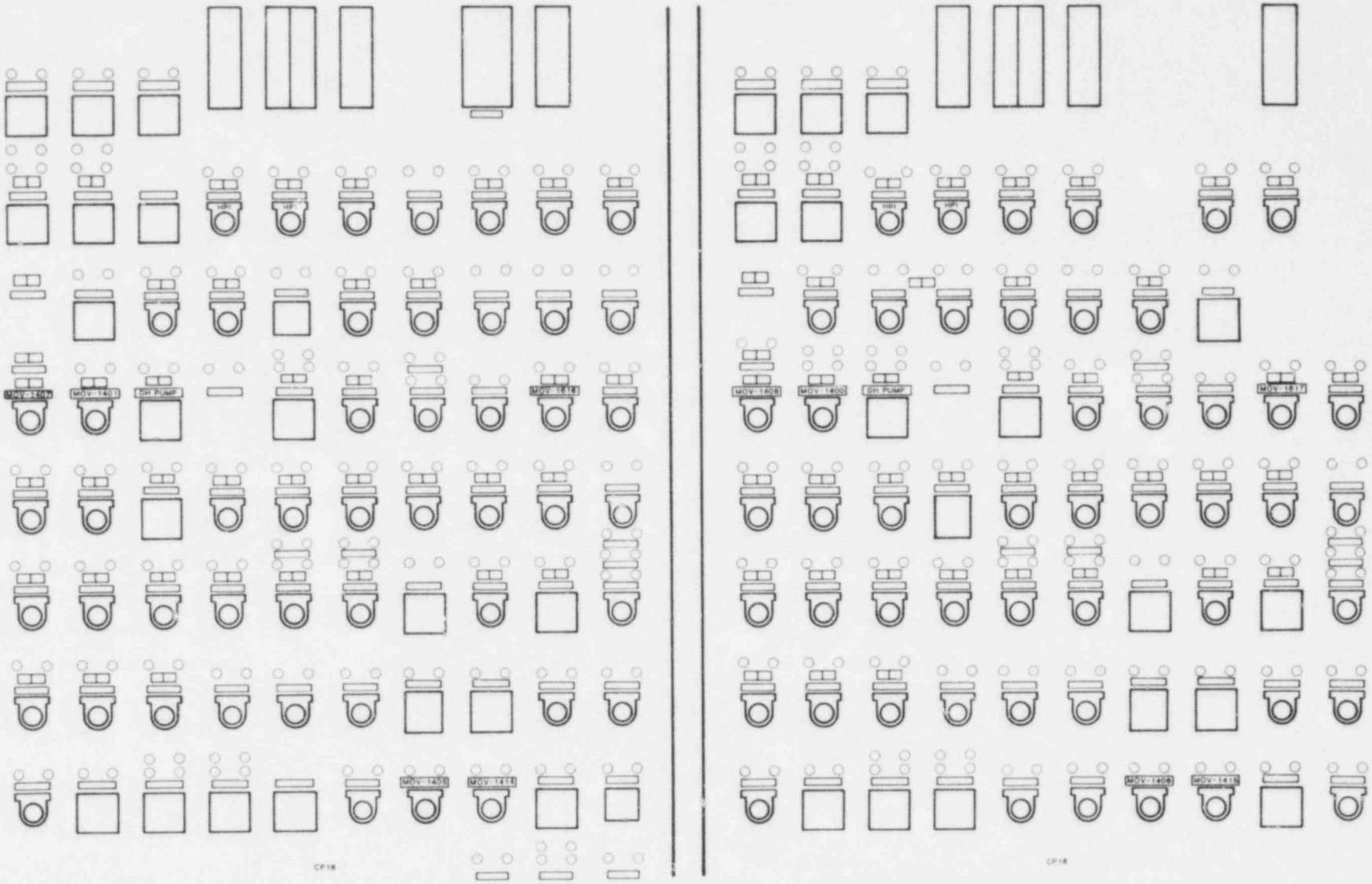


Figure 4 Layout of controls on the ESF panels CP16 and CP18.

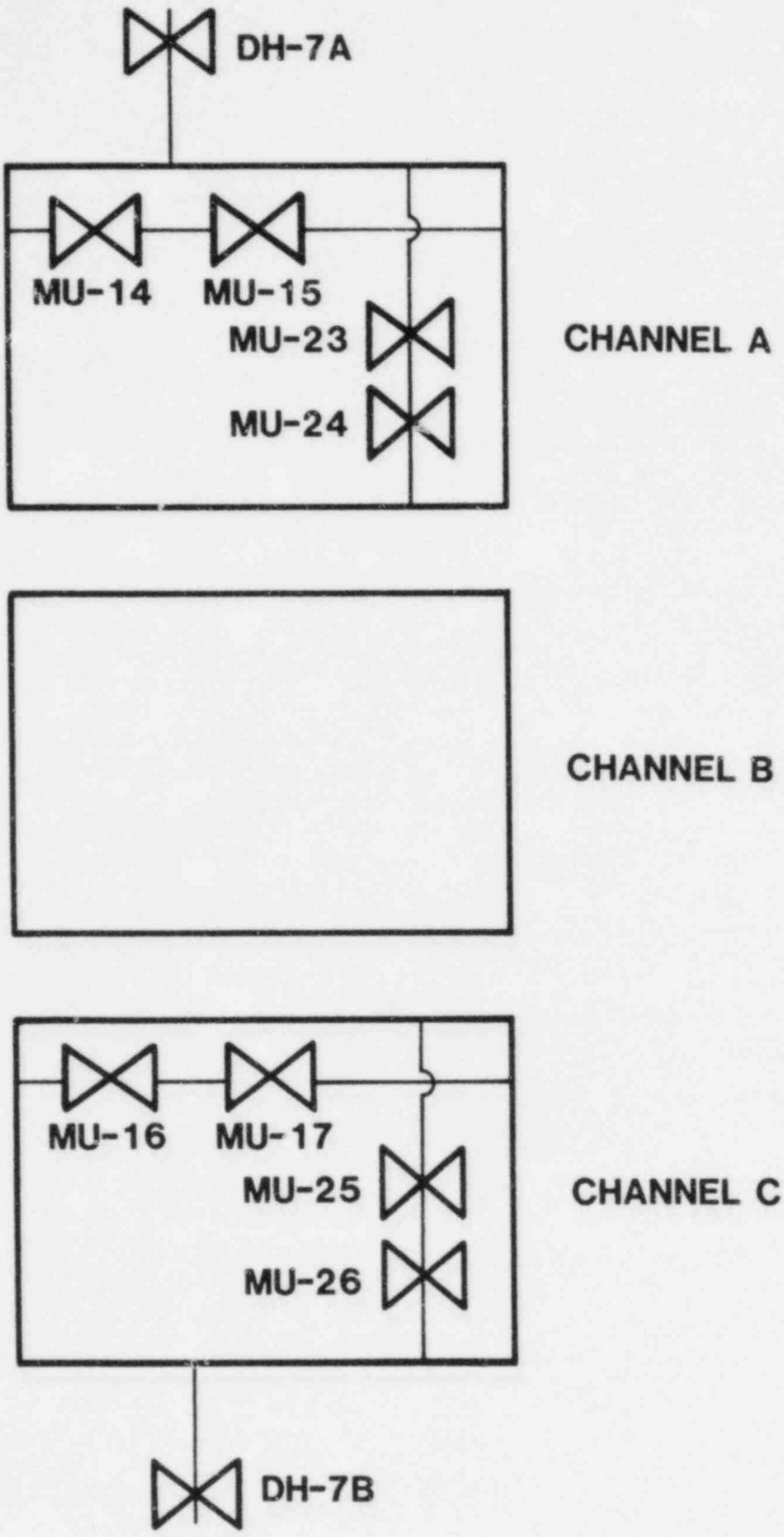


Figure 5 Layout of valves in DH pump rooms.

identified for analysis by the system analysts, individual units of operator performance must be identified, along with other information germane to these performances. These individual units of performance constitute elements of behavior for which potential errors can be identified. In other words, a large task made up of a set of steps should be broken down in order that errors associated with each step might be identified. All of this information must then be entered into a task analysis table. The format of this table is not specified other than that it contain all the information necessary to later parts of the analysis. In most cases, the necessary information will consist of such items as the piece of equipment on which an action is performed, the action required of the operator, the limits of his performance, the locations of the controls and displays, and explanatory notes. If different tasks are to be performed by different operators, the allocation of tasks to personnel can be indicated in the task analysis table, or separate task analysis tables can be made for each operator. Our example illustrates the latter approach. The level of detail necessary in a task analysis and the amount of information recorded should reflect the level of detail (qualitative or quantitative) of the PRA and are obviously determined judgmentally. The guiding rule for this determination is that one should be able at a later date (perhaps when the results of the HRA are compared to those from another analysis) to recapitulate the rationale for the HEP estimates that were used in the analysis.

Once the breakdown of task steps has been done, errors likely to be made must be identified for each step. The determination of whether an error of omission should be considered for any given step or of the types of errors of commission (selection, reversal, sequence, etc.) that are likely for that step must be made based on the relevant PSFs and on the task analysis itself. The steps should be listed chronologically.* Based on the characteristics of the actual performance situation, the human reliability analyst must determine and record which types of errors the operator is likely to make and which he is not. For example, if an operator is directed by a set of written procedures to manipulate a valve and that valve is fairly well isolated on the panel, is of a different shape than other valves on the same panel, and has been very well labeled, the human reliability analyst may determine that errors of selection are not to be considered in this case. He should also have determined that an error of omission made in following the written procedures might be made.

Extreme care should be exercised in deciding which errors, if any, are to be completely discounted for an analysis. Relative to those encountered in analyses of tasks in other industries, most of the HEPs associated with NPP tasks are very low, on the order of 10^{-3}. Although one error in a thousand opportunities seems quite low, a 10^{-3} human error probability may contribute

---

*In some cases, it may be discovered that the order of the steps in the procedure is not necessarily the one followed by the operators. The task analysis and the HRA event tree resulting from it can easily reflect any performance sequence. However, in the absence of any indications to the contrary, the order of the steps in the procedure is usually assumed to be the most likely order of performance of the tasks. Record-keeping is simplified by following the same task sequence from procedures to task analysis to HRA event tree.

substantially to the probability of system failure. Rather than failing to consider a "questionable" error, one the human reliability analyst thinks may be unlikely, the analysis should be completed including it, then a sensitivity analysis should be performed to ascertain what impact that particular error has on the probability of system success (see Section 5.12). If its impact is determined to be negligible, an indication of this can be made in the fault tree block for this error.

Once the errors likely to be made on each unit of performance have been identified, the analyst must examine the situation for other factors that may influence performance. The entire performance scenario must be considered in this examination. The analyst is looking for elements taking place usually outside the scope of the procedures the operator is following that could influence his performance. For example, if something is to be done at the discretion of the shift supervisor, whether the supervisor remembers to order the task will have a definite effect on whether the operator performs the task. These factors extraneous to the procedure itself that affect the probability of human error often involve some sort of failure of the plant's administrative control system. The quality and the potential (during a particular performance sequence) for disruption of the plant's personnel communication system will also have to be examined in these cases.

Events other than human actions that, on occurring, affect subsequent performance must also be taken into account. If an operator's cue to initiate a task involves some signal from the equipment or an order from a supervisor, the probability of that signal's being generated or that order's being given must be considered. Many times, the equipment failure probabilities are provided by the system analysts or are not considered for the analysis based on the assumptions that the system analysts provided. Such an assumption about the supervisor's order (that it will always be given when it should) should not be made unless direct evidence supports it.

The human reliability analyst usually designs and performs the task analysis to agree with the level of incorporation of the HRA into the system analysis that has been dictated by the system analysts. Whether the results of the HRA are to be included in the system event trees, at a high (subsystem) level of the system fault trees, or at a low (component unavailability) level of the system fault trees has no effect on the actual performance of the HRA other than in the formatting of the results. All tasks are to be analyzed in the contexts of their performances. Whether the information relative to these performances is considered in part or as a whole in another section of the PRA is of little consequence to the human reliability analyst. The results of his analysis can be presented so that they can be parceled into smaller collections of information for inclusion at the component level in the system fault trees or taken as a whole for inclusion at the subsystem level. The format used in the example can accommodate either.

5.5.2 Example

The task analysis for the procedures in Figure 3 has been done in two sections. First, the tasks performed by the operators assigned to the control room have been examined, then those performed outside the control room.

The table format used for this example is shown in Figures 6 and 7. In Figure 6, dashed lines are drawn between sets of actions that apply to specific plant

STEP	EQUIPMENT	ACTION	INDICATION	LOCATION	NOTES	ERRORS	EVENT TREE*
D.2	RCS pressure	Monitor		CB4		Omission (all)	1
						reading	2
	RCS temperature	Monitor		CB4		Reading	3
	heater switches	Maintain pres. & temp.	Within curve on chart	CB4		Reading	4
D.4	4 HPI MOVs	Override & throttle		CP16, CP18	ESF	Omission (all)	5
						selection (1)	6
		Initiate cooldown	Plant procedure 12			Omission	7
D.7.3	CV-7621,22,37,38 (room purge dampers)	Secure	Close switches	Ventilation Room		Omission (all)	8
						selection (each)	9,10,11,12
D.7.4	DH pumps	Verify on	Indicator lamps	CP16, CP18	ESF	Omission (for MOVs too)	13
						selection	14
						interpretation	15
	MOV-1400, 1401	Verify open	Indicator lamps	CP16, CP18	ESF	Selection	16
						interpretation	17
D.9	BWST	Monitor	>6 feet	CP14		Omission	18
						reading	19
	MOV-1414, 1415	Verify open	Indicator lamps	CP16, CP18	ESF	Selection	20
						interpretation	21
	MOV-1405, 1406	Open	MOV switches	CP16, CP18	ESF	Selection	22
						reversal	23
	MOV-1407, 1408	Close	Switches	CP16, CP18	ESF	Selection	24
						reversal	25
	MOV-1616, 1617	Close	Switches	CP16, CP18	ESF	Selection	26
						reversal	27

*The numbers in this column do not usually appear in a task analysis; they have been included for the reader's convenience. They refer to the error event numbers appearing in HRA event trees starting with Figure 9.

Figure 6 Task analysis table for actions by operators assigned to the control room.

STEP	EQUIPMENT	ACTION	INDICATION	LOCATION	NOTES	ERRORS	EVENT TREE*
D.7.1	MU-13	Verify closed	Position	Stairwell Outside MU Pump Room	Only valve	Omission	2
D.7.2	DH-7A, 7B	Open	Position	Outside DH Pump Rooms		Omission (for all D.7.2)	3
	MU-14, 15, 16, & 17	Verify open	Position	DH Pump Rooms			
	MU-23, 24, 25 & 26	Verify open	Position	DH Pump Rooms			
D.7.3	ABS-13, 14	Close	Position	Outside DH Room	Only valve	Omission (for all D.7.3 here)	4
	Watertight doors	Close	Locks in place	DH Rooms			

*The numbers in this column do not usually appear in a task analysis; they have been included for the reader's convenience.

Figure 7 Task analysis table for actions by operator outside control room.

functions. This is done to enable the system analysts to keep track during the course of the analysis of which portion of the HRA event tree should be excerpted for insertion at the subsystem level of the system fault trees. In this case, step D.2 involves the operator's diagnosis of plant status. This step should be excerpted for inclusion with all others since its correct performance affects the probability of correct performance on the rest of the steps. Once this diagnosis has been made correctly, the operator will move to effect cooldown after verifying that saturation is adequate per step D.4. Step D.7.3 involves isolating the DH room. Step D.7.4 calls for the operator's verifying the initiation of the DH function. Then, he must diagnose the need for the establishment of recirculation based on the indication of the BWST level. This involves the first part of step D.9 (monitoring the BWST), and must be excerpted along with any of the other errors from step D.9 (effecting recirculation) for inclusion in the system analysis of the recirculation system.

In actual HRAs, the format used for the task analysis is relatively unimportant; it can be modified to reflect the type and amount of information needed in later phases of the PRA. The STEP number from the written procedures is included for easy reference back to the procedures should any questions arise. The actual items of equipment to be manipulated, read, or otherwise dealt with are listed in the EQUIPMENT column. The ACTION column contains the commands made to the operator; they are usually the action verbs contained in the procedure. In the INDICATION column, the analyst notes the cues (usually from visual displays) that inform the operator whether the action has been performed correctly and of any restrictions on the operator actions. In the example task analyses in Figures 6 and 7, many of the indications are so obvious (e.g., turn switch to ON position) that no entry has been made. The physical positions of the equipment items are given in the LOCATION column. The NOTES column contains any information the human reliability analyst believes will be beneficial in later parts of the analysis. In these cases, we have indicated whether the equipment items of interest in the control room are on the ESF panel and whether locally operated valves are isolated or part of a group. The ERRORS column lists the errors determined likely for each task. They are discussed for each step in detail below, beginning with those in Figure 6.

Step D.2 -- Monitoring and maintaining RCS pressure and temperature within the curve is considered to be a unit task made up of three steps: (1) reading the pressure chart, (2) reading the temperature from the digital indicator, and (3) manipulating the heater switches to keep the above values within the acceptable range on the pressure-temperature curve. As such, the probability of an error of omission applies to the entire task--only by forgetting to perform the task itself will the operator forget to perform any element of it. The possible commission errors are those made in reading the pressure from its chart recorder, the temperature from its digital readout, and the curve which is in the form of a graph. The feedback from manipulating the heater switches is almost immediate, so the probability of making an unrecovered reversal error in their operation is not considered likely. All of these equipment items are located on one of the front control boards, with the exception of a graph of the pressure-temperature curve which hangs off the CRT console immediately adjacent. This unit task is performed very often during normal and emergency operating conditions. The equipment items are functionally grouped and well labeled. Under these circumstances, errors of selection were not

considered. These steps are considered dynamic tasks in that they involve continuous monitoring of the displays and repeated operation of the heater switches.

Step D.4 -- Because their manipulations are called out in the same procedural step and because of their close proximity (see Figure 4), the operator views the throttling of the four HPI MOVs as a single task. Therefore, the probability of an error of omission applies to them all as a unit. Because on the actual panel they are delineated with colored tape, a selection error for the group is very unlikely. However, as Figure 4 shows, a similar switch is next to the last HPI MOV control in the group. A selection error for that control is likely--instead of MOVs 1, 2, 3, and 4, the operator may throttle MOVs 2, 3, and 4 and the other control. In initiating cooldown, the operators have stated that they probably would not refer to the other set of procedures. For this reason, an error of omission is assigned to the entire task of performing that other procedure.

Step D.7.3 -- We have assumed that at this time there are three licensed operators available to deal with the transient. One of them is performing the activities shown in Figure 7. Of the two remaining in the control room, one will have to go two levels above the control room to secure the DH room purge dampers (close the switches). If he goes to perform this task, he will manipulate four MOV switches--we have said that an error of omission applies to the manipulation of all four switches because they are on the same procedural step. Because of the poor layout of the Ventilation Room (no cues are provided as to the location of functional groups), selection errors for each of the four switches are assigned.

Step D.7.4 -- Verifying that the DH pumps are on and verifying that the LPI MOVs are open are called out in the same procedural step. The equipment items are all located on the ESF panel. An error of omission is assigned for forgetting the task entirely. For the DH pumps, the wrong items of equipment could be chosen or the indications on the correct items could be interpreted incorrectly. For the LPI MOVs, the wrong switches could be selected or their indications interpreted incorrectly. Two errors of commission have been assigned to each item.

Step D.9 -- Monitoring the level of the BWST (a dynamic task) provides the operator with the cue to perform the rest of this step. If he fails to monitor or if he monitors incorrectly, the other activities in this step will not be performed. An error of omission is assigned to the monitoring task only since the rest of the activities in this step are considered to be completely dependent with respect to errors of omission. A reading error is also assigned to the monitoring task. For the manipulation of the valves, errors of selection and interpretation or reversal are possible.

The errors assigned for the operations outlined in Figure 7 were determined in a slightly different manner. First, consider the fact that the assigned operator performs these actions in response to an order from the senior control room operator. If the senior man fails to order these tasks, they will not be performed. In developing the HRA event tree for this set of tasks (see Section 5.6), this probable error will have to be considered. Regarding the rest of these tasks, the operator must perform them on three different levels of the plant. He views his job at each level as a unit task; therefore,

errors of omission apply to each of these unit tasks. If he remembers to stop at a given level, we assume that the operator will attempt all the tasks required at that level. Errors of commission are discussed below.

Step D.7.1 -- MU-13 is the only valve located in the stairwell outside the MU Pump Room. No selection error is possible. It is not deemed likely that the operator would make a reversal error on a manual valve in this situation.

Step D.7.2 -- Valves DH-7A and -7B are located outside the DH Pump Rooms, one on each end of the hall. They are very large valves, and the only other valves in that area are too small to be confused with them. Of all the valves inside the DH Pump Rooms, those called for in this step are located high on the walls of the rooms; the only other valves in the rooms are on piping lines that run along the floor. In none of these cases are errors of selection deemed likely.

Step D.7.3 -- ABS-13 and -14 are located under the grating outside the watertight doors. They are the only valves there; likewise, there is only one set of watertight doors at this location. Again, selection errors were not considered likely.

5.6 Develop HRA Event Trees

5.6.1 Discussion

In making a probabilistic statement as to the likelihood of occurrence of human error events, each error defined as likely in the task analysis is entered as the right limb in a binary branch of the HRA event tree. Chronologically, in the order of their potential occurrence, these binary branches form the limbs of the HRA event tree, with the first potential error starting from the highest point on the tree at the top of the page. An example of an HRA event tree is shown in Figure 8.

Any given task appears as a two-limb branch, with each left limb representing the probability of success and each right limb representing the probability of failure. (In a later phase of the HRA, the HEPs from the Handbook will be entered on the tree. See Section 5.7.) Once a task is diagrammed as having been completed successfully (or unsuccessfully), another task is considered; the binary branch describing the probability of the success (or failure) of the second event extends from the left (or right) limb of the first branch. Thus, every limb following the initial branching depicts a conditional probability. The initial branching also represents a conditional probability in that the probabilities for that branch are based on the existence of a given situation. However, it is defined as the starting point for the analysis, not as a conditional probability, since we do not investigate the probabilities of occurrence of the circumstances of the basic situation. (As described in Chapter 5 of the Handbook, the conditional probabilities are understood in the labeling scheme shown in Figure 8, e.g., the leftmost limb, labeled b, actually means b|a.)

Each limb is described or labeled, usually in a form of shorthand. Capital letters in quotes ("A") represent certain tasks themselves. Capital letters (A) represent failure or the probability of failure on given tasks. Lower case letters (a) represent success or the probability of success on certain

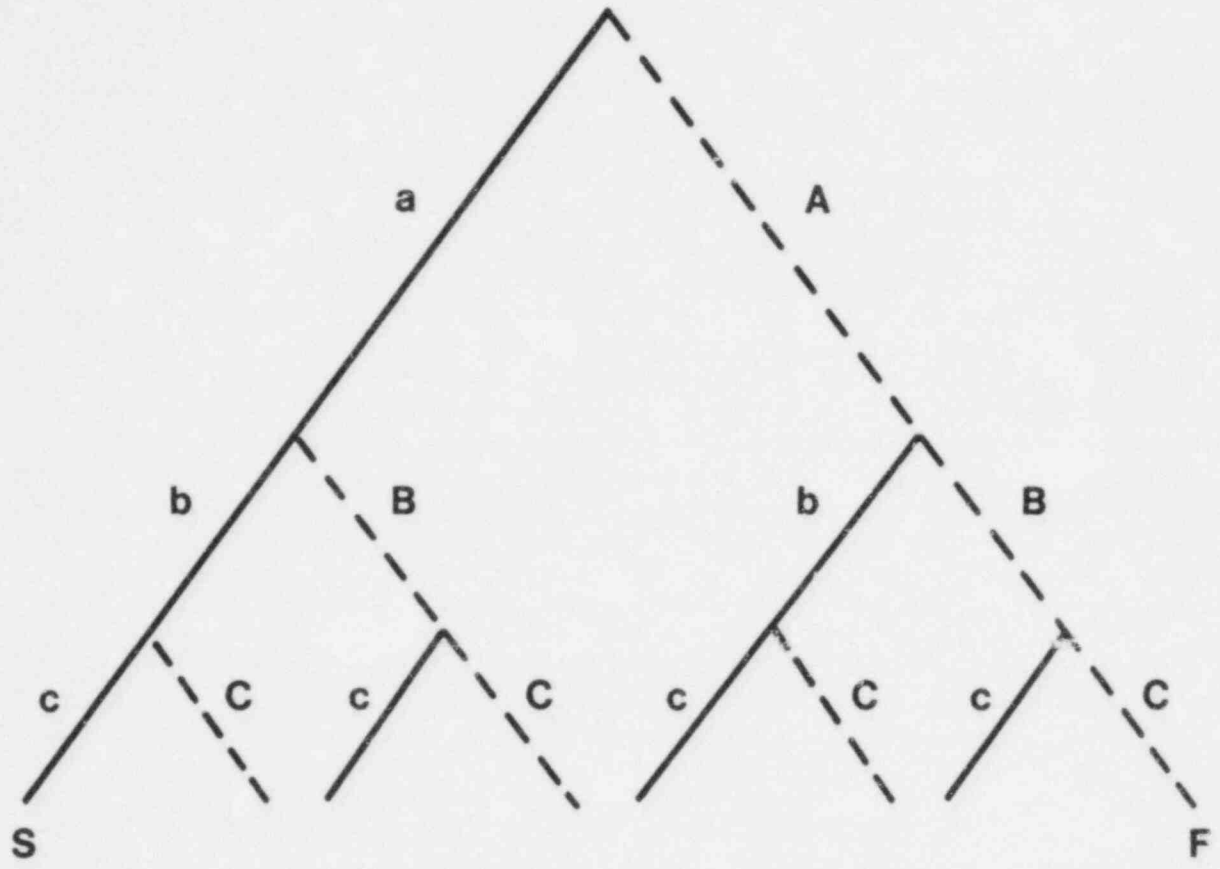


Figure 8 An example of HRA event tree diagramming.

tasks. The same convention applies to Greek letters, which represent nonhuman events such as equipment failures. The letters S and F are exceptions to this rule, in that they represent system success and failure, respectively. In actual practice, we sometimes label the limbs of an HRA event tree with a short description of the error itself. This eliminates the necessity for having a legend at the bottom of the page which defines each event by its alphabetic denotation. The labeling format used is unimportant--the critical task in developing HRA event trees is the definition of the events themselves and their translation onto the trees. (Examples of labeling formats are shown in Figures 9 and 10.)

All the limbs of an HRA event tree are heavy solid lines in the diagram. For illustration only, the limbs representing failure in Figure 8 are shown as dashed lines. (See Chapter 5 of the Handbook for a more complete discussion of the basics of HRA event tree diagramming.)

In PRA, we are usually interested in determining the probability of error on a single task or in the probability that for a set of tasks, none or all will be performed incorrectly. For the first case, no HRA event tree need be developed unless performance on that single task is affected by other factors the probabilities of which should be diagrammed. A description of the task and knowledge of the PSFs are sufficient for entering Chapter 20 of the Handbook to determine a single HEP. For the second case, in which we want to know the probability of all tasks' being performed without error, a complete-success path through the HRA event tree is followed (as discussed in Chapter 10 of the Handbook). Once an error has been made on any task, a criterion for system failure has been met. Given such a failure, no further analysis along that limb is necessary at this point. In effect, probabilities of event success that follow a failure and that still end in a system success probability constitute recovery factors and should be analyzed later in the HRA, if at all. Thus (as shown in Figures 9 and 10), we have HRA event trees that are developed along the complete-success path only. This does not indicate that we think that this is the only combination of events possible; it indicates only that in the initial analysis we go no further once system failure has been met.

Development of the HRA event tree is the most critical part of the process for quantifying the probabilities of human errors. If the task analysis has listed the possible human error events in the order of their potential occurrence, the transference of this information onto the HRA event tree is made much easier. Each potential error and success are represented as binary branches on the HRA event tree, with subsequent errors and successes following directly from immediately preceding ones. Take care not to omit the incorporation of errors not found in the task analysis table that were determined to have a potential effect on the HEPs listed in the table. For example, errors of administrative control that affect a task's not being performed but that may not appear in the task analysis table must be included in the HRA event tree.

5.6.2 Example

The HRA event trees shown in Figures 9 and 10 represent the task analyses shown in Figures 6 and 7, respectively. In Figure 9 (HRA Event Tree of Actions by Operators Assigned to the Control Room), the labeling format incorporating a short description of each event for its corresponding limb is

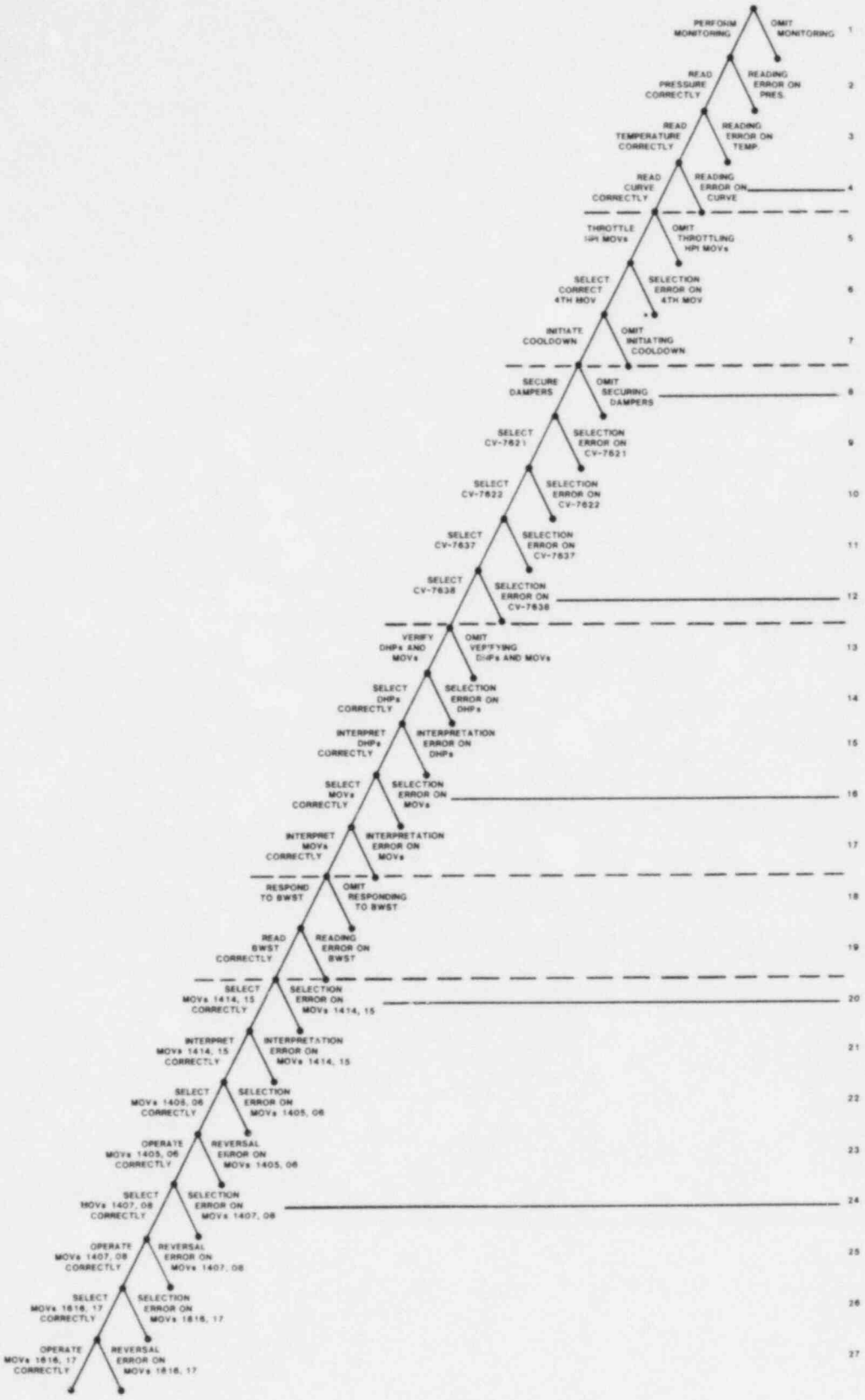
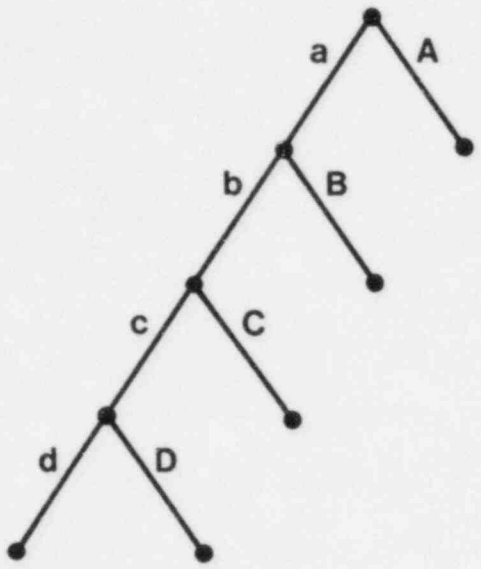


Figure 9 HRA event tree of actions by operators assigned to the control room.



Event	HEP	Source

A = Control room operator omits ordering the following tasks

B = Operator omits verifying the position of MU-13

C = Operator omits verifying/opening the DH valves

D = Operator omits isolating the DH rooms

Figure 10 HRA event tree for actions performed outside the contol room.

used. This is very convenient for analyses in which there are large numbers of events diagrammed. Referring back and forth to a legend describing the events represented would be inconvenient in these cases. The dashed lines in Figure 9 are placed according to those found in the corresponding task analysis table in Figure 6. Again, they are included to aid the system analyst in extracting information from the HRA event tree for inclusion in the system analysis.

Figure 10 (HRA Event Tree for Actions Performed outside the Control Room) shows a case in which the format consisting of alphabetic labels and an accompanying legend can be used very effectively since it consists of a small number of events. The legend format has the advantage of allowing a more complete description of the error events than does the short label format. As stated previously, however, the actual labeling format is of little importance as long as it is helpful to the analyst. Combinations of these two styles may be used, or entirely new formats may be developed by the analyst.

Both HRA event trees shown reflect the technique described above and in Chapters 4 and 5 of the Handbook. The possible errors listed in their respective task analysis tables have been put directly onto the right limbs of the branches of the HRA event trees in Figures 9 and 10. We show only the complete-success paths, as previously explained. The first branch of Figure 10 represents the adminstrative control error identified in the discussion of that set of tasks. In the HRA event tree itself, no distinction is made between the error events that appeared in the task analysis table and those that were identified during other parts of the analysis.

5.7 Assign Nominal HEPs

5.7.1 Discussion

Now that the errors have been identified, defined, and diagrammed, estimates of the probability of occurrence for each of them must be assigned. Since the analyst should be familiar with the theories, models, and limitations presented in the Handbook, he will be able to use Chapter 20 of that document to make most of these estimates.

First, the task itself must be categorized. The analyst determines whether he is dealing with an operator manipulating valves, performing a check of another's work, using a written procedure, or attempting some other type of task. Errors are then considered on the basis of their being of the omission or commission types. The tables in Chapter 20 of the Handbook are organized to contain groups of HEPs that relate to a given type of error (omission or commission) that may occur in the performance of a certain type of task. Errors of omission are found in Chapter 20 in tables describing the use of the type of plant directive being followed (e.g., written procedures, oral instructions, standard shop practice, etc.). Errors of commission are listed in tables describing the PSFs associated with equipment types.

The analyst should have "read" and should be familiar with the organization of the HEPs found in Chapter 20. The data are presented in tables that duplicate their original appearance in the subject chapters of the Handbook. An analyst who is familiar with the organization of Chapter 20 prior to his trying to use it as a source document will have decreased the time required for the performance of this portion of the HRA considerably. Also, he will have helped

himself predetermine cases in which it will be necessary for him to make estimates of HEPs directly from the task analysis since no such task description exists in Chapter 20.

Most of the tables in Chapter 20 have several numbered items, each one of which lists a short description or name of a possible task, condition, or operation together with an estimated HEP and its uncertainty bounds. The estimated HEP is usually considered to be the median of a lognormal distribution. The uncertainty bounds are usually expressed as an error factor (EF). Dividing the median HEP by the EF provides an estimate of the 5th percentile HEP as the lower uncertainty bound on the lognormal distribution. Multiplying the median HEP by the EF provides an estimate of the 95th percentile HEP as the upper uncertainty bound on the lognormal distribution. The analysts who are familiar with the organization of Chapter 20 can search the tables themselves for the HEPs relevant to their task analyses. A search scheme to direct the analyst to the appropriate table is found at the beginning of Chapter 20.

A description of each error identified for every task in the task analysis should be looked up in Chapter 20 of the Handbook. That is, the description that most closely approximates the situation under consideration should be identified. In some cases, the description in Chapter 20 will detail a scenario that differs slightly from the one in the analysis. If the differences in specifics are not large, the analyst may judge that they are so minor as not to affect materially the use of the HEP as is. In other cases, the actual situation and the one described in Chapter 20 may reflect tasks that are basically the same but that are performed under different circumstances. The HEP must then be modified to reflect the conditions of actual task performance. Usually, this is done during the assessment of the PSFs acting on the task (see Section 5.8).

Especially for cases in which an estimated HEP other than the one found in the Handbook is used, the source for the HEPs entered on the HRA event trees should be recorded, along with the assumptions made in their derivations. The table number and item number should be recorded if Chapter 20 is the source for the HEP. If an HEP from the Handbook was used as a reference point for the derivation of an estimated HEP, its specific source and the reasoning behind its modification should be noted. For easy reference, this information can be added to the task analysis tables. New columns in the table for the HEP and its source can be made. This documentation is necessary for many reasons. Other analysts may want to check the similarity of their solutions to those of other problems. Given that the estimates of many of the HEPs in the Handbook are numerically identical, these other analysts must have some method for tracing the original analysis. The assumptions should be recorded to prevent the analyst's having to reinvestigate a situation should he need to refer to an analysis again. Also, in the course of performing a series of analyses on a single facility, some sections of an analysis may be used several times. The analyst must, however, be able to demonstrate that the situations are indeed identical before reproducing part of one analysis to be used without modification in another.

In the HRA event tree shown as Figure 11 and in subsequent discussions and figures, results are shown to several decimal places merely to illustrate the arithmetic. In practice, final answers are subjected to judicious rounding.

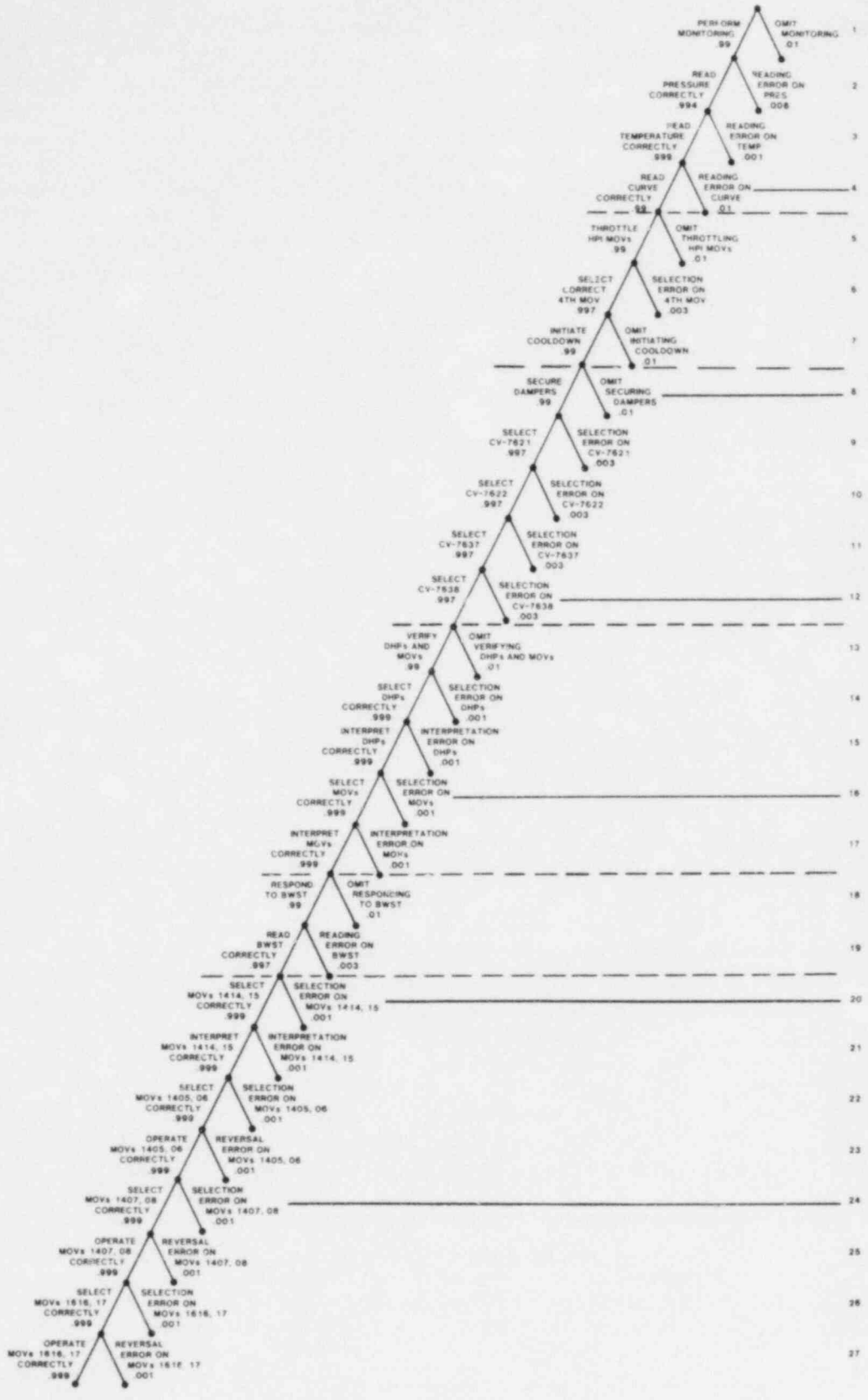


Figure 11 HRA event tree for actions by operators assigned to the control room with original estimates of HEPs.

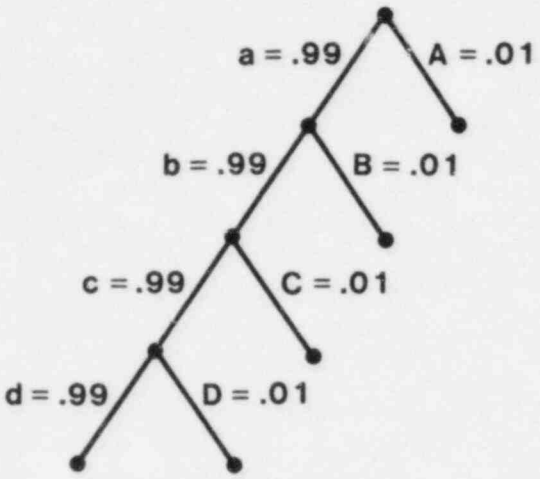
NOTE: In Section 1.4, it is stated that one of the limitations of the tabled HEPs in the Handbook is that most of them apply to rule-based human actions. For diagnosis errors related to the evaluation of display indications that result from a transient, we suggest using the Nominal Model for Diagnosis that appears in Chapter 12 of the Handbook. This model lists the cumulative values for estimated HEPs and EFs for combined recognition and diagnosis of an abnormal event (e.g., a transient or LOCA) as a function of time since some compelling indication of the event. Unlike other human performance models in the Handbook, the Nominal Model for Diagnosis is based on the estimated collective performance of the control room personnel. Instructions for use of the model are given in Chapter 12 of the Handbook. Also included in that chapter are screening values for diagnosis and for following the rule-based activities subsequent to the diagnosis of an abnormal event. The first example in Chapter 21 of the Handbook illustrates the use of the nominal model for diagnosis. For some kinds of transients, there are plant-specific operating rules that, if rehearsed properly, will effectively eliminate any initial indecision on the part of the operator when a transient occurs. (For an example, see the third case study described in Chapter 21 of the Handbook.) In such a case, the main effort of the human reliability analyst will be to estimate the effectiveness of the provisions for in-plant rehearsal of these operating rules. This type of treatment reflects the state-of-the-art in HRA and points to the need for the type of NRC-sponsored studies mentioned in Section 1.4.

5.7.2 Example

Keep in mind the situational characteristics that affect the performance of this set of tasks. For example, in this case, we are analyzing the actions of operators who are following a set of written procedures. Any errors are made in the context of using those procedures. Also, remember that recovery factors are not to be considered at this time. Even though there will be three licensed operators available in the control room at this time following the transient, we will only consider the actions of one of them in this first analysis.

In the first part of this example, each error and the source of its estimated HEP will be discussed in detail. Later in the example, errors that have already been discussed will simply have their source HEPs mentioned. Figures 11 and 12 show the same HRA event trees diagrammed in Figures 9 and 10, but with the derived estimates of the HEPs for each error included as part of the diagram. As shown, this can be done by adding the HEP as part of the label for each limb or by including the HEPs as columns in the legend for the HRA event tree. Again, the method employed for displaying the HEPs on the HRA event tree is unimportant.

For simplicity, the EFs in this example are taken directly from the referenced tables and are not modified when the effects of stress and type of task are considered. In a real analysis, the EFs for certain tasks may be increased per Table 20-20 of the Handbook. In examples 3 and 5 in the appendix, appropriate modifications are made to EFs for unusual situations.



Event	HEP	Source
A = Control room operator omits ordering the following tasks	.01 (EF = 3)	T20-6, #1
B = Operator omits verifying the position of MU-13	.01 (EF = 3)	T20-8, #3
C = Operator omits verifying/opening the DH valves	.01 (EF = 3)	T20-8, #3
D = Operator omits isolating the DH rooms	.01 (EF = 3)	T20-8, #3

Figure 12 HRA event tree for actions performed outside the control room with original estimates of HEPs.

The first error* on the HRA event tree in Figure 11 is that of the operator's omitting the performance of the monitoring task for the RCS pressure and temperature. This is the first part of step D.2. If the operator fails to do this part of step D.2, it is presumed that he will fail to carry out the remainder of the step. This failure to maintain RCS temperature and pressure was designated as a failure by the system analysts. Since we are dealing with the operator's following a set of written procedures, we use an estimate of this error from Table 20-7, in the Handbook.** This table consists of estimates of errors of omission made by operators who are using written procedures. In other words, these estimates reflect the probability, under the conditions stated, of an operator's omitting any one item from a set of written procedures. Since the procedures in our example are emergency procedures that do not require any checkoff of steps by the operator, we use the section of Table 20-7 that deals with procedures having no checkoff provision. Looking at the procedures in Figure 3, we see that more than 10 steps must be performed by the operator. This analysis deals with fewer than 10 procedural steps, but these must be considered in the context of their performance. The fact that we are analyzing only a few steps has no effect on the operator as he follows the set of procedures. Given that this error occurs when using a long list of written procedures that does not require a checkoff, the estimated HEP for it is given in item 4 of Table 20-7, .01 (EF = 3). At this point in the analysis, the nominal value of the HEP is entered on the HRA event tree.

The second error shown in Figure 11 is that of the operator's making a reading error on the indicator for RCS pressure. This indicator is a chart recorder. Reading errors are errors of commission and are found grouped in Chapter 20 according to the type of information they display and to the type of indicator that makes up the display. In this case, the operator is reading a value, an exact numerical representation, from the chart recorder. Table 20-10 consists of estimated HEPs for errors made in reading quantitative information from different types of displays. For the chart recorder in question, item 3 from that table is used, .006 (EF = 3).

The third error also involves reading an exact value from a display. The display in this case is a digital readout, therefore, item 2 from Table 20-10 is used, .001 (EF = 3).

The fourth error is also a reading error, this time involving the pressure-temperature curve. The curve is presented in a graph format, so the HEP for errors made in reading quantitative information from a graph is used, item 5 from Table 20-10, .01 (EF = 3).

Another error of omission appears as the fifth error limb on the HRA event tree in Figure 11, that of the operator's not throttling the HPI MOVs. For errors of omission, the nature of the task does not affect the probability of the error. Therefore, the same HEP that was used on the first error, .01 (EF = 3), is used again here.

---

* References to error numbers correspond to the numbered events in all related HRA event trees and to like-numbered entries on the task analysis table.

** All references to table and item numbers are from the 1983 issue of the Handbook.

A selection error for the fourth of the HPI MOVs was identified as likely in the task analysis. It is the sixth of the errors found on the HRA event tree. Figure 4, which shows the layout of the control panels containing the HPI MOVs, demonstrates that the HPI MOVs are in similar positions on control panels CP16 and CP18. Surrounding them are several similar switches, one of which (to the immediate right of the HPI MOVs on CP18) is the switch most likely to be the target of the selection error. An estimate of this error of commission is found by looking in the tables in Chapter 20 that deal with errors made in the manipulation of the switches in the control room which are used to change the state of MOVs. Table 20-12 consists of HEPs for commission errors made in manipulating manual controls (such as the hand switch for an MOV). Item 2 ("select wrong control in an array of similar-appearing controls identified by labels only") most closely approximates the situation described here, so the HEP of .003 (EF = 3) is used as the estimate for this error.

The seventh error involves an omission on the part of the operator to initiate cooldown procedures by following another set of written procedures. As far as we are concerned here, this is a case of his omitting a single step of this procedure, so .01 (EF = 3) is used again. It is also used for the eighth error, that of omitting to secure the DH room purge dampers.

The 9th, 10th, 11th, and 12th errors are selection errors involving the manipulation of the switches for 4 MOVs. The switches are probably grouped close to each other on a wall of the Ventilation Room, but we have no specific information relative to the ease or difficulty of locating the group. Since it is unknown whether the layout and labeling of the switches in the Ventilation Room helps or hinders the operator in his search for the controls, we take the conservative position of assuming them to be among similar-appearing items. We use the same HEP as was used for the selection error associated with the fourth HPI MOV (error No. 6), .003 (EF = 3), for each of these MOVs.

The 13th error is one of omitting a procedural step. The HEP of .01 (EF = 3), discussed earlier, was used. If this procedural step is performed (is not omitted), errors of selection for both types of components mentioned (the DH pumps and the LPI MOVs) are possible. These selection errors appear as the 14th and the 16th errors on the event tree. We know from Figure 4 that both of these sets of controls are part of groups that have been arranged functionally on the control panels. They are very well delineated and can be identified more easily than can most of the switches in the control room. Item 3 from Table 20-12 involves making a selection error in choosing a control from a functionally grouped set of controls; its associated HEP is .001 (EF = 3).

Errors of interpretation are also possible for the DH pumps and the LPI MOVs. Given that the operator has located the correct switches, there is a possibility that he might fail to notice their being in an incorrect state. In effect, this constitutes a reading error, one made in "reading" (or checking) the state of an indicator lamp. No quantitative information is involved, so Table 20-11, which deals with commission errors made in check-reading displays, is used. Item 8 from that table states that the error of misinterpreting the indication on an indicator lamp is negligible. However, for this example we will assign an HEP of .001 (EF = 3) so as not to simplify the HRA event tree. The 15th and 17th errors on the event tree represent these interpretation errors.

The HRA event tree's 18th error is defined as the operator's omitting to respond to the BWST level. The same omission HEP used previously, .01 (EF = 3), is repeated here. Given no such omission error, a reading error (No. 19 on the event tree) could be made on the BWST meter. Going back to Table 20-10 for commission errors made in reading quantitative information, the HEP to use when considering an analog meter is .003 (EF = 3), the first term in the table.

Errors 20, 22, 24, and 26 involve selecting the wrong set of MOV switches from sets of functionally grouped switches. As above, this HEP is item 3 of Table 20-12, .001 (EF = 3).

The 21st error (interpretation) is made while checking the status of an indicator lamp. An HEP of .001 (EF = 3) (as cited for the 15th error above) is assigned.

The 23rd, 25th, and 27th errors are representations of reversals made by the operator. Instead of opening the MOVs, he closes them, or vice versa. As discussed in the section, "Estimated Probabilities of Errors of Commission," in Chapter 13, "Manual Controls," of NUREG/CR-1278, reversal errors for two-position switches are so infrequent that they can be assigned a probability of zero. However, for PRA purposes, a nominal value of .0001 (EF = 10) is suggested because of the occasional exception that occurs when a switch was left in the wrong position previously (Table 20-12, item 8). For the present example, we use the upper bound, .001, to avoid simplifying the HRA event tree. We retain the EF = 10.

For the HRA event tree in Figure 12, we are analyzing the actions that take place outside the control room. The first error diagrammed is one of administrative control that did not show up in the task analysis: the shift supervisor omits ordering another operator to perform this set of tasks. Since the ordering of the tasks is his responsibility, this constitutes a failure to carry out plant policy. An HEP of .01 (EF = 3) from Table 20-6, item 1, is used.

The second, third, and fourth errors shown in Figure 12 represent errors of omission made by the operator who performs the tasks. These tasks call for the manipulation of valves located on levels of the plant under the control room. We assumed that the operator would not be working from a set of written procedures (he would not take a copy of the procedures with him) but from an oral instruction given him by the control room operator. The model accounting for errors of omission made in following a set of oral instructions will be followed. The data for this model are found in Table 20-8. We stated in the talk-through section that the operator sees these as three distinct unit tasks, one to be performed on each of the three levels he must visit. We therefore assume that he must recall three specific tasks, so item 3 in the table is used, an HEP of .01 (EF = 3) for each of the tasks.

5.8 Estimate the Relative Effects of PSFs

5.8.1 Discussion

A primary consideration in conducting an HRA is the variability of human performance. This variability occurs within any given individual in the performance of tasks across time (from day to day, from week to week, etc.).

Variability also results from the performances of different personnel (from man to man, shift to shift, or from plant to plant). Variability is caused by PSFs acting within the individual or on the environment in which the task is performed. Because of this variability, the reliability of human performance usually is not predicted solely as a point estimate but is determined to lie within a range of uncertainty. A point value HEP for the PRA can be estimated by considering the effects of relevant PSFs for the task in question. Estimates provided so far in this document apply to nonstressful, normal working conditions. Modifications of these nominal estimates can be made on the basis of guidelines provided in the Handbook.

The nominal HEPs are to be used when the scenario outlined in the Handbook reflects the situation being analyzed. If the plant situation is worse in terms of the PSFs or the response requirements than the one described in the Handbook, the HEP for that task should be higher than the nominal value. That is, if the analyst judges that the situation under study is more likely to result in error than the one outlined in the Handbook, an HEP closer to the upper uncertainty bound than the nominal is should be used. Likewise, if a plant's situation is judged to be less likely to result in a human error than the one outlined in the Handbook, an HEP closer to the lower uncertainty bound than the nominal is should be used.

In judging these effects, the analyst should first consider the error events individually. For each error probability assigned, a judgment must be made as to whether the nominal HEP should be used. The analyst should examine the performance situation for factors potentially affecting each event. For errors of omission, for example, the analyst should search for cues or reminders that would make forgetting any item less likely or, for poorly written procedures, that would make forgetting an item more likely. For errors of commission, those elements of the performance situation that might affect the actions themselves or the operator as he performs them must be identified. For example, if the face of a display is such that reading it is unusually difficult, an HEP higher than the nominal value for reading errors for such a display should be assigned.

Next, the analyst should consider the influence of PSFs that have a global effect--those that affect the probability of error on all or most of the events in the analysis. Some models presented in the Handbook reflect the influences of these overriding PSFs. The most commonly encountered ones deal with stress and the level of experience of the operators.

The compilation of data in the Handbook reflects by its organization the effects of some PSFs. For example, the distinction made for errors of omission in using a written procedure on the basis of whether a checkoff provision is available is really one based on the quality of the procedure as a PSF. Whether an available checklist is used <u>properly</u> is an example of the PSF of administrative control. Reading errors for displays are given relative to the difficulty of the reading task. In these cases, the effects (to some extent) of the PSFs have been determined for you.

5.8.2 Example

In evaluating the effects of PSFs on the individual error events, we judge that in each case the scenario described in the Handbook reflects that of our "plant" closely enough so that no modification of the nominal HEPs is necessary.

Now we must consider the effects of overriding PSFs--those that will affect all of the HEPs. We have stated in the original assumptions that the operators are experienced. Since they are following an emergency procedure, we will consider them to be under a moderately high level of stress. We see from Table 20-16, that the HEPs for experienced personnel operating under a moderately high level of stress should be doubled for step-by-step tasks (item 4a) and multiplied by 5 for dynamic tasks (item 5a). Step-by-step tasks are defined as those tasks requiring essentially one well-defined action (such as manipulating a switch) by the operator. Dynamic tasks require a greater degree of man-machine interaction than is required in step-by-step tasks. Dynamic tasks may require decision-making, keeping track of several functions, or any combination of these. Monitoring an indicator over a period of time in conjunction with other tasks is often considered to be a dynamic task.

Figure 13 shows the HRA event tree for control room actions with the nominal HEPs presented in Figure 11 modified to reflect the effects of a moderately high stress level. The only dynamic tasks in Figure 13 are those calling for monitoring activities. These are the monitoring of the RCS temperature and pressure indicators and the interpolation of these values onto the cooldown curve and the monitoring of the BWST level. The nominal HEPs for these tasks have been multiplied by 5; those for the other events in this figure have been doubled.

Another overriding PSF that must be considered, this time for the tasks performed outside the control room, is the effect of the operator's having to wear protective clothing. For cases in which protective clothing is necessary, we assume that the operator is highly motivated to complete his assigned tasks quickly because of the heat in the working environment, his isolation, and the general discomfort caused by the protective clothing. These factors combine to increase the HEPs for tasks performed by operators wearing such protection. This is discussed in Chapter 3 of the Handbook in which it is stated that HEPs for such tasks should be doubled.

Figure 14 shows the events taking place outside the control room, with their HEPs having been modified to reflect these PSFs. The first error (failure of administrative control) takes place in the control room. The HEPs for this and for the other events have been doubled to reflect the effects of the moderately high stress level. The HEPs for the three tasks that actually take place outside the control room have been doubled again to reflect the effects of the operator's wearing protective clothing. This doubling and redoubling results in a conservative estimate of the final HEP; in some analyses, it might be judged that this level of conservatism is unreasonable.

5.9 Assess Dependence

5.9.1 Discussion

It is stated earlier in this paper that except for the first branch of an HRA event tree, all branches represent conditional probabilities of success and failure. Dependence between events directly affects these conditional probabilities. Some cases of dependence will be spotted during the talk-through. This is a good time to take note of equipment similarities that contribute to the level of dependence between actions performed on like items.

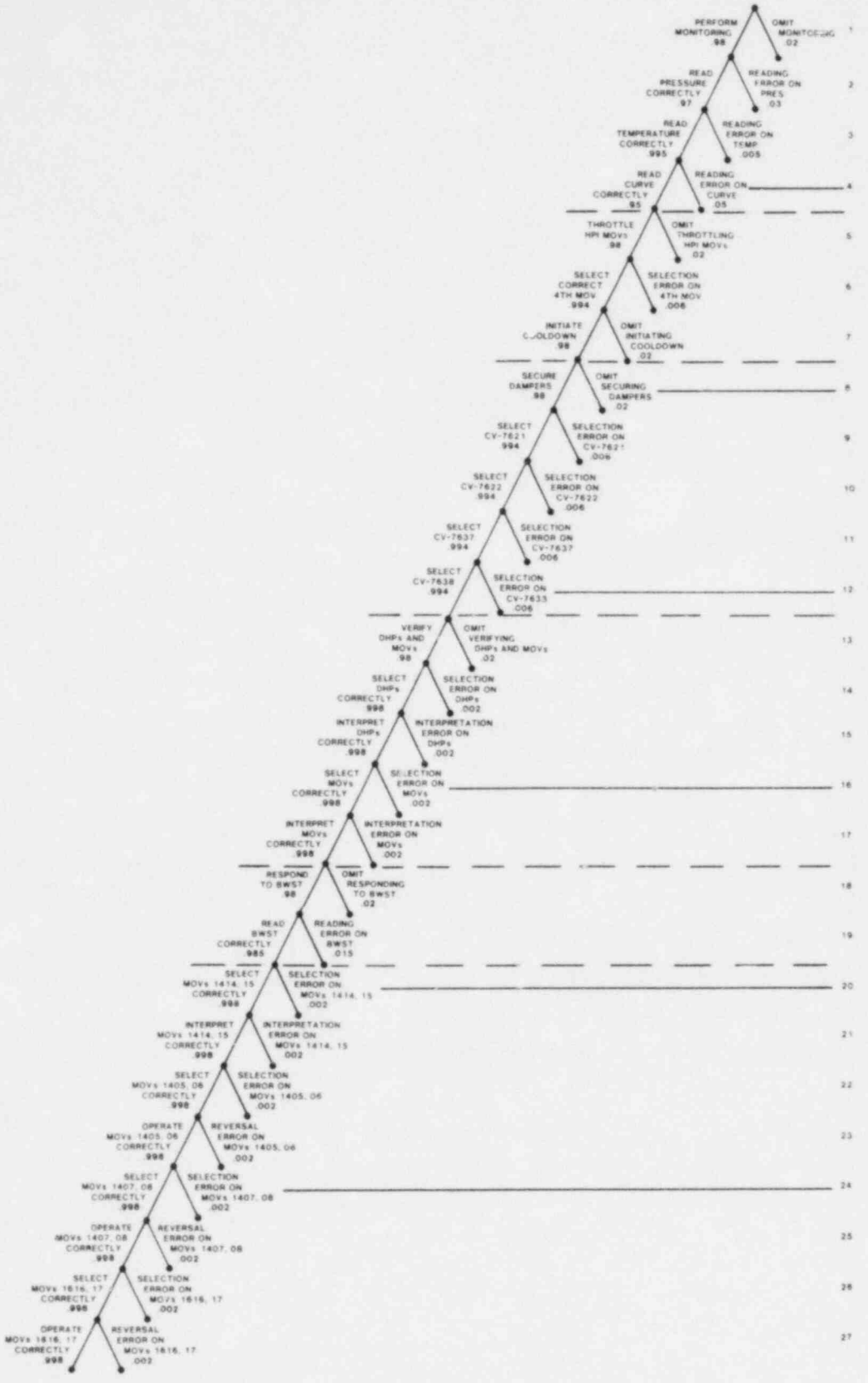
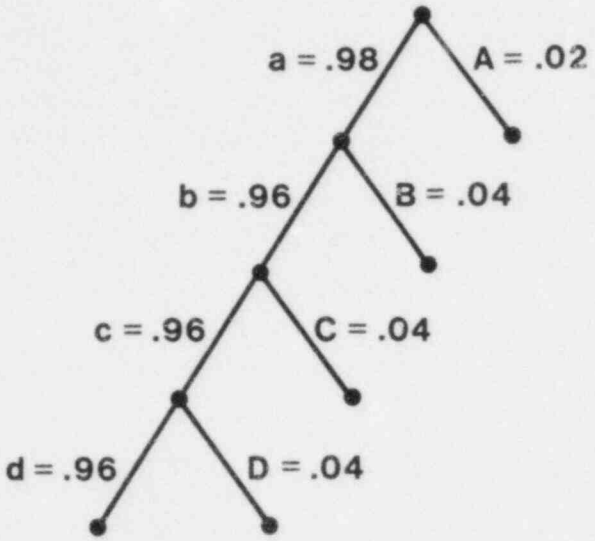


Figure 13 HRA event tree for actions by operators assigned to the control room with HEPs from Figure 11 modified to reflect PSFs.



Event	HEP	Source
A = Control room operator omits ordering the following tasks	.02 (EF = 5)*	T20-6, #1
B = Operator omits verifying the position of MU-13	.04 (EF = 5)**	T20-8, #3
C = Operator omits verifying/opening the DH valves	.04 (EF = 5)**	T20-8, #3
D = Operator omits isolating the DH rooms	.04 (EF = 5)**	T20-8, #3

* Modified to reflect the effects of moderately high stress

** Modified to reflect the effects of moderately high stress and protective clothing

Figure 14 HRA event tree for actions performed outside the control room with HEPs from Figure 12 modified to reflect PSFs.

Dependence can occur between two performances with respect to errors of omission, errors of commission, or both. If dependence is assessed due to the fact that two actions are called for in the same procedural step, dependence is likely to affect HEPs for errors of omission. If components are to be manipulated at different times in a given procedure, the dependence may affect the HEPs for errors of commission, especially for selection errors.

Guidelines for determining the level of dependence assigned to a situation are found in Chapter 10 of the Handbook. There are no cut-and-dried rules for this kind of determination; rather, it is one that must be made only after a carefully detailed study of the performance situation since determinations of dependence levels are highly situation-specific. These determinations should be made for every task performed as part of every procedure targeted for HRA. This is necessary because dependence may exist between one task that is analyzed in the HRA and one that is not. Given the performance context of each analysis, the effects of such dependence must still be quantified.

A decision as to whether complete dependence or complete independence applies to a given case can be made relatively easily. That is, it should be obvious if one action is the causal factor for another or if two actions are totally unrelated. Distinctions between the three intermediate levels of dependence are more difficult to make. First, decide whether dependence exists at all--whether the actions are completely independent. If dependence exists, decide whether complete dependence is appropriate and, if so, to what circumstances it applies. If you judge that the dependence that exists is greater than zero but less than complete, an intermediate level must be assigned. This judgment can be made based on the relation of the actual situation to zero and complete dependence. If you decide that the dependence demonstrated by the situation is much closer to zero than to complete dependence, assign a low level of dependence. If, on the other hand, you decide that the situation exhibits a degree of dependence that is very close to but not equal to complete dependence, assign a high level of dependence. If you cannot make a definitive statement to the effect that either of the above is true, assign a moderate level of dependence. Chapter 10 of the Handbook provides guidance in assigning levels of dependence.

Another method of assigning an intermediate level of dependence is to make a precise estimate as to the percentage of time the effects of zero or complete dependence will be seen. From that estimate, assign the intermediate dependence level that most closely approximates it. For example, if you make a judgment (perhaps based on a frequency count from actual data or from your knowledge of the work situation) that task "B" will be performed correctly half of the time given that task "A" has already been performed correctly, you have assigned a conditional probability of $b|a = .5$. This conditional HEP of .5 reflects an estimated high level of dependence using the Handbook model for basic HEPs $\leq .01$.

Remember that the dependence model in the Handbook deals only with the effects and the quantification of positive dependence. If you judge negative dependence to be appropriate to a situation, its effects will have to be determined directly rather than by using the dependence model. Also, keep in mind that dependence is not necessarily symmetrical. The same level of dependence may not exist for the success and the failure paths of an HRA event tree.

The model presents some point estimates that may be used in lieu of the exact equations to determine the conditional probabilities of dependent events. These are conditional HEPs of .05 for low dependence, .15 for moderate dependence, and .5 for high dependence. The conditional HEPs for zero dependence and complete dependence are, respectively, the basic HEP (BHEP) and 1.0. The point estimates of .05, .15, and .5 should be used only when the BHEP is less than or equal to .01. In other cases, the equations should be used. For illustrative purposes, the example calculations in this document are based on the equations.

5.9.2 Example

In the sample problem, several cases of dependence have already been accounted for. For example, in the case of the 4 HPI MOV switches, their physical similarity, their positions in the procedure, and the fact of their being located in relatively identical positions on the control panels resulted in our assumption that, for errors of omission, they are completely dependent. In considering dependence for the selection errors that could be made on these switches, the same factors plus the layout of the rest of this control board resulted in our determining that the first three are completely dependent for selection errors (none are considered likely) while the fourth is susceptible to such an error. The nature of the tasks performed outside of the control room and the operator's perception of them (from interviews with plant operators, we determined that the operator typically views each set of tasks performed on a plant physical level as a single unit task) led to our considering them to be completely dependent with respect to errors of omission.

The estimation of the effects of more than one operator in a given location constitutes a recovery factor. If we determine the effects of having more than one operator in the control room during the performance of this procedure, we are in fact quantifying a recovery factor for the procedure. However, since we will show that some level of dependence exists among the operators in the control room, we will quantify these effects now as an illustration of dependence.

As noted in Section 5.3.2, Chapter 18 of the Handbook states that there will be three reactor operators and a shift technical adviser in the control room well before 60 minutes into the small LOCA, the time of interest in this example. In the example, we assume that the shift technical adviser is engaged in other activities at this time, and that there are available for the procedures to be analyzed the three reactor operators: two reactor operators and the shift supervisor (SS). Table 20-4 indicates that there is a high level of dependence between the two operators and a low-to-moderate level of dependence between them and the SS, who is also a licensed operator.

Since this procedure calls for the performance of several tasks outside the control room and since the performance of these tasks requires that the operator wear protective clothing, we assume that one of the three men available will leave the control room during the entire procedure to prepare for and then perform these tasks. We assume that this will be the most junior man in the control room since the other two are more capable of handling the transient from the control room. Responding to the nature of the control room tasks, we assumed high dependence between the operators there. This assumption is based on the fact that at this time following the transient, one of the operators will be primarily involved in directing the actions of the

junior operator as he changes the positions of locally operated valves. Telephone communication between the two will call for most of this operator's concentration as he describes the necessary operations. The other control room operator will be involved with monitoring the displays and performing the manipulations necessary at the ESF panels. High dependence is assumed because we judge that the man on the telephone will, for the most part, rely on the operator at the ESF panels to perform those tasks correctly. Nevertheless, we judge that, despite his primary task of coordinating the junior operator's tasks by phone, this operator will catch errors made by the other control room operator about half the time.

Figure 15 shows the HRA event tree of the actions performed by the control room operators with the HEPs (already modified to reflect the effects of PSFs) modified to reflect the effects of dependence. The probabilities of error of both the available operators have been collapsed onto a single limb for each type of error. The numbers in parentheses (shown for illustration only) are the conditional HEPs for the probability of the second operator's failing to catch the error made by the first operator. The other numbers are the products of these conditional HEPs and the basic HEPs of the first operators; thus, they represent the joint probability of an error's being made by one operator and not being recovered by the other, i.e., an unrecovered error.

Those actions taking place in the Ventilation Room do not demonstrate any dependence between operators since we assume that one operator will be performing them.

The only event in Figure 16 that is affected by dependence is the first. If the senior control room operator forgets to order those tasks, the other senior man or the junior man himself may remind him of the necessity to do this.

5.10 Determine Success and Failure Probabilities

5.10.1 Discussion

Once the human error events have been identified and quantified individually, their contribution to the probabilities of system success and failure must be estimated. All paths in an HRA event tree should be defined as resulting in system success or failure in terms of their possible system consequences, not in terms of the specific human errors leading to these consequences. The system analysts will have identified the human-system interfaces to be analyzed in the HRA, but errors made in operating at these interfaces may not significantly degrade system reliability or safety. For example, an error made in manipulating a system-critical component may not result in system failure as defined by the system analysts. The human reliability analyst must point out potential human errors for a given set of tasks and then must quantify the probability of these errors; usually he does not, however, decide whether a given sequence through the HRA event tree will contribute to system success or failure.

At this point in the HRA, the system analyst could examine the HRA event tree for discrepancies between his understanding of the system and the human reliability analyst's representation of it. He should consider the implications of each path through the HRA event tree, then he should label each end point of the tree as a system success or failure. These end points should be

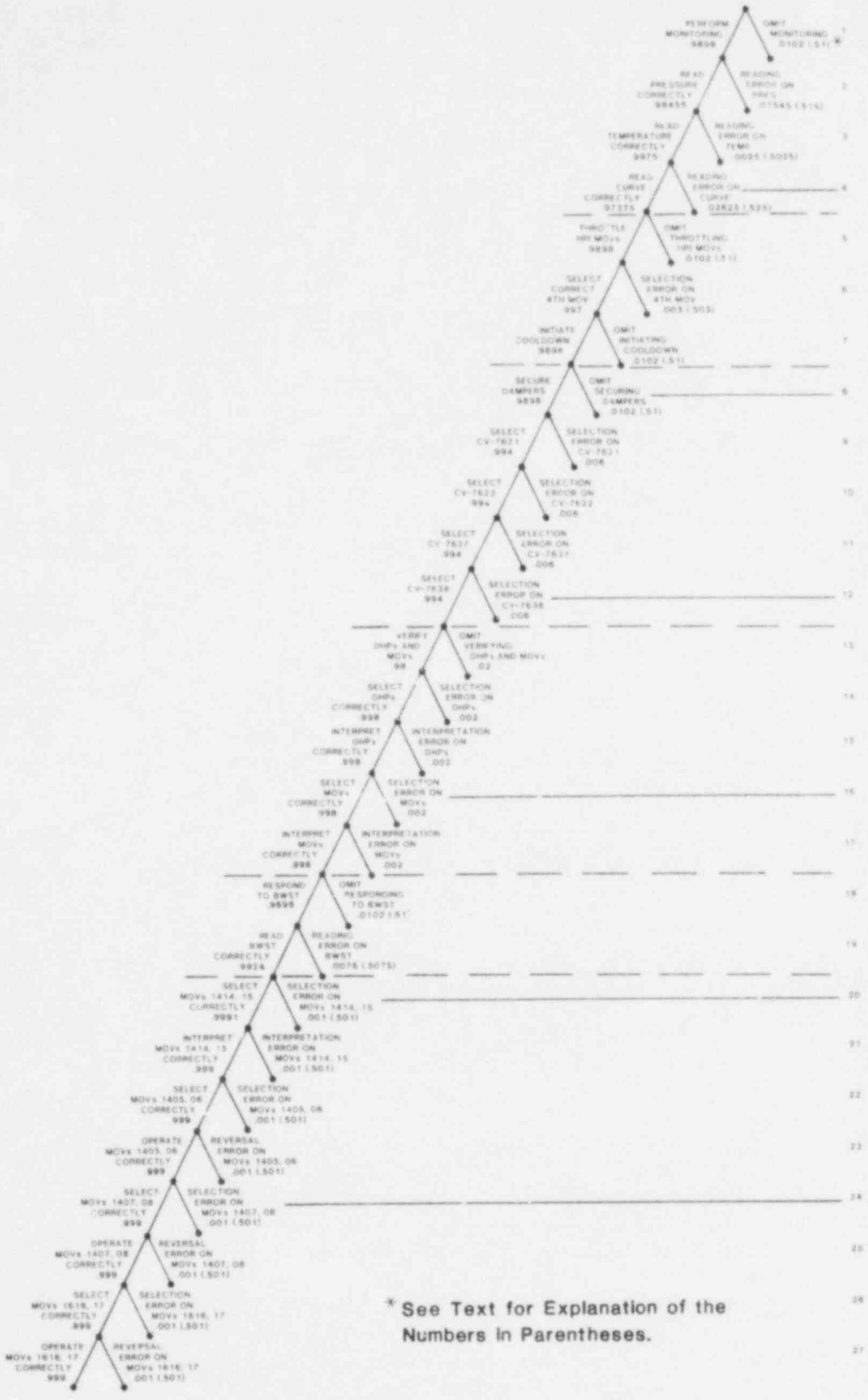
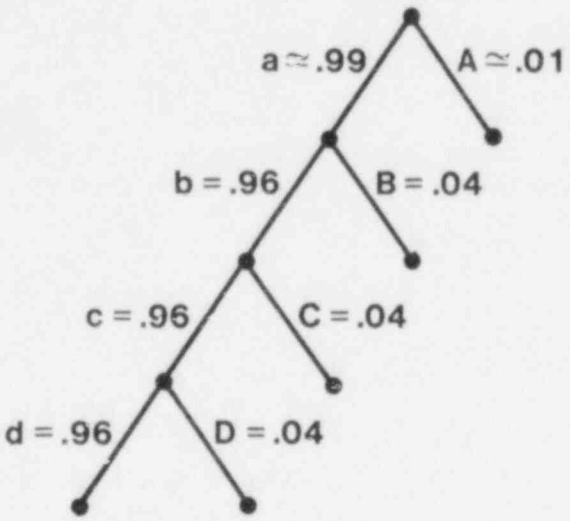


Figure 15 HRA event tree for actions by operators assigned to the control room with HEPs from Figure 13 modified to reflect dependence.



Event	HEP	Source
A = Control room operator omits ordering the following tasks	.01 (EF = 3)*	T20-6, #1
B = Operator omits verifying the position of MU-13	.04 (EF = 5)**	T20-8, #3
C = Operator omits verifying/opening the DH valves	.04 (EF = 5)**	T20-8, #3
D = Operator omits isolating the DH rooms	.04 (EF = 5)**	T20-8, #3

* Modified to reflect the effects of moderately high stress

** Modified to reflect the effects of moderately high stress and protective clothing

Figure 16 HRA event tree for actions performed outside the control room with HEPs from Figure 14 modified to reflect dependence.

quantified as probabilistic statements; the statements will be combined to formulate total system success and failure probabilities. This examination of the HRA event tree by the system analysts could be performed during the early stages of the HRA or during the initial screening of the system. It is done here for illustrative purposes.

5.10.2 Example

For Figure 15 (the analysis to this point of the actions performed by the control room operators), the system analyst made the following adjustments based on his decision as to whether given errors constituted contributions to system failure probabilities. He defined the paths through the HRA event tree ending in error events 1, 2, 3, 4, 7, 18, 19, 22, and 23 as system failure contributions and those ending in error events 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 20, 21, 24, 25, 26, and 27 as system success contributions. The implications of the accident at TMI-2 have great potential impact on error events 5 and 6, so they were removed from the analysis at this point, to be considered as a separate case.

For Figure 16, a similar decision was made by the system analyst. In this case, all of the paths through the HRA event tree terminating in a human error were determined to constitute contributions to system failure.

Once the decision has been made as to which paths through the HRA event tree result in system failure, human error contributions to total system success and failure probabilities can be quantified either of two ways. The first method is the simpler, requiring no redrawing of the HRA event trees. In it, the end points of the limbs on the existing HRA event tree are simply labeled as success or failure. All of the terminal success probabilities are summed to reach the total system success probability. The failure probabilities are obtained by the same method, or by subtracting the total system success probability from 1.0.

The second method is more complex and requires that the HRA event tree be redrawn. When error on a human task does not contribute to system failure, both limbs representing this task on the HRA event tree contribute to the probability of system success. Algebraically, the probability of 1.0 is being multiplied by the system success probability since the results of paths going through both limbs are combined into the system success probability. In effect, that error has no influence on system failure. Therefore, we need not even consider it since we are concerned with estimating the probability of human error contribution to the probability of system failure in a risk assessment. Those branches representing events the outcomes of which do not contribute to total system failure probabilities can be deleted from the HRA event tree altogether. The tree should be redrawn, diagramming only those events that have some effect on the probability of system failure. Figure 17 shows how the HRA event tree for actions performed by the control room operators is changed when this second method for quantifying total system success and failure probabilities is used.

5.11 Determine the Effects of Recovery Factors

5.11.1 Discussion

Complete analyses are performed for the dominant sequences that show up in the computer modelling of the fault trees. To save time and effort in the HRA,

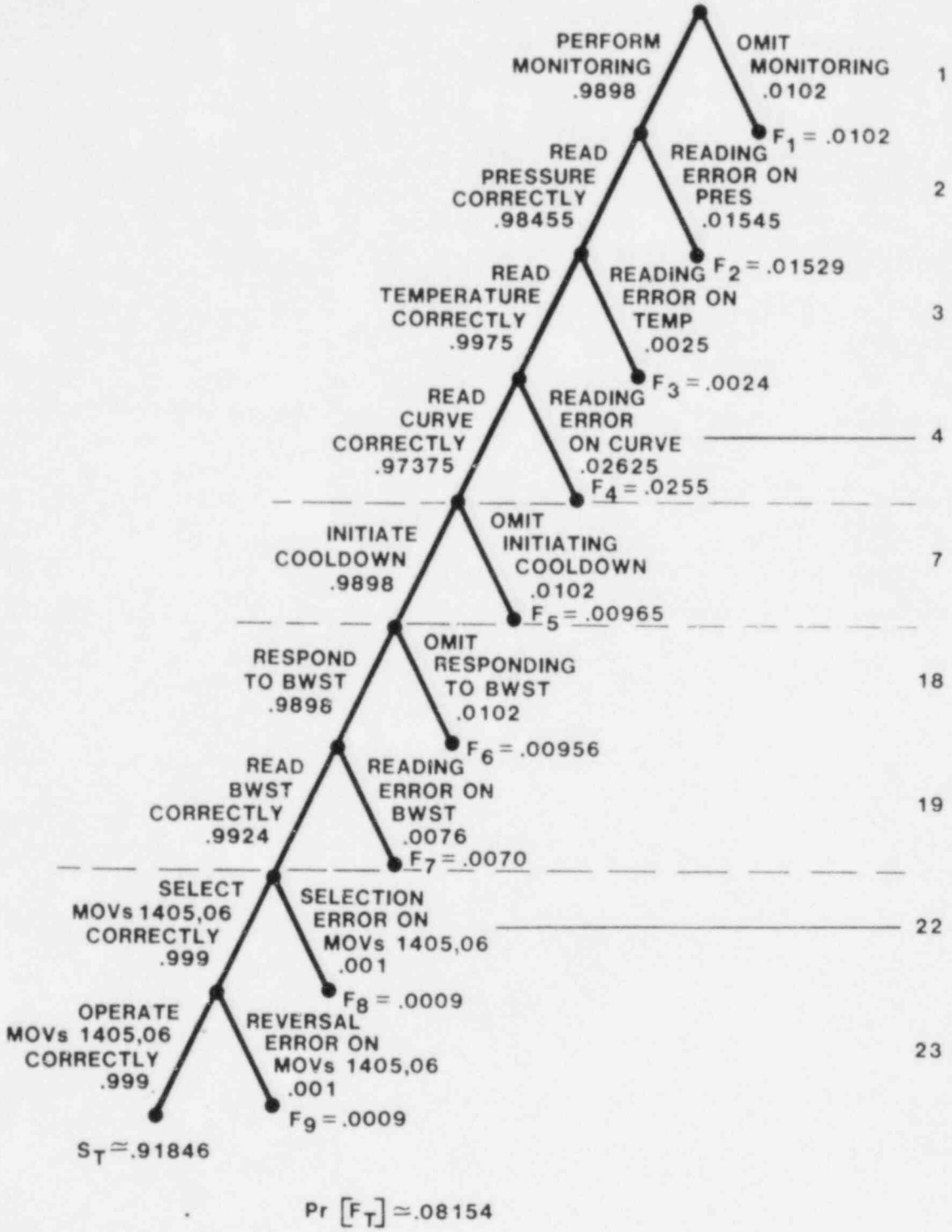


Figure 17 HRA event tree from Figure 15 for actions by operators assigned to the control room modified by second method for quantifying system success and failure probabilities.

consideration of the effects of recovery factors is delayed until it is determined if a given analysis is part of a potentially dominant sequence. The probability of system failure due to human error will certainly be higher when recovery factors are ignored than when they are included in the analysis. If a situation being analyzed does not appear as a potentially dominant sequence when this inflated system failure probability is used, there is no need to analyze it further. In fault tree terms, the frequency of an accident sequence can only be decreased by considering recovery factors.

To decrease the level of effort for the HRAs that must be performed for each plant, we recommend that recovery factors not be included in the preliminary analyses. Once potentially dominant sequences have been identified, recovery factors for each of them can be included for analysis to see whether a complete representation of human performance within the system as it operates will cause the potential dominance to disappear. This incorporation of recovery factors can be done in stages, the purpose of this being to decrease the amount of time required for each HRA. If there are five recovery factors operating for a given scenario, the human reliability analyst may choose to model only two of them at first. If the inclusion of these results in that sequence's ceasing to be potentially dominant, no more work need be done at this time. If this scenario still shows up as one of the system's potentially dominant sequences, the other three recovery factors should be analyzed.

Some recovery factors are highly situation-specific, while others can be applied generically. Alerting cues for recovery actions for any given transient will always depend on the specifics of the response requirements for that transient. However, when analyzing recovery factors operating after maintenance activities it will sometimes be possible to generate generic HRA event trees that can be applied without modification to every such case for that plant. This is possible because in many plants a single procedure dictates the steps to be followed in restoring components following maintenance. In either case, the recovery factor can take the form of a point value (an HEP) or of a separate HRA event tree. The point value or the total success probability of the recovery HRA event tree should be inserted on the associated error limb of the main HRA event tree. The probability of error for that limb is then multiplied by the success probability of the recovery HRA event tree and by the probabilities of the other events in that path to obtain the probability of recovery from the error. The end point of the original system failure path for that error is multipled by the failure probability for the recovery factor to obtain the probability of an unrecovered error.

5.11.2 Example

As mentioned earlier in the analysis, human redundancy as a recovery factor has already been analyzed for this problem so the quantification of the effects of dependence could be demonstrated. We can now consider cases in which the operator himself could catch his own errors, or in which another operator working at a later date could catch his errors. One such case would be during an inspection process such as the walk-around (see Chapter 19 of the Handbook). Since this problem deals with responding to an emergency, use of the walk-around as a recovery factor is inappropriate. It is also possible for the operator to catch his own errors when the situation provides some additional alerting cue either to the action that should be taken or to the error itself.

In this problem and from the procedures in Figure 3, we see that the operator should respond to the borated water storage tank (BWST) falling to the 6-foot level. His response is cued from two sources: if he is following the written procedures correctly, he will be monitoring the meter indicator of the BWST level; if he is not using the written procedures, there is still a possibility that the lo-lo-level alarm (annunciator) will remind him that he needs to perform the follow-up actions. We will treat the alarm as an additional alerting cue and analyze its effect as a recovery factor. From Chapter 20 of the Handbook, we need to find an estimate of an HEP pertaining to responding to an annunciator. Table 20-23 lists HEPs for failing to respond to one of any number of annunciating indicators. We have no exact information on this but will assume that, at this time into the transient, there are 10 annunciators alarming. From the table, the probability of the operator's failing to respond to any one of these 10 is .05 (EF = 5) (item 10k). Figure 18 shows the diagramming for this recovery factor (noted as RF [recovery factor] in the tree). Note that its inclusion in the analysis increased the unrounded probability of total system success from .91846 to .92745. If this is an adequate increase (if the sequence does not prove to be potentially dominant when using the success probability of .92745), no more recovery factors need be analyzed.

5.12 Perform a Sensitivity Analysis, If Warranted

5.12.1 Discussion

At times during the course of performing an HRA, the analyst will want to determine the effects of manipulating the values of one or more of the elements analyzed. He may do this because of some uncertainty he has about the assumptions he made, because the data he used are very uncertain (e.g., estimates of diagnosis errors by control room personnel), or because he has not been able to obtain detailed information about some set of PSFs he judges to be important determiners of the reliability of performing a task he has to analyze. Changing the assumptions of the analysis or changing the values of certain parameters may affect the probabilities of system success and failure. It may be of interest to manipulate these values to determine the effects of design, equipment, or procedure change before such changes are incorporated.

If the probabilities of some errors in an analysis are outstanding with respect to those of others, or if the system consequences of a given human error are significant, the analyst may want to see what effect lower probabilities for these errors would have. The HEPs can be decreased by the action of recovery factors (see Section 5.11) or by changing the characteristics of the task to reflect a less error-likely situation. These changes can be accomplished by improving human-system interfaces, by increasing feedback adequacy, or by upgrading the quality of associated procedural steps. The new, lower HEPs can be entered onto the HRA event tree, and the resulting differences in total system success and failure probabilities evaluated. Sensitivity analyses are extremely useful as tradeoff analyses of proposed design changes and in pinpointing areas of potential system improvement.

In performing best- and worst-case analyses (special types of sensitivity analyses) for a PRA, a bounding analysis can be executed as described in detail in the Appendix. For this exercise, two sets of HEPs are utilized and the results of the two HRAs compared. The upper and lower uncertainty bounds of the nominal HEPs for a given situation can be used, or two sets of assump-

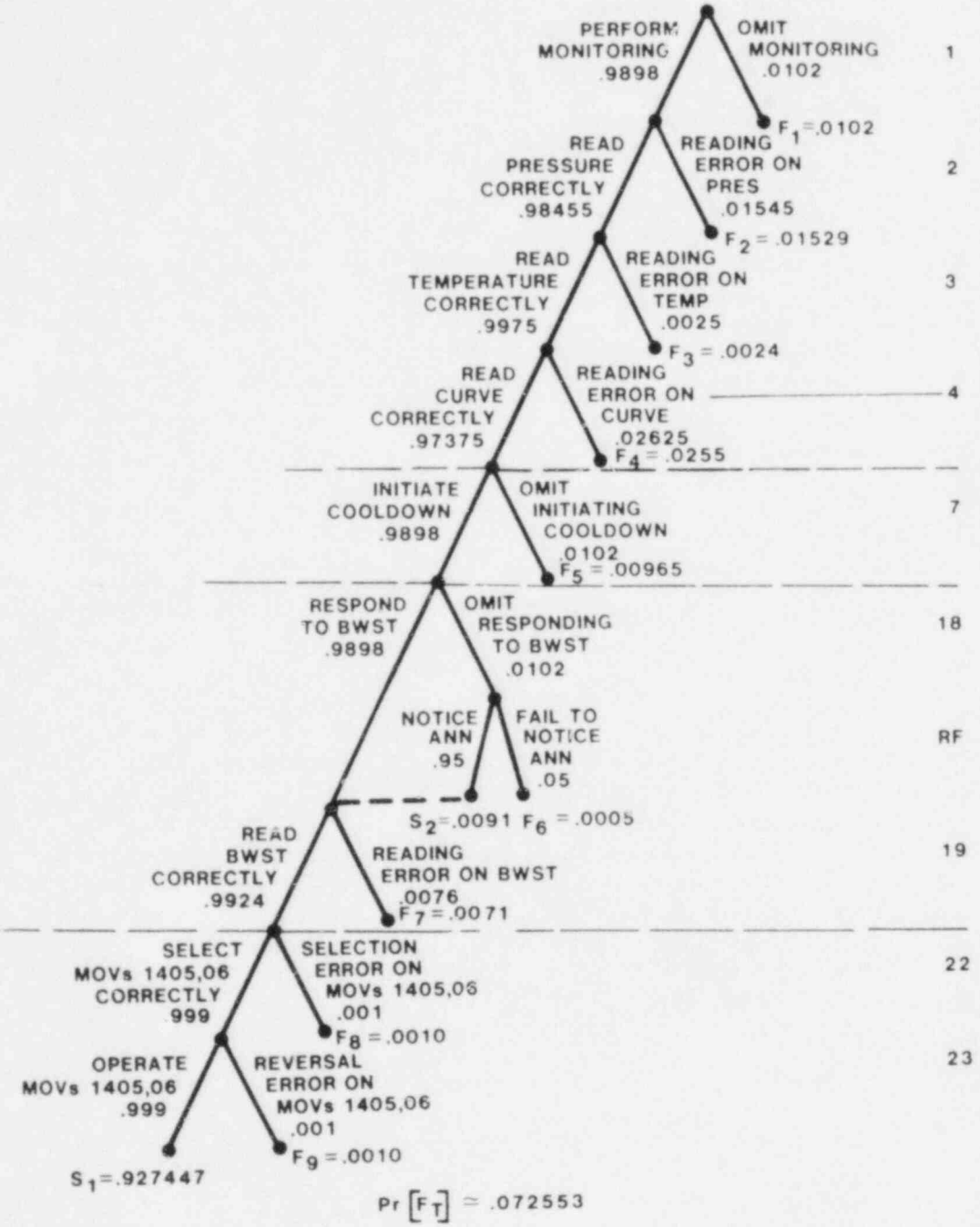


Figure 18. HRA event tree for actions by operators assigned to the control room, including one recovery factor.

tions and PSFs relating to the situation can be defined. The results of these two HRAs can be evaluated by entering them onto the appropriate fault tree to see how sensitive some part of the PRA is to the two sets of HEPs. For PRA, the criterion for evaluating the sets of results should be risk significance. If there is very little difference in outcome, the analyst may decide to select the more conservative set for inclusion in the final PRA, at least as a temporary measure. If the difference in outcome is considerable, he should take steps to obtain better data.

5.12.2 Example

In this problem, the two most important errors, in terms of their probabilities of occurrence, are numbers 2 and 4, reading errors on the RCS pressure chart recorder and the graph of the pressure/temperature curve. As a design tradeoff comparison, suppose we want to decide whether changing either or both of these tasks to result in lower task HEPs is worthwhile in terms of system success probability. The simplest change involves changing the nature of the displays themselves to make reading errors less likely. For RCS pressure, the display could be a digital meter instead of a chart recorder. From Table 20-10, items 2 and 3, we see that this would change the basic HEP for that task from the .006 (EF = 3), shown as failure limb 2 in Figure 11, to .001 (EF = 3). This new HEP must be modified to .005 (EF = 3) to reflect the effects of stress on a dynamic task, then modified again to reflect the effects of dependence, becoming .0025 rather than the .01545 shown as failure limb 2 in Figure 18. Recalculation of the total system success probability using .0025 instead of .01545 increases S_1 in Figure 18 from .9275 to .9396.

If we make the same sort of adjustment for error number 4 in Figure 18, we might redesign the graph so that it is comparatively easy to read. If we now use the lower bound of the HEP in Table 20-10, item 5, instead of the nominal value of .01, we have .003 (EF = 3). This becomes .015 when modified for stress and .0076125 when modified for human redundancy (high dependence). Modifying only this graph results in a total system success probability, S_1 in Figure 18, of about .9452.

For a larger increase in the total system success probability, we could analyze the effects of both changes. An HRA event tree incorporating these new values is shown in Figure 19. The total system success probability becomes .95763. Whether the new estimate of the probability of system success is large enough to warrant the incorporation of both changes is, of course, a management decision and can be made in terms of a cost/benefit analysis.

5.13 Supply Information to System Analysts

5.13.1 Discussion

All of the information used in performing the HRA, especially the assumptions made and the modified HRA event trees, should be presented to the system analysts. The human reliability analyst should then go over his analysis with them to ensure that there are no misunderstandings--no unresolved conflicts between the two concepts of the operating system. The system analyst should be familiar enough with the basic principles of HRA event tree diagramming so that he can use the HRA event tree itself to obtain the necessary inputs for his fault trees or event trees. He should be able to use the total system success and the failure probabilities, an HEP for a single item of equipment,

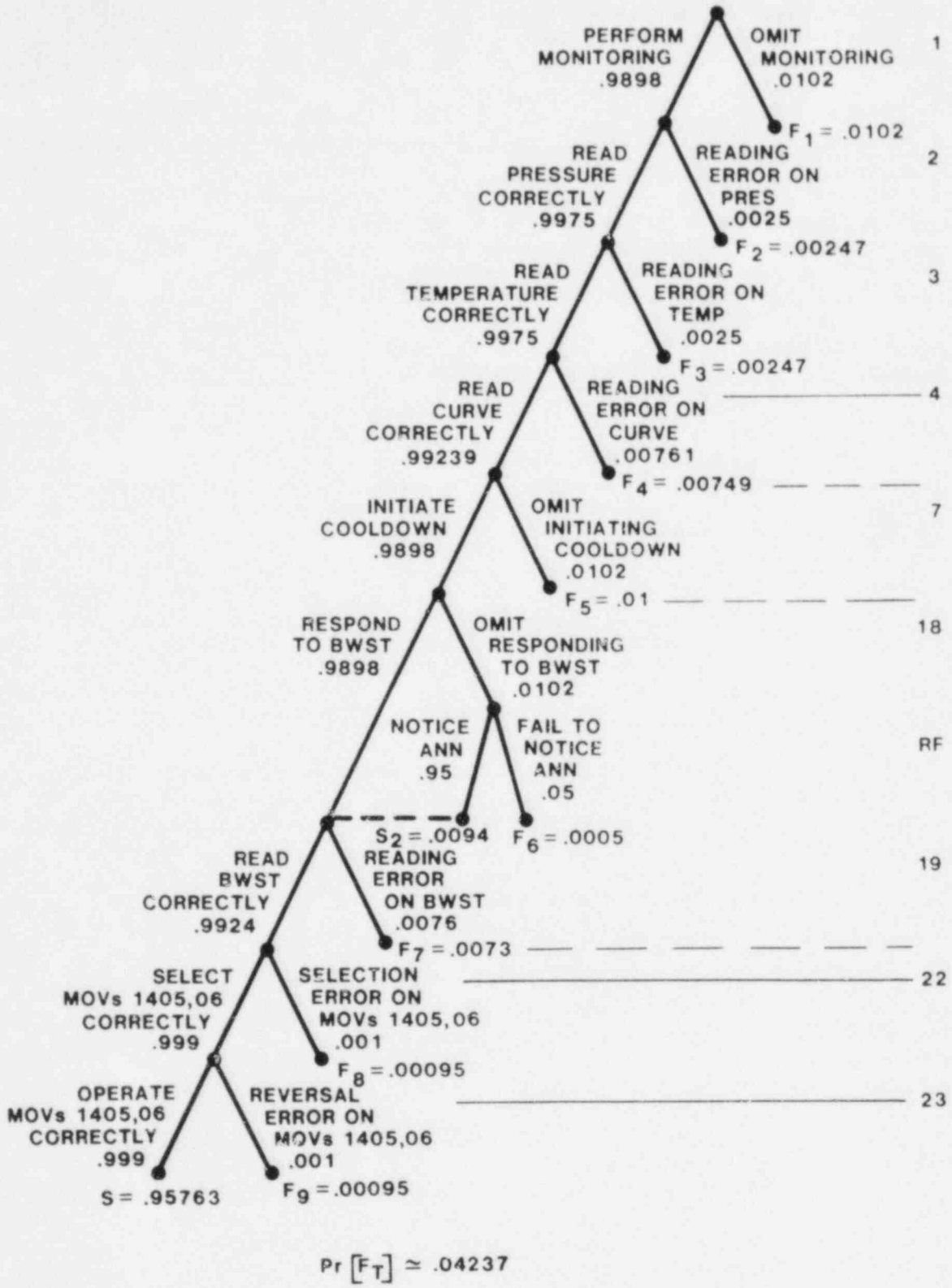


Figure 19 HRA event tree from Figure 18 for actions by operators assigned to the control room with tasks 2 and 4 modified.

or an HEP for a single error for a given piece of equipment. These values can be entered directly into the human error blocks of his fault trees or system event trees. Listings of the sources of the HEPs may be of interest to the system analysts but are not strictly necessary. Section 6 discusses the method for formatting this information so that it is usable.

Any dependence found by the human reliability analyst should be specifically indicated to the system analysts, especially in the case of dependence occurring between tasks performed on different items of equipment. When dependence exits because of two operators performing the same task, combined HEPs representing the performances of both are entered into the human error block of the fault tree--no change in the system fault tree model is necessary. When dependence exists between performances on different items of equipment, the fault trees must be modified to reflect this common mode failure. Identifying where and between which system elements the dependence exists will enable the system analyst to modify his models accordingly.

5.13.2 Example

If the system analyst needs an HSP for the entire scenario diagrammed in Figure 19, he should use the total system success probability, = .958. If he needs a value for all the possible human errors made in operating MOVs 1405 and 1406, he must consider all three of those errors diagrammed: the error of omission for the entire step (18) including the annunciator recovery factor (RF), the selection error (22), and the reversal error (23). In effect, the combination of these errors represents a small HRA event tree. The system analyst must use the product of the success probabilities for each error event (.9995 x .999 x .999 = .998) as the probability of success on those components. If the system analyst were only interested in the likelihood of an error of omission when dealing with MOVs 1405 and 1406, he would use the HEP for that specific error, .0102. The human reliability analyst should point out to the system analyst that MOVs 1405 and 1406 are completely dependent for all errors considered in the analysis. They (as a perceptual unit) are also dependent on the monitoring task (1)--certain kinds of equipment failure of the BWST meter, if not noticed, could result in an error on MOVs 1405 and 1406.

6.0 METHODS OF DOCUMENTATION

The results of the HRA go directly into the system analysis as probability statements. The only information from the HRA used in the rest of the PRA are the HEPs for given error events or for total system success and failure probabilities and the information on where and what kind of dependence exists. The most important part of any final report for an HRA is the cataloging of the HEPs on a per item (of equipment) or a per step basis, depending on the level of detail of the fault trees and the system event trees and the pinpointing of existing dependence. Other information included in the final report is not necessary as an input to the analysis itself but is instead necessary as a reference on the performance of any particular HRA.

The purpose of this procedure is to ensure the similarity of the PRAs performed for each of the several plants using the guidelines outlined in the Handbook. The additional material to be included in the final report for each analysis will provide points of reference that can be used to evaluate the

similarities of the HRAs. This similarity must be established if the results from different plants are to be compared to allow us to make relative statements about risk across plants.

Other human reliability analysts must be able to trace through your analyses and to understand them fully. To provide them the information necessary to accomplish this, they must have access to that material on which the HRA was based. A set of the written procedures analyzed or of your written version of the "standard operating procedures" should be included along with the assumptions made in your definition of the situation under which the procedure would be performed. These assumptions will have been made during your visit to the plant and during the talk-through of the procedures with plant personnel. A copy of the final HRA event tree resulting from the analysis should be included. The basic HEP used for each limb and its source as well as the source for any modifications (PSFs, dependence) you made should be included. These can be included as columns in the table of the task analysis: this is a clear, concise method for presenting a definition of the error events found in the HRA event tree. If recovery factors were considered or a sensitivity analysis performed, the outcome of these should be included.

In short, the final report should include all information necessary for the system analyst to check his assumptions about the performance situation against yours. It should also include sufficient information so that another human reliability analyst could perform an HRA for the same scenario and arrive at a similar result.

7.0 DISPLAY OF FINAL RESULTS

As mentioned in Section 6, the most efficient method for displaying the results of an HRA is to use the task analysis format shown in Figures 6 and 7. These tables can be expanded to include the other information necessary for complete documentation of the HRA. This has been done for the example that was worked in this chapter in Figures 20 and 21. With these tables and copies of the HRA event trees, the system analysts should be able to take information in any form or at any level needed for input into the fault trees or event trees. The expanded task analysis tables, HRA event trees, list of assumptions, and copy of the procedure should provide sufficient documentation for an HRA.

This type of complete documentation of an HRA is important for PRAs to be performed at various times in the life of a plant. As the plant equipment, manning, or operations change over time, the PRAs reflecting the different assumptions become points of comparison for the effects of these changes.

STEP	EQUIPMENT	ACTION	INDICATION	LOCATION	NOTES	ERRORS	EVENT TREE*	HEP	T,1**	FINAL***
D.2	RCS pressure	Monitor		CB4		Omission (all)	1	.01	7, 4	.0102
						reading	2	.006	10, 3	.01545
	RCS temperature	Monitor		CB4		Reading	3	.001	10, 2	.0025
	heater switches	Maintain pres. & temp.	Within curve on chart	CB4		Reading	4	.01	10, 5	.02625
D.4	4 HPI MOVs	Override & throttle		CP16, CP18	ESF	Omission (all)	5	.01	7, 4	.0102
						selection (1)	6	.003	12, 2	.003
		Initiate cooldown	P1.Pr.12			Omission	7	.01	7, 4	.0102
D.7.3	CV-7621,22,37,38 (room purge dampers)	Secure	Close switches	Ventilation Room		Omission (all)	8	.01	7, 4	.0102
						selection (each)	9,10,11,12	.003	12, 2	.006
D.7.4	DH pumps	Verify on	Indicator lamps	CP16, CP18	ESF	Omission (for MOVs too)	13	.01	7, 4	.02
						selection	14	.001	12, 3	.002
						interpretation	15	.001	11, 8	.002
	MOV-1400, 1401	Verify open	Indicator lamps	CP16, CP18	ESF	Selection	16	.001	12, 3	.002
						interpretation	17	.001	11, 8	.002
D.9	BWST	Monitor	>6 feet	CP14		Omission	18	.01	7, 4	.0102
						reading	19	.003	10, 1	.0076
	MOV-1414, 1415	Verify open	Indicator lamps	CP16, CP18	ESF	Selection	20	.001	12, 3	.001
						interpretation	21	.001	11, 8	.001
	MOV-1405, 1406	Open	MOV switches	CP16, CP18	ESF	Selection	22	.001	12, 3	.001
						reversal	23	.001	text	.001
	MOV-1407, 1408	Close	Switches	CP16, CP18	ESF	Selection	24	.001	12, 3	.001
						reversal	25	.001	text	.001
	MOV-1616, 1617	Close	Switches	CP16, CP18	ESF	Selection	26	.001	12, 3	.001
						reversal	27	.001	text	.001

*The numbers in this column do not usually appear in a task analysis; they have been included for the reader's convenience. They refer to the error event numbers appearing in HRA event trees starting with Figure 9.

**These numbers refer to table and item numbers from Chapter 20 of the Handbook.

***The nominal HEPs have been modified to reflect the effects of a moderately high stress level and (in some cases) high dependence between two operators.

Figure 20 Display of final results using task analysis table for actions by operators assigned to the control room.

STEP	EQUIPMENT	ACTION	INDICATION	LOCATION	NOTES	ERRORS	EVENT TREE*	HEP	T,I**	FINAL***
D.7.1	MU-13	Verify closed	Position	Stairwell outside MU Pump Room	Only valve	Omission	2	.01	8, 3	.04
D.7.2	DH-7A, 7B	Open	Position	Outside DH Pump Rooms		Omission (for all D.7.2)	3	.01	8, 3	.04
	MU-14, 15, 16, & 17	Verify open	Position	DH Pump Rooms						
	MU-23, 24, 25 &26	Verify open	Position	DH Pump Rooms						
D.7.3	ABS-13, 14	Close	Position	Outside DH Room	Only valve	Omission (for all D.7.3 here)	4	.01	8, 3	.04
	Watertight doors	Close	Locks in place	DH Rooms						

*The numbers in this column do not usually appear in a task analysis; they have been included for the reader's convenience.

**These numbers refer to table and item numbers from Chapter 20 of the Handbook.

***The nominal HEPs have been modified to reflect the effects of a moderately high stress level and (in some cases) high dependence between two operators.

Figure 21 Display of final results using task analysis table for operations by operator outside control room.

APPENDIX

Sample Human Reliability Analysis Problems

Based on problems devised by
the authors and H. E. Guttmann,
Sandia National Laboratories,
as modified by M. Weinstein
and M. E. Fitzwater, Human
Performance Technologies, Inc.

PREFACE

This appendix presents the same set of problems used in our Handbook Exercises Project, performed under our direction by Human Performance Technologies, Inc. Approximately 30 individuals, both U.S. and foreign, participated in the study. They included reliability analysts, whose familiarity with human performance technology ranged from little to considerable, and human factors specialists, whose familiarity with reliability analysis ranged from zero to considerable. The results of this study are presented in SAND82-7056.[11] The study was used as one source of inputs for the final versions of NUREG/CR-1278[1] and the present document.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

LIST OF FIGURES

LIST OF TABLES

APPENDIX

SAMPLE HUMAN RELIABILITY ANALYSIS PROBLEMS

1. INTRODUCTION

1.1 Purpose and Organization of Exercises

The purpose of the following exercises is to familiarize you, the presumed reliability analyst, with the use of Chapter 20 of the Handbook[1] in performing a quantitative analysis of human reliability in a practical situation. (Additional exercises are found in Chapter 21 of the Handbook, including a problem illustrating use of the Nominal Diagnosis Model.) The exercises in this appendix are greatly simplified descriptions of real-world situations. In a real-world setting, you, as the analyst, will observe many aspects of any situation that will not be mentioned in the exercises. Some of the aspects you observe will not affect reliability and safety, whereas others may have significant effects, and you will have to judge which ones should be included in your analysis. In the exercises that follow, only the most relevant factors are listed. The exercises are hypothetical presentations of generic problems. They are not representative of any specific situation at any specific nuclear power plant (NPP). You should keep in mind that, when equipment is mentioned, your primary concern, for HRA purposes, is not with the system function of the equipment but rather with the operator interface. (Obviously, in the context of the entire PRA, system functioning is vital information.) Thus, for HRA purposes, in the case of a motor-operated valve (MOV), this interface is a switch in the control room; for a locally operated valve, it is a turning wheel at the valve site.

This appendix is divided into four sections: an introduction, a set of two example exercises with suggested answers, a set of four problem exercises for you to work out, and, finally, suggested answers for these four problems. Following are some additional comments about Sections 2, 3, and 4:

1.2 Example Exercises (Section 2)

Section 2 consists of two completed exercises that illustrate how to use the Handbook and some worksheets in developing the solutions. The worksheets were developed to aid in the solving of human reliability problems and to keep a record of the rationale for using particular estimates of human error probabilities (HEPs). Without such a record, the analyst will often forget why he made certain estimates. With a record, he can document the need to make changes in subsequent analyses when changing situations warrant changes to prior solutions.

1.3 Problem Exercises (Section 3)

Section 3 consists of four exercises that you are to work out. Each section contains the instructions necessary to complete the required work.

The following supplementary notes are provided to aid in the completion of the problem exercises.

Note 1: Some of the exercises use the following equations from Chapter 9, "Unavailability," in the Handbook.

$$U = \frac{p\bar{d}}{\bar{T}} \qquad \text{(Eq. 9-1)*}$$

$$A = 1 - U = \frac{\bar{u} + \bar{d}(1 - p)}{\bar{T}} \qquad \text{(Eq. 9-2)}$$

$$p = ER \qquad \text{(Eq. 9-3)}$$

$$\bar{d}_t = h_1 + C_1 h_2 + C_1 C_2 h_3 + \cdots + C_1 C_2 \cdots C_{m-1} h_m \qquad \text{(Eq. 9-4)}$$

where

A = Availability--the probability that a component or system is operating or will operate satisfactorily if called on

U = Unavailability--the probability that a component or system is inoperable or will not operate if called on ($U = 1 - A$)

p = The probability that an unrecovered human error results in a component being in the failed condition

$\bar{d}$ = Mean downtime--the average time the component or system is unable to operate within a given time period, given that a human error has induced a failed condition

$\bar{T}$ = The time period of interest when estimating unavailability

$\bar{u}$ = Mean uptime--the average time that a component or system is operating or able to operate within a given time period; $\bar{u} = \bar{T} - \bar{d}$

E = Probability of committing the error per act

---

*The equation numbers are from Chapter 9 of the Handbook.

R = Probability of failing to recover the error at or about the time the error is committed

$\bar{d}_t$ = Total mean downtime--the sum of the $\bar{d}$ values for the time periods between the first test and the first check, between all subsequent checks, and between the last check and the next test

h_1, h_2, h_3, h_m = The number of hours (or any other time unit) between the first test and the first check, the first check and the second check, the second and third checks, and the last check and the next test, respectively

C_1, C_2, C_{m-1} = The probabilities of nondetection of the error at the first, second, and last checks performed between the two tests, respectively

Note 2: The figures and tables in this appendix begin with A-. All references to other figures and tables are to those in the Handbook. For example, Table 20-5, #1, refers to the first HEP and associated error factor (EF) in Table 20-5 in the Handbook. In this appendix, we represent the Handbook EFs as uncertainty bounds (UCBs). The lower UCB is calculated by dividing the Handbook HEP by the EF, and the upper UCB is calculated by multiplying the HEP by the EF. Thus, a Handbook HEP stated as .001 (EF = 3) is stated in this appendix as .001 (.0003 to .003). Rounding is used to maintain a total range ratio of 10 between the lower and upper UCBs when the EF is 3. Rules for assigning EFs are provided in Table 20-20. For further discussion, see Chapter 7 in the Handbook.

Note 3: Chapter 16 in the Handbook describes the importance of administrative controls, i.e., the kinds of checking of human performance mandated in a plant and the extent to which plant policies are carried out and monitored, including tagging controls and lock and key controls for valves and other components. One of the most serious errors that could be made in a human reliability analysis of a specific plant is to assume, without investigating, that all plant policies will invariably be carried out. It is noted in Chapter 16 of the Handbook that since there is ample history in NPPs of valves left in inappropriate positions having affected the availability of safety systems, the user must evaluate the probability that NPP personnel will not faithfully follow plant policies and procedures. A probability of .99 that every person in an NPP intends to carry out plant policies and procedures (whether or not he makes errors of omission or commission in carrying out this intent) would indicate a plant with reasonably good quality control.

1.4 Candidate Solutions for Problems 3 through 6 (Section 4)

The solutions are considered "candidate" solutions since they are based on the situations described in Section 3, and, as was stated earlier, not all of the performance shaping factors (PSFs) were considered. In any given plant, the PSFs might be different--in some cases, markedly different. At some plants, for example, the recovery factors for certain classes of error are so well designed and implemented that the probability of an unrecovered error will be relatively small compared with other plants where considerable and nearly exclusive reliance is placed on individuals' not making errors in the first place.

2. EXAMPLE EXERCISES

Review the two example exercises contained in this section. Familiarize yourself with the format of the exercises and the application of the Handbook data to their solutions. Note how the Problem Worksheet and the Event Tree Worksheet are used. Table A-1 provides instructions for the use and interpretation of the Problem Worksheet (Figure A-1), provided below.

Table A-1 Instructions for using problem worksheet

---

1. Exercise No./Problem No. -- Identify exercise and problem.
2. Performance Shaping Factors -- The use of these entries is optional. The problem scenarios frequently describe Performance Shaping Factors (PSFs) that affect the performance of an entire procedure. These factors, in turn, affect the selection and use of tables in Chapter 20 of the Handbook. A record of these general PSFs on the worksheet will serve as a reminder and facilitate the completion of the remainder of the worksheet.
3. Written Procedure Step No. or Task Description -- Record the Task or Step No. and/or enough information to aid recall of the content of the action.
4. Dependence -- If applicable, record the level of dependence between the actions stated. Enter ZD, LD, MD, HD, and CD for zero, low, moderate, high, and complete dependence, respectively.
5. Potential Error -- Enter a brief description of the error(s) that could be committed by someone performing the step or action.
6. Table Number and Item Number -- Identify the table number and item number from the Handbook that are used to obtain the HEP associated with the error.
7. Tabled HEP -- Record the HEP and its lower and upper uncertainty bounds (UCBs), as calculated from the tabled error factor (EF).
8. Stress/Skill Factor -- Record multiplier of HEP as a result of the combined stress/skill level associated with performance of the task described in the step or action.
9. Adjusted HEP --
   a. Record the value of the HEP multiplied by the stress weight, or
   b. If you disagree with the tabled HEP (Column 7), record the new estimated HEP.
10. Comments -- If you disagree with the Handbook values or models related to the errors described in Column 5 (e.g., HEPs, uncertainty bounds, dependence value, stress/skill weights), identify the basis of your disagreement (judgment or related data). Possible sources of related data might be experimental studies, power-generating industry reports, findings from other industries, etc.

PROBLEM WORKSHEET

Page___of___

1. Exercise No._____ Problem No._____ Analyst_____

2. Performance Shaping Factors:

Instruction		Experience		Stress Level		Tagging Level	
Written:		≤6 months	____	Low	____	1	____
≤10 items	____	>6 months	____	Optimum	____	2	____
>10 items	____			Mod. High	____	3	____
Oral	____			High	____	NA	____
None	____						

3. Written Procedure Step No. or Task Description	4. Dependence	5. Potential Error	6. Table No. & Item No.	7. Tabled HEP & UCBs	8. Stress/ Skill Factor	9. Adjusted HEP	10. Comments*

*Cite studies, if available, to back up any disagreement with the stated HEP and EF in the Handbook.

Figure A-1 Worksheet to be used for exercises #3 through #6.

2.1 Exercise #1. Monthly Test of Diesel Generator

2.1.1 Background

The diesel generator test is a routine test performed under optimal stress. It is performed by an experienced auxiliary operator who is directed to perform it by the shift supervisor. The probability of the supervisor's failing to order the test will be disregarded. The area of concern is the influence of human actions on the post-test availability of the diesel generator (DG), not the mechanical reliability of the component. Assume that the generator is already in the automatic start mode and that it will start upon receipt of a start signal. Note that the performance of the generator during the 2-hour test does not affect the probability that the component will start if called on--only the start mode status (automatic or manual) affects this probability. Therefore, consider the probability that the operator has left the component in the manual start mode instead of returning it to the automatic mode.

2.1.2 Task Description

Exercise #1 is based on the written operating procedures of an NPP. The actual procedures include some plant-specific instructions which have been omitted from the condensed procedures shown in Figure A-2.

2.1.3 Problem

In evaluating the performance of the test, address two questions:

(1) What is the probability that the diesel generator will fail to start if it is called on after the test?
(2) What additional recovery factors do you recommend?

2.1.4 Performance Shaping Factors

(1) The task is routine and the stress level optimal; i.e., normal.
(2) The task is performed by an experienced auxiliary operator.
(3) Written procedures with checkoff provision and having more than 10 items in the list are available.
(4) There is no checking by another person.
(5) The only indication of start mode status is at the diesel generator.

2.2 An Approach to Exercise #1

First we will discuss the failure of the DG to start. If the test is not carried out at all, the availability of the generator is unaffected by human actions. If the test is carried out, the availability of the component after the test will depend almost entirely on whether step 4.7 in Figure A-2 is carried out. Given the preceding PSFs, we have defined (see Figure A-3) five human error events: (1) failure to use the written procedure, (2) omitting step 4.7 when the procedure is not used, (3) failure to use the checkoff provision properly, (4) omitting step 4.7 when the checklist is used improperly, and (5) omitting step 4.7 when the checklist is used properly. The HRA event tree for this portion of the exercise, which illustrates the five human error events previously defined, is shown in Figure A-4.

EMERGENCY DIESEL GENERATOR NO. 3

INITIALS

1.0 Purpose

1.1 To determine that the emergency diesel generators will respond promptly and properly every month.

2.0 Initial Conditions

_____ 2.1 Normal station operation will not be affected by this test.

_____ 2.2 Unit will be at stable operating conditions with no anticipated large load changes or shutdown.

_____ 2.3 The "No. 1 and No. 2" diesel will be ready for automatic start-up and placed in standby.

_____ 2.4 Reference Initial Conditions and use OP-6 to perform this check.

_____ 2.5 Verify that this test is to be performed on Unit 1.

3.0 Precautions

_____ 3.1 Reference Precautions in OP-6.

_____ 3.2 Advise Shift Supervisor to notify system operator that the load will be put on the system at Step 4.

4.0 Instructions

_____ 4.1 Start the emergency diesel generator by following OP-6.

_____ 4.2 Advise the Shift Supervisor to notify the system operator that the diesel generator will be synchronized onto the system.

_____ 4.3 Manually synchronize the diesel with other power sources and assume load on diesel up to 2750 kW.

_____ 4.4 After approximately two (2) hours of operation, notify the system operator that the diesel will be shutdown.

_____ 4.5 Stop the diesel as stated in OP-6.

Figure A-2 Procedures for monthly test of emergency diesel generator (page 1 of 2).

INITIALS

_____ 4.6 Notify the electrical maintenance department that the test is complete.
Operator

_____ Personnel from this department must verify that the mechanical terminal connections are tight on the voltage regulator. The individual making the check shall initial the space provided to indicate that he has made the verification.
Electrician

_____ 4.7 Verify that the diesel is set for automatic start when the test is complete.

_____ 4.8 Notify the Shift Supervisor that the test is complete.

Completed By_____

Date_____

Figure A-2 (Continued) Procedures for monthly test of emergency diesel generator (page 2 of 2).

PROBLEM WORKSHEET

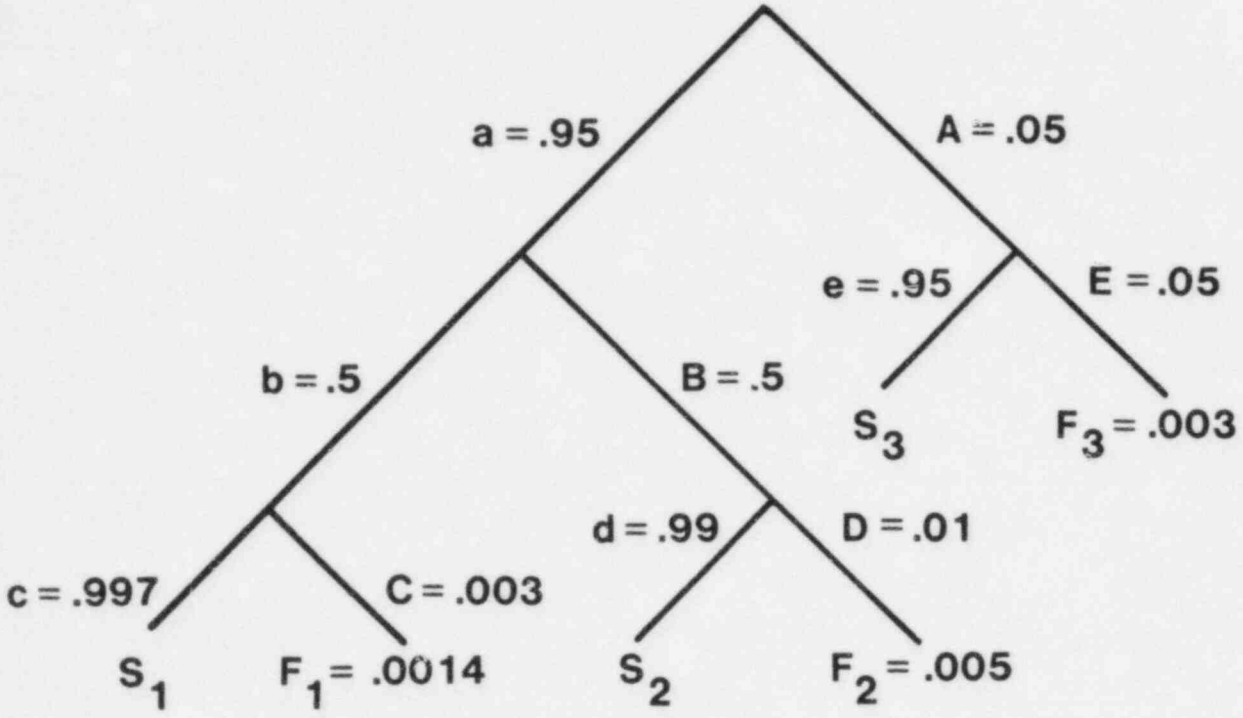
1. Exercise No. 1 Problem No. 1a Analyst

2. Performance Shaping Factors:

Instruction		Experience		Stress Level		Tagging Level	
Written:		≤6 months		Low		1	
≤10 items		>6 months	X	Optimum	X	2	
>10 items	X			Mod. High		3	
Oral				High		NA	X
None							

3. Written Procedure Step No. or Task Description	4. Dependence	5. Potential Error	6. Table No. & Item No.	7. Tabled HEP & UCBs	8. Stress/ Skill Factor	9. Adjusted HEP	10. Comments
4.7 Verify diesel set for auto start	ZD	A. Failure to use written procedure.	20-6 #6	.05 (.01 to .25)			
		B. Failure to use checkoff provision properly.	20-6 #8	.5 (.1 to 1.0)			
		C. Omit step 4.7, long list, checkoff used properly.	20-7 #2	.003 (.001 to .01)			
		D. Omit step 4.7, long list, checkoff used improperly.	20-7 #4	.01 (.003 to .03)			
		E. Omit step 4.7, procedures not used.	20-7 #5	.05 (.01 to .25)			

Figure A-3 Worksheet for event tree for restoring diesel generator to automatic mode after test.



$$\Pr[F] = (.05 \times .05) + (.95 \times .5 \times .01) + (.95 \times .5 \times .003)$$

$$= .0025 + .00475 + .001425$$

$$= .008675 \simeq .009$$

Figure A-4 HRA event tree for restoring diesel generator to automatic start mode after test.

The estimated HEPs and uncertainty bounds (UCBs) for the events in Figure A-3 involving the correct or incorrect use of procedures are found in tables in Chapter 20 of the Handbook as noted in the figure. The probability of failure to use the procedures is also found in Chapter 20. Summing the three failure paths (F_1, F_2, and F_3) from Figure A-4 yields a probability of .009 that the diesel generator will be left in the wrong state and will not be available if called on. We assume that the error will be detected the next time the generator is tested, therefore, $\bar{d} = \bar{d}_t = 720$ (30 days times 24 hours) and $\bar{T}$ also equals 720. Since $\bar{d}$ and $\bar{T}$ are equal, the unavailability, U, numerically equals p, the probability of the original error. The unavailability of the component can be calculated using Eq. 9-1:

$$U = \frac{.009 \times 720}{720} = .009$$

If an inspection is made in the middle of the month (360 hours after the completion of the test), with an HEP of .05 for the inspection (from Table 20-22, #3 from the Handbook), $\bar{d}_t$ will change as follows, using Equation 9-4:

$$\bar{d}_t = 360 + (.05 \times 360) = 378 \text{ h}$$

and

$$U = \frac{.009 \times 378}{720} = .004725 \simeq .005$$

Note that in preparing the HRA event tree, we used the tabled value of .5 for the probability that the checkoff requirements of the written procedures would not be followed properly. This is the value to use when no more information is available than was furnished here. In an actual situation, you might observe that the administrative control is excellent and judge that the probability of improper use of the checkoff provisions is much lower than the Handbook value of .5. On the other hand, in a plant with very poor administrative control, a value greater than .5 might be appropriate. Obviously, you would use the value that seemed to be most realistic.

In addressing the second question (What additional recovery factors do you recommend?), several approaches are feasible. The most obvious is that of providing human redundancy by requiring a second person to verify the status of the diesel shortly after completion of the test. If performed in response to an oral instruction as an individual task, the HEP for this checking task will be quite small. Let us assume that the supervisor is supposed to designate a second operator to check the switch--there is a probability of .01 that the supervisor will not do so (Table 20-6, #1). The designated operator will be carrying out a verbal order, indicating an HEP of .001 for errors of omission (Table 20-8, #1a). The probability of his making a discrimination error is .05 (Table 20-22, #3). The high HEP of .05 is based on the checker's high expectancy that the switch will be in the correct position, so there will be a tendency for him to "see" the switch in the correct position even if it is in the incorrect position. Thus, the probability that an incorrect switch status will be noticed by a checker can be illustrated by the worksheet in Figure A-5 and the HRA event tree in Figure A-6.

PROBLEM WORKSHEET

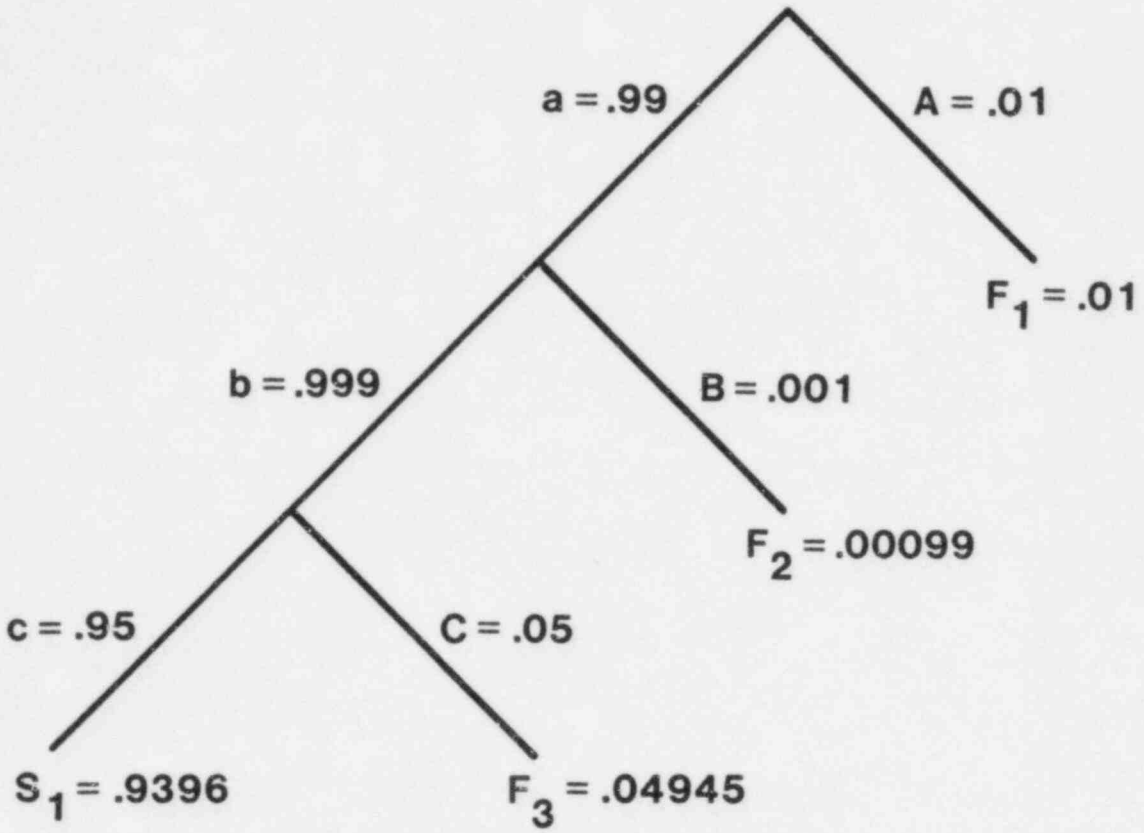
1. Exercise No. 1 Problem No. 1b Analyst _____

2. Performance Shaping Factors:

Instruction		Experience		Stress Level		Tagging Level	
Written:		≤6 months		Low		1	
≤10 items		>6 months	X	Optimum	X	2	
>10 items				Mod. High		3	
Oral	X			High		NA	X
None							

3. Written Procedure Step No. or Task Description	4. Dependence	5. Potential Error	6. Table No. & Item No.	7. Tabled HEP & UCBs	8. Stress/ Skill Factor	9. Adjusted HEP	10. Comments
Verify diesel set for auto start.	ZD	A. Supervisor fails to order 2nd oper. to check status switch.	20-6 #1	.01 (.003 to .03)	--	--	--
		B. 2nd oper. fails to check status of switch.	20-8 #1	.001 (.0003 to .003)	--	--	--
		C. 2nd oper. fails to recognize an incorrect status (if incorrect).	20-22 #3	.05 (.01 to .25)	--	--	--

Figure A-5 Worksheet for development of HRA event tree for additional checker for test procedures shown in Figure A-2.



$$\Pr[F] = (.01) + (.99 \times .001) + (.99 \times .999 \times .05)$$

$$= .01 + .00099 + .04945$$

$$= .0604 \simeq .06$$

Figure A-6 HRA event tree for addition of a checker for test procedures shown in Figure A-2.

Summing the failure paths (F_1, F_2, and F_3) for the recovery factor tree yields a failure probability of .014. Assuming that there are no additional checks on the diesel's automatic start status other than that of the auxiliary operator who performs the test and that of the second operator who checks the status soon after completion of the test, the probability that the diesel generator will be left unavailable after the completion of the test (given in recovery factor of human redundancy) is U = .009 x .06 = .00054. Thus, the assignment of a second operator to serve as a checker will reduce human unreliability by a factor of 17; i.e., .009 ÷ (.009 x .06) = 17. Keep in mind that this sizeable reduction in human unreliability is based on the issuance of an oral instruction by the checker's supervisor. Ordinarily, the incorporation of human redundancy in the form of a checker will not result in such a substantial reduction in the probability of an unrecovered error.

2.3 Exercise #2. Periodic Pump Test

2.3.1 Background

This exercise involves the monthly test of a high-pressure injection pump, part of the Emergency Core Cooling System (ECCS). The major concern is that the system tested be available for use after the test is completed (restored to operating condition). The test requires that the pump be valved out of (isolated from) the ECCS and tested. The valves are then restored so that the pump is again available for ECCS use. This exercise requires that the position of three valves be changed: two motor-operated valves (MOVs) and one large locally operated valve (see Figure A-7). The switches for the MOVs and for the pump are located in the control room.

2.3.2 Task Description

A hypothetical procedure for the monthly test is presented in Figure A-8. Note that errors committed on steps 1 through 6 in the procedure will not affect the posttest availability of the system. Such errors will only invalidate the test. For example, an error of omission on step 1 would prevent the carrying out of step 4, and errors of omission or commission on steps 1 through 6, such as operating a wrong valve, would also result in a bad test. However, only steps 7 through 9 are crucial for the availability of the system after the test; therefore, the analysis should begin with step 7. (We assume that if, in performing steps 7 through 9, the operator notices an earlier error, he will correct it and start the test again.)

2.3.3 Problems

You are to estimate the probability that the ECCS system tested will be available if called on after the test. The system will not be available if any of the above valves are in the wrong state or if the pump is in the manual mode. Errors of omission for other items of equipment will be ignored for this problem.

Using the nominal HEPs in Chapter 20 of the Handbook, derive two probability estimates of the posttest availability of the ECCS based on the following different assumptions about the test situation.

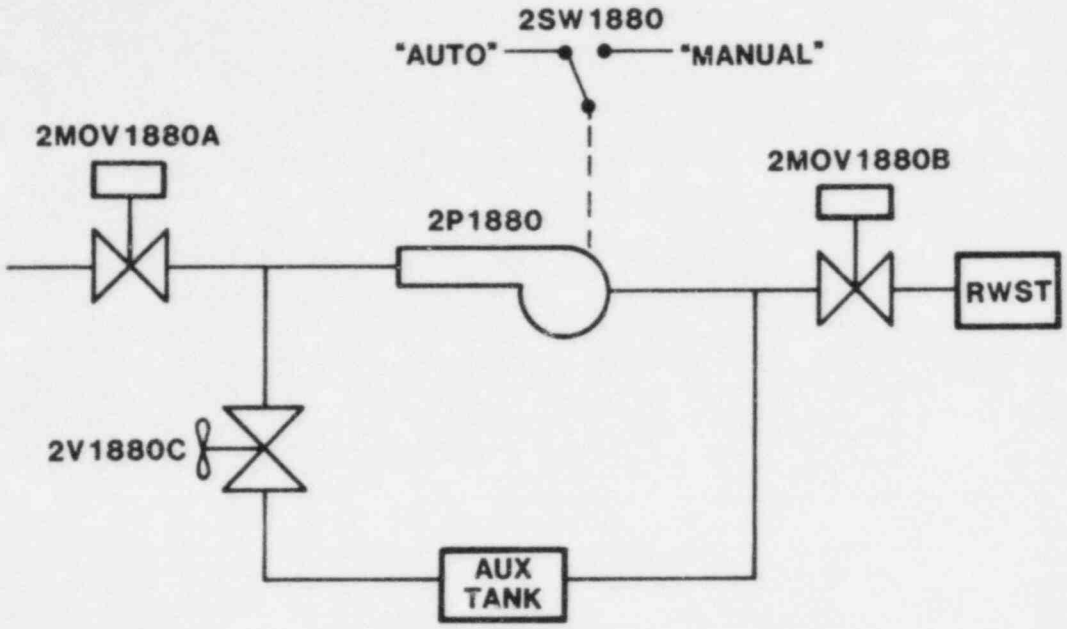


Figure A-7 Schematic of components in monthly test of a high-pressure injection pump.

INJECTION PUMP TEST

1. Set SI pump with switch #2SW1880 to "Manual."
2. Close SI pump valves 2MOV1880A and 2MOV1880B.
3. Open SI pump recirc. valve #2V1880C.
4. Start SI pump, switch #2P1880.
5. After 15 minutes, record flow rate in pump discharge leg.

Flow rate _____

6. Stop SI pump, switch #2P1880.
7. Close SI pump recirc. valve #2V1880C.
8. Open SI pump valves 2MOV1880A and 2MOV1880B.
9. Set SI pump switch #2SW1880 to "Auto."

Figure A-8 Hypothetical test procedure for monthly test of a high-pressure injection pump.

2.3.4 General Performance Shaping Factors

(1) A level 2 tagging system is used, as noted in Table 20-15 of the Handbook. This is the usual type of tag control employed in NPPs. Tags are not accounted for individually--the operator may take an unspecified number of tags and use them as required. In such a case, the number of tags in his possession does not provide any cues as to the number of items remaining to be tagged. Note that with a level 2 tagging system, no adjustments to the Handbook's tabled HEPs are necessary. Note also that in this exercise errors of tag preparation will not affect availability. If a tag is made out incorrectly and the wrong valve is changed as a consequence, the test will be invalid. Ultimately, the condition will be corrected and the test rerun. Therefore, for the purpose of this exercise, it can be assumed that the valves and switches in question are in their respective correct positions for normal operating conditions prior to the test.
(2) The test is a routine operation, placing no unusual demands upon the operator. This scenario reflects an optimal stress level, as defined in Chapter 17 of the Handbook.
(3) For the purpose of this exercise, the test (steps 7, 8, and 9) will be conducted by an operator using the written procedures. Checkoff is not required.
(4) Upon completion of the test, the operator will sign the test form and give it to the shift supervisor. The shift supervisor will note the flow rate reading on the form and will verify that the operator has signed the form.
(5) The operator has more than 6 months' experience.

2.3.5 Specific Problem 2a Performance Shaping Factors

(1) The MOV switches are the type that does not have to be held by the operator until its operating cycle is complete.
(2) The MOV switches are close together and are operated as a unit, i.e., completely dependent, and they are readily distinguishable from other switches on the panel.
(3) The locally operated rising-stem valve, 2V1880C, is readily identifiable.
(4) There is a position indicator on the locally operated valve, and the valve does not stick while being restored.

2.3.6 Specific Problem 2b Performance Shaping Factors

(1) The MOV switches are the type that has to be held while the valve cycles, and the switches are widely separated so that restoration involves two separate acts.
(2) The MOV switches are located among similar appearing items, at least one of which is also tagged, so that selection errors must be considered.
(3) The manual valve sticks when restored, and there is no position indicator on it. Consequently, there is probability of failing to restore it completely. Although it is separated from similar valves, its label is unclear.

2.4 An Approach to Exercise #2

The task in Exercise #2 is to "estimate the probability that the ECCS system will be available if called on after the monthly test." For the first case, the MOVs are treated as a completely dependent unit and the locally operated rising-stem valve is distinct from the others nearby and does not stick as it is being restored. The problem worksheet and the HRA event tree for this case, as shown in Figures A-9 and A-10, consist of only three branches, depicting errors of omission for steps 7 through 9 of the procedure.

Using the nominal HEP of .003 for each step, the probability of failure is $1 - .997^3 \approx .01$. Note that no credit is allowed for the fact that the supervisor signs off the procedures since his signature indicates only that he has approved the flow rate recorded at step 5 and that he has seen the operator's signature on the form. In some plants, this type of supervisor signoff is erroneously considered a verification of test accuracy. In reality, it verifies only the operator's signature.

For the second estimate, the assumptions are that MOVs are separated and have to be held until activation, that the MOVs and the manual valve could be confused with other valves, and that the rising-stem manual valve sticks as it is restored and has no position indicator. In this case, errors of omission and of selection (commmission) must be considered for each valve and for the pump switch. The problem worksheet is shown in Figure A-11. The HRA event tree for the restoration now consists of 10 branches, shown in Figure A-12.

In the HRA event tree shown in Figure A-12, every branch in the success path must be accomplished for the system to be available. Using the nominal HEPs, the probability of failure is $1 - (.995^2 \times .997^8) \approx .03$.

Note: It has been estimated that the probability of a rising-stem valve's sticking is .001 (.0001 to .01). We assume that if a rising-stem valve does not stick as it is being restored, the probability of the operator's failing to restore it completely is negligibly small. If we include this assumption in our analysis, the probability of system failure does not change materially; i.e., $1 - (.995 \times .997^8)$ still rounds to .03.

PROBLEM WORKSHEET

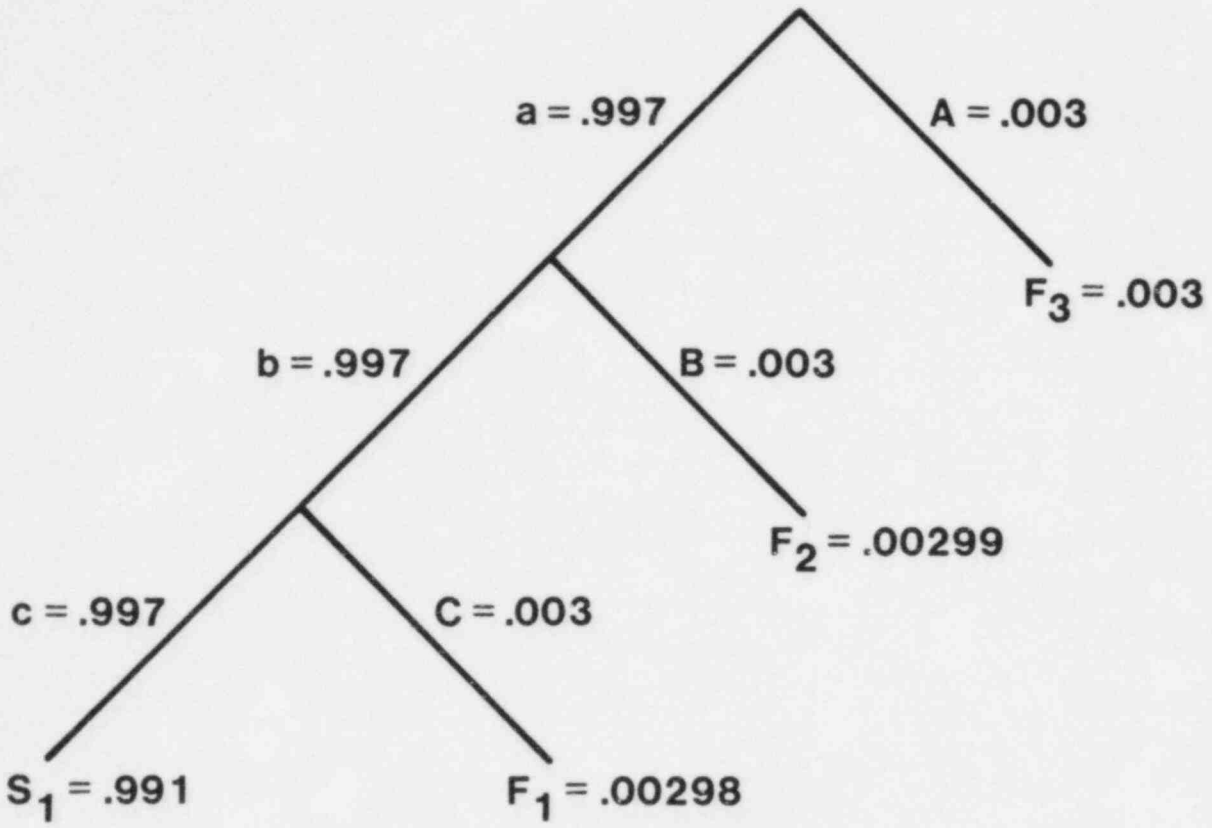
1. Exercise No. 2 Problem No. 2a Analyst

2. Performance Shaping Factors:

Instruction		Experience		Stress Level		Tagging Level	
Written:		≤6 months		Low		1	
≤10 items	X	>6 months	X	Optimum	X	2	X
>10 items				Mod. High		3	
Oral				High		NA	
None							

3. Written Procedure Step No. or Task Description	4. Dependence	5. Potential Error	6. Table No. & Item No.	7. Tabled HEP & UCBs	8. Stress/ Skill Factor	9. Adjusted HEP	10. Comments
7. Close SI pump recirc. valve 2V1880C	--	A. Failure to close valve 2V1880C	20-7 #3	.003 (.001 to .01)			
8. Open SI pump valves 2MOV1880A and 2MOV1880B	CD	B. Failure to open 2MOV1880A and 2MOV1880B	20-7 #3	.003 (.001 to .01)			
9. Set SI pump switch 2SW1880 to "Auto"	--	C. Failure to set switch 2SW1880 to "Auto"	20-7 #3	.003 (.001 to .01)			

Figure A-9 Worksheet for the development of human-caused unavailability of high-pressure injection pump after monthly test.



$$Pr\,[F] = 1 - .997^3 \simeq .01$$

Figure A-10 HRA event tree of human-caused unavailability of high-pressure injection pump after monthly test.

PROBLEM WORKSHEET

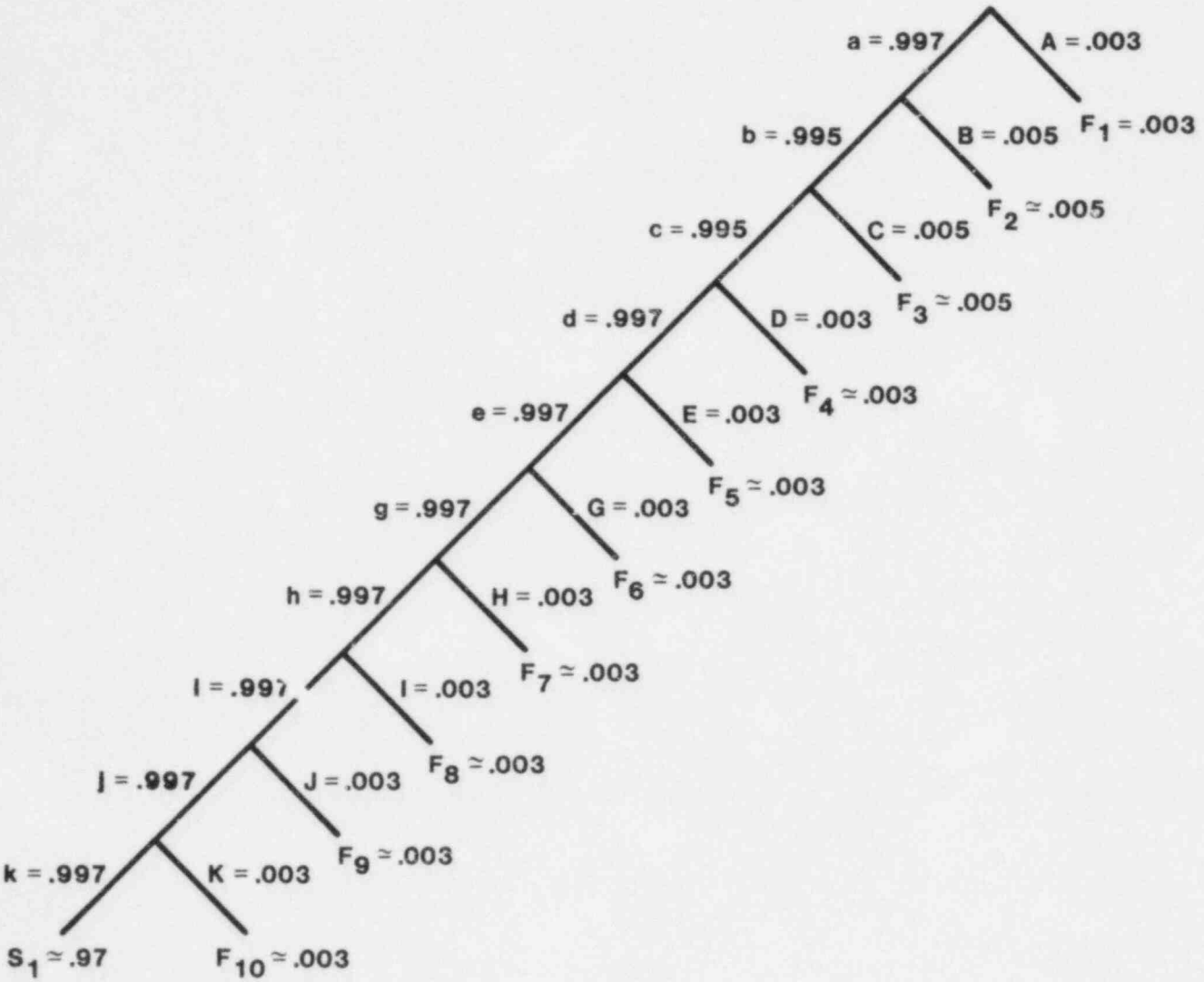
1. Exercise No. 2 Problem No. 2b Analyst

2. Performance Shaping Factors:

Instruction		Experience		Stress Level		Tagging Level	
Written:		≤6 months		Low		1	
≤10 items	X	>6 months	X	Optimum	X	2	X
>10 items				Mod. High		3	
Oral				High		NA	
None							

3. Written Procedure Step No. or Task Description	4. Dependence	5. Potential Error	6. Table No. & Item No.	7. Tabled HEP & UCBs	8. Stress/ Skill Factor	9. Adjusted HEP	10. Comments
7. Close SI pump recirc. valve 2V1880C		A. Omit Step 7	20-7 #3	.003 (.001 to .01)			
		B. Select wrong valve	20-13 #3	.005 (.002 to .02)			
		C. Fail to close valve fully	20-14 #3	.005 (.002 to .02)			
8. Open SI pump valves 2MOV1880A and 2MOV1880B	ZD	D. Omit 2MOV1880A	20-7 #3	.003 (.001 to .01)			
		E. Select wrong MOV switch	20-12 #2	.003 (.001 to .01)			
		G. Fail to open MOV fully	20-12 #10	.003 (.001 to .01)			
		H. Omit 2MOV1880B	20-7 #3	.003 (.001 to .01)			
		I. Select wrong MOV switch	20-12 #2	.003 (.001 to .01)			
		J. Fail to open MOV fully	20-12 #10	.003 (.001 to .01)			
9. Set SI pump switch 2SW1880 to "Auto"		K. Omit resetting 2SW1880 to "Auto"	20-7 #3	.003 (.001 to .01)			

Figure A-11 Worksheet for the development of the modification of the Figure A-10 HRA event tree by incorporating some human factors problems.



$$Pr[F] = 1 - (.995^2 \times .997^8) \simeq .03$$

Figure A-12 Modification of Figure A-10 HRA event tree by incorporating some human factors problems.

3. PROBLEM EXERCISES

Work out the four problem exercises contained in this section. Construct and fill out Problem Worksheets, construct the HRA event trees, and calculate the Pr[F] for each tree. Suggested solutions are found in Section 4.

3.1 Exercise #3. Readjustment of Bistable Amplifiers after Reactor Trip

3.1.1 Background

In this exercise, a reactor trip has occurred. It has been determined that the trip was caused by a miscalibration of all three bistable amplifiers monitoring the output of the level sensors in the pressurizer. The specified trip point for high-level trip is 93%, but the amplifiers were tripping at 88%. A calibration technician has been assigned to readjust the three amplifiers and is working as rapidly as possible to minimize the downtime for the plant. After the three amplifiers are adjusted, the technician must retest the coincidence circuits to verify that the reactor trip signal will occur when any two amplifiers trip.

3.1.2 Task Description

No written procedure will be used for this task. The technician will perform the following operations from memory.

(1) Obtain the reference voltage source that simulates the inputs from the level sensors in the pressurizer.
(2) Adjust the reference voltage to a value of .93 on the digital readout on the simulator.
(3) Connect the simulator to amplifier #1.
(4) Apply voltage to amplifier #1.
(5) Adjust trip to proper voltage level (.93). The point at which the trip occurs is indicated on a digital readout on the simulator. The trip indication on the amplifier involves a change of state of an indicator lamp.
(6) Repeat steps 3, 4, and 5 for amplifiers #2 and #3.
(7) Test the coincidence circuits.

The coincidence circuits will be tested in conjunction with an operator in the control room who will confirm the alarm trips when the calibration technician trips successive pairs of amplifiers. Under normal operating conditions, the probability of his failing to note the status change is negligibly small (Table 20-11, #7).* The HEP for this two-man task will therefore be disregarded, as will the recovery factor it affords. Upon completion of this test, the plant may be brought up to normal operation.

---

*In the text in Chapter 11 associated with Item 7, the Handbook states, "Confirming status change after an operation, such as changing the status of an MOV, is an active task. The operator has initiated the change and ordinarily will watch the indicator lights for confirmation of the response. In most situations, the probability of his failing to note the status change is negligibly small and will be disregarded."

3.1.3 Problem 3a

Assume that the technician is experienced and that he is responding to a direct order from his supervisor. Determine the probability that the recalibration task will be carried out correctly. Prepare an HRA event tree outlining the various steps and their associated HEPs. Indicate the most likely errors that the technician may make. The recalibration task is defined as steps 1 through 5 of the procedure. The coincidence circuit test is not considered to be part of this problem.

3.1.4 Problem 3b

After making the above calculations, draw an HRA event tree for a bounding analysis. State the assumptions you are making for both the upper and lower UCBs, assuming an experienced technician for the best case and a novice for the worst case. An example of a bounding analysis is illustrated in Figure A-13.

3.1.5 Performance Shaping Factors

(1) No written procedure is used.
(2) The technician is responding to an oral instruction from his shift supervisor.
(3) Because of the time pressure, assume a moderately high level of stress.
(4) The correct adjustment of all three amplifiers is completely dependent on the initial adjustment of the simulator--there are no alerting cues in this situation. The technician expects to find all the amplifiers out of adjustment by a considerable amount. Therefore, if he adjusted the simulator incorrectly, there would be no reason for him to become suspicious when each of the amplifiers required a large adjustment.
(5) Assume that the simulator is designed so that it will not operate if it is incorrectly connected to the amplifiers. Disregard any errors in hookup, since the technician will have to correct them in order to perform the task.
(6) Assume that the simulator has been calibrated.

3.2 Exercise #4. Core Spray System Test

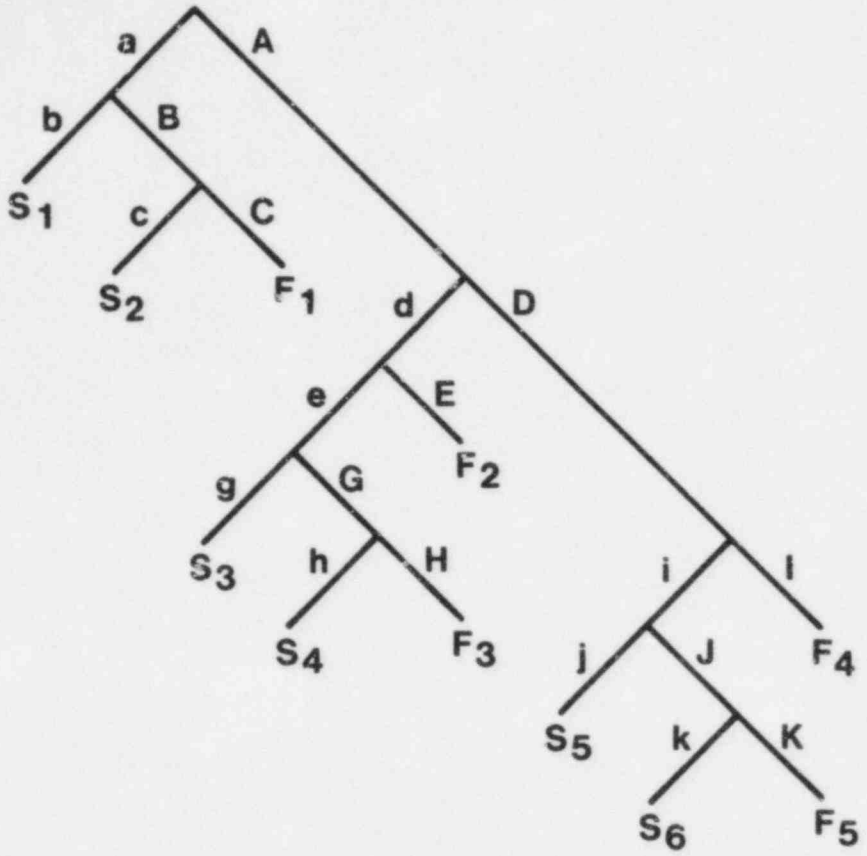
3.2.1 Background

This exercise consists of conducting a test of the core spray pumps of the Emergency Core Cooling System (ECCS). In involves changing and restoring valves and recording the performance of the pumps.

3.2.2 Task Description

The procedure that is relevant to this exercise is taken from a longer set of actual procedures. It is reproduced almost verbatim in Figure A-14. There are certain points relevant to this procedure that should be kept in mind during the analysis. These points include

(1) Certain valves appear under different designations within the procedure. For example, MOV1402-4A in step 2 appears as 1402-4A in steps 3b and 4. This is one indication of a less-than-optimum written procedure.



Best-Case Analysis: For each success path S through the tree, use the lower UCBs of the HEPs and upper UCBs of the HSPs. Sum the terminal values at each S and subtract from 1.0 to obtain the lower UCB of the overall failure probability.

Worst-Case Analysis: For each failure path F through the tree, use the upper UCBs of the HEPs and lower UCBs of the HSPs. Sum the terminal values at each F to obtain the upper UCB of the overall failure probability.

Assume all HEPs = .01 (.003 to .03).

Lower UCB of system failure probability (using HEP of .003, HSP of .997)

$= 1 - [S_1 + S_2 + S_3 + S_4 + S_5 + S_6]$

$= 1 - [ab + aBc + Adeg + AdeGh + ADij + ADiJk]$

$= 1 - .99998 = .00002$

Upper UCB of system failure probability (using HEP of .03, HSP of .97)

$= F_1 + F_2 + F_3 + F_4 + F_5$

$= aBC + AdE + AdeGH + ADI + ADiJK$

$= .00179 \simeq .002$

Nominal system failure probability (using HEP of .01, HSP of .99) = .0002 (using either equation)

Figure A-13 An example of a bounding analysis with its associated HRA event tree.

CORE SPRAY SYSTEM TEST

1. Verify that the ECCS Fill System is in service and vent the Core Spray System. (The tasks for step 1 of this procedure have been omitted here to facilitate the analysis.)
2. Set up the following valve alignment:

Valve No.	Alignment	Normal Position
MOV1402-3A	open	open
MOV1402-24A	closed	open
MOV1402-25A	closed	closed
MOV1402-38A	open	open
MOV1402-4A	closed	closed
Valve 1402-6A	open	open
MOV1402-3B	open	open
MOV1402-24B	closed	open
MOV1402-25B	closed	closed
MOV1402-38B	open	open
MOV1402-4B	closed	closed
Valve 1402-6B	open	open

3. a. Start the core spray pumps, 1402A and 1402B.
   b. Open valves 1402-4A and 1402-4B.
   c. After 15 minutes, record the pump flow from flow indicators FI 1450-4A and FI 1450-4B, and record the pump discharge pressure from pressure indicators PI 1450-1A and PI 1450-1B.

Pump	Indicator	Flow	Indicator	Pressure
1402A	FI 1450-4A	____	PI 1450-1A	_____
1402B	FI 1450-4B	____	PI 1450-1B	_____

Note: Flow rates should be 4500 gpm, and minimum discharge pressure should be 230 psig.

4. Close valves 1402-4A and 1402-4B, and stop pumps 1402A and 1402B.
5. Return all control Switches to NORMAL operating position.

Unit No._____ Date/Time_____

Operator_____ Shift Supervisor_____

Figure A-14 Abbreviated procedure for a core spray system test.

(2) Although this is a test procedure, there is no checkoff provision. The operator's signature at the end of the procedure does not constitute checkoff as defined in the Handbook.
(3) No credit for human redundancy should be given for valve positioning. The supervisor checks the flow rate and pressure and to see that the operator signed the form. He does not inspect the valve restorations themselves. Valve restorations are the only part of the procedure that affects the posttest availability of the system.
(4) Instead of providing a valve and control restoration list or a posttest restoration procedure, the procedure as written includes only a blanket statement to the effect that all control switches should be returned to their normal operating positions.
(5) There is always the possibility that the operator will not use the written procedure (except to fill in the required flow and pressure values) but will rely on his memory instead.

3.2.3 Problem 4a

Starting with step 2 of the procedure, derive an estimate of the unavailability of the system after the monthly test. Assume that the core spray system will not be available unless all valves and controls are restored to their normal operating positions after the test.

3.2.4 Problem 4b

Assume that the test is performed routinely every 3 months and that an operator is assigned to check the status of the valves and controls of the core spray system at monthly intervals between the tests. If this inspection is done without error, assume the recovery factor will be 1.0 for the ECCS. Determine the unavailability of the system given the two intervening inspections using the appropriate equations from Chapter 9 of the Handbook, as revised and presented in the Introduction section of this document.

3.2.5 Performance Shaping Factors

(1) The test will be conducted by one operator.
(2) Written procedures not requiring checkoff are available.
(3) The procedures should be considered as a long list.
(4) Level 2 tagging is used.
(5) The test is routine, placing no unusual demands on the operator.
(6) Upon completion of the test, the operator will sign the test form and give it to the shift supervisor. The supervisor will check the flow rate and pressure readings on meters in the control room and will verify that the operator has signed the form.
(7) All like-numbered switches for channels A and B are located next to each other. Because of their locations, the fact that they are in the same procedural step, and the fact that they can be identified easily, the manipulations of the control room switches for MOV1402-4A and MOV1402-4B are considered to be completely dependent. Similarly, the manipulations of pump switches 1402A and 1402B in the control room are considered to be completely dependent. These pump switches are spring-loaded to return to the normal operating position after activation.
(8) In general, valves prefixed MOV are motor-operated valves operated from the control room by momentary activation of switches labeled with the

same MOV designation used on the valves themselves. All other valves are rising-stem, locally operated valves with position indicators on the valves.

3.3 Exercise #5. Emergency Procedure: Station Blackout

3.3.1 Background

In this exercise, a station blackout has just occurred. All auxiliary power has been lost except dc battery power. When this condition happens, several annunciators and associated alarms indicate the nature of the problem. However, the most salient cue in the control room is the automatic changeover from ac to dc lighting.

The operations hierarchy at this plant is as follows: Shift Supervisor, Control Room Operator, Assistant Control Room Operator, First Auxiliary Operator, Second Auxiliary Operator (AO2), and General Maintenance Operator. The AO2 reports to the Control Room Operator or the Shift Supervisor. He is the second most junior member of the Operations Staff. His level of experience can be critical.

The specific concern in this exercise is the determination of adequacy of response of the AO2. His duties are asterisked in the set of procedures shown in Figure A-15. Assume that it is critical that the AO2 initiate his tasks within 5 minutes of the blackout in order to preclude damage to safety-related equipment.

Even though a loss of auxiliary power is not an immediately life-threatening situation, the plant does follow an emergency procedure. Knowledge of this, plus his own lack of experience, will place the AO2 under some level of stress. (Oak Ridge National Laboratory surveys[12] suggest that operators consider this to be one of the three most stressful response situations encountered in NPP operations). The operators at this plant estimate that the level of stress they will be under is a moderately high level of stress.

This particular plant has an entry- and access-control system that enables the computer to keep track of the approximate locations of all plant personnel. It requires that a badge be inserted and a personal identification number be entered into a control console for passage from one room to another. In the event of a loss of power, this control system fails with the doors open to egress but locked to entry, in which case access is afforded by using keys. Master keys are provided that permit the opening of any door in the operator's field of action. There is a set of keys designated for each operator position. These are passed on to the next person at shift change. It is assumed that each person will carry his keys with him when out of the control room for any reason. If he does so, the operator will be able to make his way through the plant should a station blackout occur while he is outside the control room. Based on direct observation it was determined that it takes the AO2 30 seconds to find his master key and unlock a door, remove his key, and enter.

The physical layout of the part of the plant area relating to this exercise is shown in Figure A-16. The North Piping Penetration Room (NPPR) is one floor below the tagging office and the control room. The Emergency Feedwater Pump Room (EFPR) is one floor below the NPPR. From the control room, the AO2 must

1672.2

E.P. -- Station Blackout p. 1

A. Symptoms

1. All normal lighting lost; dc lighting on
   [others omitted here for brevity]

B. Immediate Actions

1. Attempt to energize 4160 V buses
2. Initiate emergency feed per p. 2
3. Secure letdown by closing CV-1333 and 1334

C. Follow-up Actions

1. If 4160 V buses cannot be energized
   a. Protect secondary plant and reduce dc power demand per p. 3
   b. Verify RCS temp >50°F margin to saturation
2. If 4160 V buses are energized, follow OP 1672.3 (Partial Power Loss)

1672.2

E.P. -- Station Blackout p. 2

p. 2 -- Manual OTSG Feed

1. Proceed directly to Steam Line Penetration Room and manually open MS Supply MOVs CV-3226 and CV-3213 to Emergency FW Pump Turbine.

*2. Proceed to N. Piping Penetration Room; secure Seal Return by manually closing CV-1337. Begin Emergency Feed to A OTSG by manually opening either Emergency FW Valve CV-3202 or CV-3250.

*3. Proceed to Emergency FW Pump Room; open either FW valve (in adjacent Piping Room) CV-3215 or CV-3219.

*4. Contact Control Room; modulate Feed to B OTSG by throttling CV-3215 or CV-3219, modulate Feed to A OTSG by throttling either discharge crossover valve (in Pump Room) CV-3436 or 2317 to maintain stable temp. TH<570°F.

*5. Monitor Emergency FW Pump Suction and Discharge Pressures; notify Shift Supervisor if Suction Pressure falls below 10 psig. (Disch. press. should be >1000 psig.)

*Duties of the AO2

Figure A-15 Emergency procedure for a station blackout.

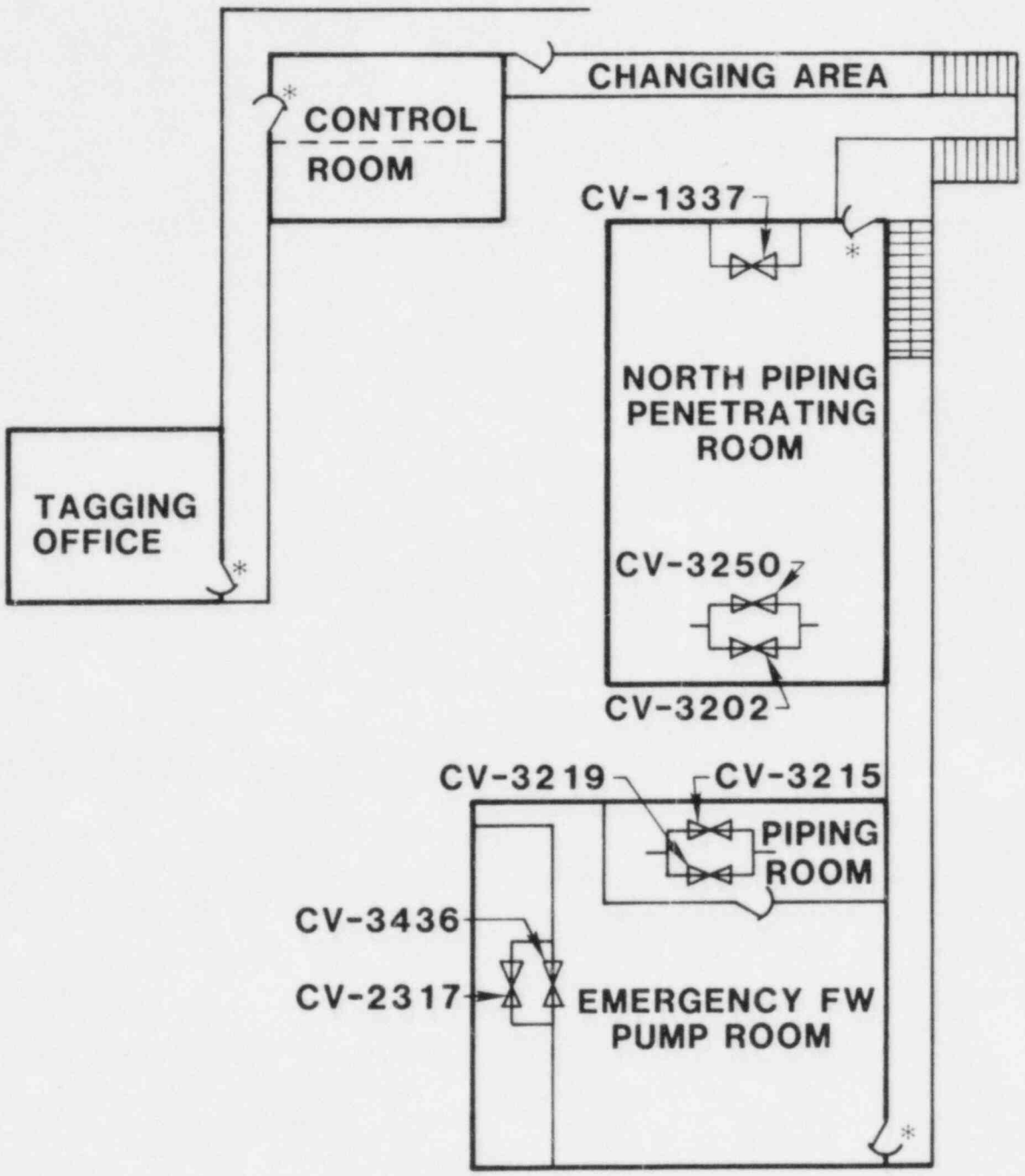


Figure A-16 Layout of plant relevant to exercise #5. (Only valves called out in this procedure are shown although there are several valves in each room.)

pass through one controlled entry door to reach the NPPR. From there, he must pass through two such doors, one of which is an exit, to reach the EFPR. During an interview, the operator estimated that, coming from the control room, the AO2 will be able to get to the NPPR "within 2 minutes, anyway." Assume the estimate to be 2 minutes.

3.3.2 Task Description

As can be seen from the procedure (Figure A-15), the AO2 is responsible for performing steps 2 through 5 of page 2. Step 2 should be initiated within 5 minutes into the blackout.

It is assumed that the AO2 knows his duties in the case of a station blackout--he need carry no written procedures with him to perform his tasks. If not in the control room at the time of the blackout, the AO2's first duty is to proceed toward the control room immediately or to contact the control room by telephone. It is likely that he will be paged before he has time to get there and will be given his instructions. In any event, it is assumed that the control room operator or the assistant control room operator will tell the AO2 where to go and what to do.

3.3.3 Problems

Analyze the activities of the AO2 considering the following two scenarios.

Problem 5a. The blackout occurs while an experienced AO2, i.e., one having more than 6 months' experience, is in the control room.

Problem 5b. The blackout occurs while a novice AO2, i.e., one who has less than 6 months' experience, is in the tagging office.

For each situation, determine the probability of the AO2's failing to perform all of his assigned tasks successfully. Include the probability that the AO2 may freeze and never initiate the task. Develop an HRA event tree for each AO2 using the Handbook Chapter 20.

In addition, for each situation, make as assessment of the time elapsed from the onset of the emergency to the AO2's initiation of the first task.

3.3.4 Performance Shaping Factors

(1) Written procedures are not carried by the AO2. He has been trained to perform his tasks without them.
(2) The AO2 is considered to be under a moderately high level of stress.
(3) In an emergency, the AO2 will stop on his way to the controlled access area long enough to throw on a lab coat, shoe covers, and gloves before entering. He will not take time to undress completely and put on coveralls.
(4) The site operator's estimate of the transit time for an experienced AO2 from the control room to the NPPR is 2 minutes. He also estimates no significant time difference for the novice operator coming from the tagging office. (Consider the possibility that the operator may be underestimating the performance time through ignorance, possible halo effect, or a desire to make a good impression on the interviewer. Data

from Oak Ridge National Laboratory suggest that operator estimates of response times should be doubled, especially when decision-making is involved.[12])

(5) All manual valves are of the large, turning wheel type (about 12 inches in diameter). They are fairly well isolated from other valves in the same room and are clearly labeled as to their valve numbers and functions.

(6) Where the procedures call for the manipulation of one valve or another, e.g., CV-3202 or CV-3250, whatever the AO2's response is, it will be treated as one event on the HRA event tree.

(7) Step 4 in the procedure requires that two valves be throttled. The AO2 is in contact with the control room by telephone. He modulates the position of the valves based upon instructions given by the control room operator who is monitoring a display. One likely error is that the control room operator might misread his display. This would lead to the valve's being left in an incorrect position. Since the AO2 is not at fault here and since the evaluation involves his ability to complete his assigned tasks within the time constraints, we will disregard this type of error. (For a complete analysis, this error would likely be included.)

(8) The measured time for the AO2 to open a door with the master key is 30 seconds.

(9) In both cases (experienced or novice), the AO2 and the rest of the operations staff see their tasks as one complete job--that of supplying emergency feedwater to steam generators A and B. Therefore, it is assumed that the performance of the AO2's tasks are completely dependent with respect to errors of omission.

(10) Reversal errors involve closing a valve that should be open and vice versa. They will be disregarded in the analysis, since the AO2 is in almost constant contact with the control room.

11. Step 5 in the procedure, monitoring the emergency feedwater pump suction pressure, is an activity that is not required until almost 2 hours into the blackout. Therefore, it should not be included in the emergency procedure event trees.

3.4 Exercise #6. Risk Assessment for Valve Restoration Following Maintenance

3.4.1 Background

An activity common to many maintenance operations is the restoration of the subsystem after the maintenance has been completed. The scenario* presented relates to maintenance that has been performed on a safety-related item of equipment. The procedure requires that a number of locally (manually) operated valves be manipulated prior to the maintenance in order to isolate the subsystem. Upon completion of the maintenance, these valves must be restored to their original positions.

The principal means of ensuring proper valve alignment before and after maintenance is the use of tags, logs, and other administrative controls. In addition, in some plants, the valve status is displayed on an Engineered Safety Feature (ESF) panel. (Reminder: see Note 3, page A-9.)

*This scenario is not a representation of a specific plant. It addresses a generic problem common to all NPPs.

3.4.2 Task Description

While specific procedures and policies differ from plant to plant, Figure A-17 presents an assumed flow of events associated with the maintenance of safety-related equipment for this particular problem.

3.4.3 Problem 6a

A single locally operated ESF valve that has an associated position indicator on the ESF panel must be restored after the maintenance. Determine the joint probability that the operator will fail to restore the valve and that this error will not be recovered in the next shiftly inspection of the control room panels using a written checklist.

The following questions should be considered for Problem 6a.

(1) What sort of tagging/logging procedure (what level) is required by the plant?
   - What percentage of the time is the procedure actually followed?
   - What are the restoration requirements?
(2) What are the type and the location of the indicator?
   - How is position/state of component displayed?
   - Is the display isolated?
   - Is the display labeled clearly?
(3) How many indicators are being considered?
(4) How often is the ESF panel scanned/inspected for deviations?
   - Is the scan/inspection always performed on schedule?
   - What are the requirements of the scan/inspection?

3.4.4 Performance Shaping Factors for Problem 6a

(1) The isolation and maintenance were performed correctly.
(2) Level 1 tagging control is assumed (Table 20-15). (Note that a level 1 tagging system does not preclude errors of commission.)
(3) The position indicator is a standard "red for open, green for closed" backlit display located on the ESF panel. It is clearly labeled and visible.
(4) The ESF panel is scanned formally at the beginning of each shift. Using a checklist, an individual inspects the position of each component on the panel.
(5) The deviant indicator on the ESF panel is the only factor in the control room that alerts the operator to the position of the valve.

3.4.5 Problem 6b

Assume that there is no position indicator for the misaligned valve. The only recovery factor is a walk-around inspection performed once per shift.

What is the probability that the incorrect valve status will be detected within 30 days or less?

Before maintenance is performed:

- Isolation of the subsystem must be approved by the shift supervisor.
- Each component affected must be issued a tag, the number of which is entered into a logbook.
- Maintenance personnel perform maintenance acts; operators perform status changes of tagged items.

After maintenance is performed:

- Shift supervisor verifies (or has someone verify) that the maintenance was performed.
- The logbook identifies which tags relate to that maintenance act.
- The tags are removed as their respective components are restored.
- The tags are then returned to the control room where they are checked against the logbook to determine whether all of them have been removed.
- Position indicators on the ESF panel are checked to ensure proper valve alignment.

Figure A-17 General flow of operator actions before and after maintenance is performed.

3.4.6 Performance Shaping Factors for Problem 6b

(1) There are three shifts per day.
(2) There are three inspectors available per shift, and each inspector is equally likely to be assigned to the walk-around inspection.
(3) There is one walk-around inspection per shift.
(4) There is zero dependence between inspectors.
(5) The valve in question is a rising-stem valve with no direct indication of what its status should be.

4. CANDIDATE SOLUTIONS FOR PROBLEMS 3 THROUGH 6

4.1 An Approach to Exercise #3

In this exercise, the supervisor gives a direct order to the operator to perform a task which he then checks to see was performed. In this case, the HEP for the operator's failure to initiate the task is .001 (.0003 to .003) (Table 20-8, #1a), but the joint probability of the operator's failing to initiate the task and the supervisor's failing to check the operator's performance is considered to be negligible.

4.1.1 Solution to Problem 3a

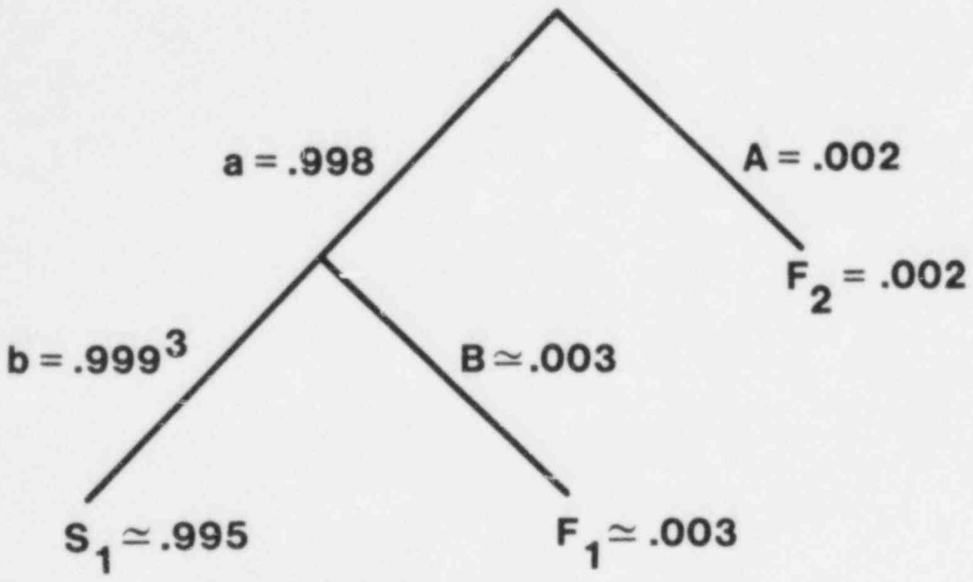
For our initial analysis, we will assume that an experienced technician performs the tasks. The tasks to be performed are listed below, along with their unmodified HEPs, UCBs, and Source for each HEP. As in the main body of this document, the T stands for the table from the Handbook, and the item number within the referenced table follows.

Task	HEP (UCBs)	Source
"A" - adjust simulator (involves one digital readout)	.001 (.0003 to .003)	T20-10, #2
"B" - adjust amplifiers	Negligible	T20-11, #7

Adjustment of the amplifiers involves turning a control until a change in a status indication is obtained, such as a lamp turning on or off. Although the HEP for this task is usually negligible, we are assigning a value of .001 because of the stress level involved. This value is somewhat arbitrary--it is a reasonably small number that reflects our feeling that, under stress, even very well-practiced, easy tasks are subject to disruption. By the same reasoning, for the first task, we take the nominal HEP of .001 and double it to .002 to allow for the effects of moderately high stress; for the second task, we take the value of .001 as the HEP for adjustment of each of the three amplifiers. The EFs also must be modified for moderately high stress, as indicated in Table 20-20. Item 5 in this table assigns an EF of 5 to HEPs $\geq$ .001 for the performance of step-by-step procedures carried out in nonroutine circumstances. Thus, for the HEP of .002, the lower UCB is .002 $\div$ 5 = .0004, and the upper UCB is .002 x 5 = .01. For the HEP of .001, the lower and upper UCBs are, respectively, .0002 and .005.

Note that the adjustment of all three amplifiers is completely dependent on the adjustment of the simulator--there are no alerting cues in this situation. The technician expects to find all the amplifiers out of adjustment by a considerable amount. Therefore, if he adjusted the simulator incorrectly, there would be no reason for him to become suspicious when each of the amplifiers required a large adjustment.

The HRA event tree for the recalibration consists of just two branches, as shown in Figure A-18. (The success probability for branch b is raised to the third power because there are three operationally similar amplifiers.)



$$Pr[F] = 1 - (.998 \times .999^3) \simeq .005$$

Event	HEP (UCBs)
A = Adjust simulator incorrectly	.002 (.0004 to .01)
B = Adjust at least 1 amplifier incorrectly	.001 (.0002 to .005) (per amplifier)

Figure A-18 HRA event tree of readjustment of three bistable amplifiers after reactor trip.

Using the above modified HEPs, the failure probability is $1 - (.998 \times .999^3) \approx .005$.

4.1.2 Solution to Problem 3b

To do a bounding analysis, we assume an experienced technician for the best case and a novice for the worst case. Therefore, for the novice, we will double the above HEPs given for the experienced personnel. For Task "A," the HEP for the experienced technician is .002 (.0004 to .01); for the novice, it is .004 (.0008 to .02). For Task "B," the corresponding values are .001 (.0002 to .005) and .002 (.0004 to .01). For the best case, we use the lower UCBs of the HEPs for the experienced technician, and for the worst case, we use the upper UCBs of the HEPs for the novice, in both cases using the HEPs that have been modified for stress. Thus, the lower UCB is

$$1 - (.9996 \times .9998^3) \approx .001$$

and the upper UCB is

$$1 - (.98 \times .99^3) \approx .05$$

4.2 An Approach to Exercise #4

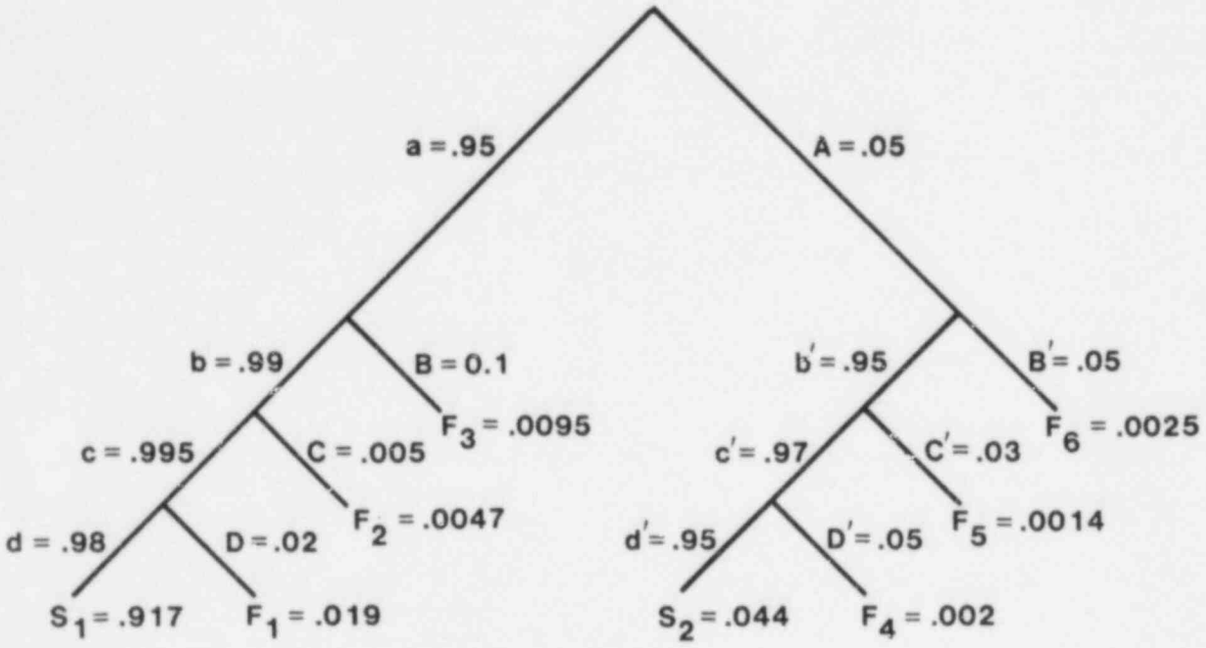
4.2.1 Solution to Problem 4a

In approaching a solution to this problem, let us define the possibilities for human error. The only errors we will describe are those associated with the restoration of all switches to their normal operating positions since failure to restore any given switch(es) is the definition of system unavailability. The system event tree is shown in Figure A-19; a discussion of the events appears below.

(1) The operator could fail to use the written procedures in performing this test. Since we have no information dealing with the administrative controls at this plant, we do not know how likely or unlikely it is that this happen. Therefore, we use the nominal value of .05 (.01 to .25) for this probability (Table 20-6, #6).

(2) The operator could forget to close MOVs 1402-4A and 1402-4B. The problem states the rationale for assuming complete dependence between the switches for these valves, so we will treat them as a unit. If the procedures are used, the HEP for this task is .01 (.003 to .03), the probability of omitting an item from a long list that does not require checkoff (Table 20-7, #4). If the procedures are not used, the HEP is .05 (.01 to .25 (Table 20-7, #5). This estimate does not include any recovery factor. Since we are assuming complete dependence between the two switches (making the conditional HEP of the second switch 1.0, given an error on the first one), the HEP of .05 is the probability that both will be overlooked.

(3) The operator may fail to stop pumps 1402A and 1402B. These pumps are also completely dependent and will be treated as a unit. The task called for here is in the same procedural step as that calling for the closing of MOVs 1402-4A and 1402-4B. Because of this less-than-optimum written procedure, some level of dependence exists between the two sets of switches for errors of omission, i.e., between the set of the MOV



$$Pr[F_T] = 1 - (.917 + .044) \simeq .04$$

Event	HEP (UCBs)	Source
A = Failure to use the written procedures	.05 (.01 to .25)	T20-6, #6
B = Failure to close MOVs 1402-4A and 1402-4B, given that the procedures are used	.01 (.003 to .03)	T20-7, #4
B′= Failure to close MOVs 1402-4A and 1402-4B, given that the procedures are not used	.05 (.01 to .25)	T20-7, #5
C = Failure to stop pumps 1402A and 1402B, given that the procedures are used	.005 (.002 to .02)	see text
C′= Failure to stop pumps 1402A and 1402B, given that the procedures are not used	.03 (.006 to .15)	see text
D = Failure to open MOVs 1402-24A and 1402-24B, given that the procedures are used	.02 (.004 to .1)	see text
D′= Failure to open MOVs 1402-24A and 1402-24B, given that the procedures are not used	.05 (.01 to .25)	see text

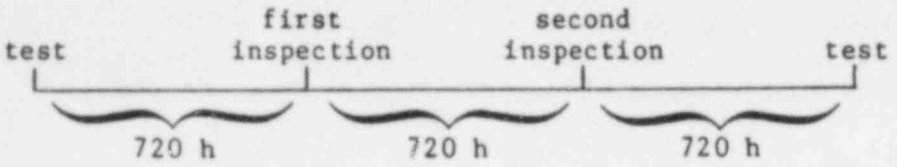
Figure A-19 HRA event tree for restoring core spray system to normal operating condition after test.

switches and the set of pump switches. We have no information on the relative positions of the switches for the MOVs and pumps. Certainly they are all in the control room, but they could be separated by several yards. If so, the operator could be distracted or interrupted between performing one task and the next and could fail to perform the second task. So the level of dependence is not complete, but still is considerable; assume high dependence between closing the MOVs and stopping the pumps. Use the same nominal HEP for stopping the pumps as was used for closing the MOVs. To reach an actual estimate of the probability of an error here, the conditional HEP for the second task (stopping the pumps) will reflect modifications made to this nominal value based on the dependence model given in Table 20-19. The resulting values assume success in closing the MOVs. It is not necessary to consider the possibility of pump stop errors if the MOVs are not closed since forgetting to close the MOVs already results in system failure as defined in the problem. The nominal HEP for stopping the pumps is .01 if written procedures are used and .05 if the task is done from memory, and the corresponding HSPs are .99 and .95. To calculate the conditional HSPs of .995 and .975, given high dependence, use Equation 10-12 from Figure 20-17. The conditional HEPs are now 1 - .995 = .005 and 1 - .975 = .03. Using Table 20-20, #3 and #5, we assign UCBs for the conditional HEPs, and the full expressions of these HEPs become .005 (.002 to .02) for the case in which procedures are used and .03 (.006 to .15) for the case in which procedures are not used.

(4) The operator could fail to open MOVs 1402-24A and 1402-24B. This task is not specified in the procedure but is covered in the blanket order to return all control switches to their normal operating positions. We assume that, since in the 12 tasks called for in step 2 only these 2 required operations, the operator will not refer to step 2 to perform this task but will rely on his memory. Given that he used the procedures in the first place, we would not expect this HEP to be as low as that for the case in which the MOVs were called out for restoration by their labels, nor would we expect this HEP to be as high as that for the case in which the operator relied completely on his memory. Thus, the HEP should be greater than .01 and less than .05. The Handbook offers no explicit guidance for this particular situation, so we suggest doubling the .01 HEP. Using Table 20-20, #3, to assign UCBs, the derived HEP is .02 (.004 to .1), given that he used the procedures initially but did not use them as a restoration checklist. For the case in which the operator relied only on his memory, we used the same HEP of .05 (.01 to .25) as was used for the other cases of not using the written procedures. The probability of failure for the system, as defined, is equal to 1 minus the sum of the two success paths, 1 - (.917 + .044) = .04. This, then, is the value of U, the probability that the system will be unavailable if called on between the tests due every 3 months.

4.2.2 Solution to Problem 4b

To investigate the effects of two intervening inspections on the probability of system unavailability, assume that one such inspection is made 1 month after the test, that one is made 2 months after the test, and that the HEP for each inspection is .05 (Table 20-22, #3). Thus, a time line like the one shown below can be said to represent these events.



In terms of the variables defined in the Introduction to these exercises,

$$p = .04 \qquad \bar{T} = 2160 \qquad h_1 = h_2 = h_3 = 720 \qquad C_1 = C_2 = .05$$

and

$$\bar{d}_t = 720 + (.05 \times 720) + (.05 \times .05 \times 720) \simeq 757.8$$

Therefore,

$$U = (.04 \times 757.8) \div 2160 \simeq .014 \ .$$

Thus, the incorporation of the two monthly checks reduces the system unavailability by nearly a factor of 3: $(.04 \div .014 \simeq 2.9)$.

4.3 An Approach to Exercise #5

4.3.1 Solutions to Problems 5a and 5b

The solution of this problem requires quite a bit of troubleshooting on the part of the analyst, especially with respect to the time requirements. In both cases (experienced and novice operators), the AO2 (and the rest of the operations staff) sees his tasks as one complete job: that of supplying emergency feedwater to steam generators A and B. Therefore, we will assume that the performances of the AO2's tasks are completely dependent with respect to errors of omission. Errors of commission are defined below for each task.

(1) Close CV-1337 -- This is a manual valve. Errors of selection and reversal* are possible.
(2) Open CV-3202 (or CV-3250) -- This is a manual valve. (Remember we are considering "either...or" commands to require one manipulation.) Errors of selection and reversal* are possible.
(3) Open CV-3215 (or CV-3219) -- This is a manual valve. Errors of selection and reversal* are possible.
(4) Throttle CV-3215 (or CV-3219) -- This is a manual valve. Errors of selection and reversal* are possible. Though not in the same procedural step as the order to open the same valve, this instruction to throttle CV-3215 is still considered to be completely dependent on the previous CV-3215 instruction with respect to errors of selection.
(5) Throttle CV-3436 (or CV-2317) -- The manipulation of this manual valve is called out in the same procedural step as that for CV-3215. However, this is the crossover discharge valve for the A steam generator; whereas, CV-3215 is the main feedwater valve for the B steam generator. They are not considered to be dependent with respect to errors of commission. Errors of selection and reversal* are possible.

There is a possibility that the entire task will not be initiated. For the first case, this would involve an experienced AO2's forgetting to perform his primary responsibility and the two senior staff members' forgetting to order the task. Given that the task is called out in the procedures and that all three people have considerable operating experience, their joint probability of failing to recall the need for this is negligibly small and will be disregarded here. (This points out the favorable effects of human redundancy.)

Table 20-13 lists five sets of PSFs and associated HEPs pertinent to estimating an HEP for the experienced AO2. The first item from this table most closely matches the PSFs for the present problem, as described above in section 3.3.4, PSF #5: "All manual valves are of the large turning wheel type (about 12 inches in diameter). They are fairly well isolated from other valves in the same room and are clearly labeled as to their valve numbers and functions." Therefore, we assess .001 (.0003 to .003), from Table 20-13, #1, as the estimated BHEP for the experienced AO2 for errors of selection. This

---

*Reversal errors involve closing a valve that should be open and vice versa. These will be disregarded in the analysis since the AO2 is in almost constant contact with the control room and receives feedback from them. (See the section, "Reversal Errors," in Chapter 14 of the Handbook.)

BHEP and its EF must now be modified to reflect the effects of a moderately high level of stress for a step-by-step task. According to Table 20-16, #4a, the HEP becomes .002, and according to Table 20-20, #5, the UCBs are .004 to .01. The HRA event tree for the experienced A02 is shown in Figure A-20.

In addressing the question of whether an experienced operator (in the control room at the time of the blackout) could respond in time, consider all the time estimates given for the following events.

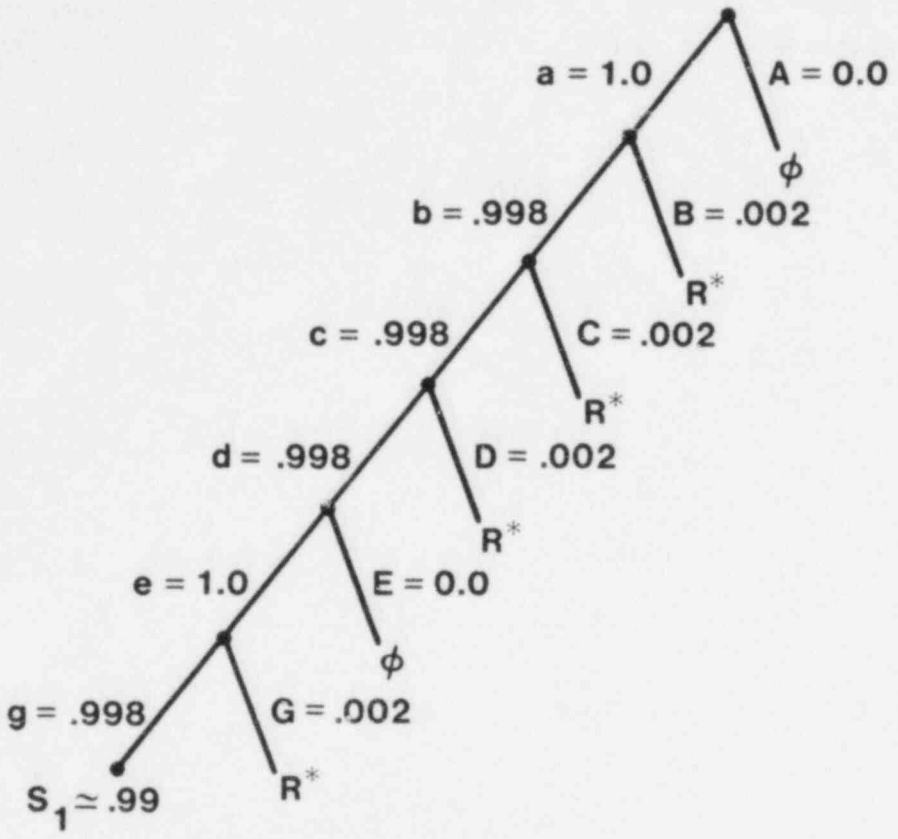
Event	Time
Decision and travel time from control room to NPPR	4 minutes
Entry into NPPR	0.5 minute
Total time to initiation	4.5 minutes

We see that this best-case scenario barely provides enough time to initiate the tasks on schedule. Now let's look at a worst-case scenario.

For the second case, given that the A02 is a novice, there is some probability that he himself will not remember his responsibilities during a station blackout. He may freeze in the Tagging Office and make no response, he may completely forget his duties and call for instructions, or he may pause before going to the control room because he is confused. The probability of his freezing and making no response is highly unlikely because of his training, but we assign it a token probability of .0001 (.00001 to .001) because of the moderately high stress level. We assign the two senior staff members a joint probability of failing to order the tasks done of .00001 (.000001 to .0001). If the A02 merely waits in the Tagging Office or exhibits uncertainty in responding, the probability is still negligibly small that he will fail to receive proper instructions. He may call or go to the control room himself, be paged by the control room, or be prompted to contact the control room by someone in the Tagging Office. Thus, the probability of failure to initiate the task, taking into account the recovery factors, is negligibly small ($.0001 \times .00001 \ll 10^{-5}$).

The estimated BHEP for errors of selection of .001 (.0003 to .003) (Table 20-13, #1) is modified as it was for the experienced operator. However, as seen in Table 20-16, #4b, the effects of moderately high stress are more pronounced for a novice than for an experienced operator, i.e., quadrupled rather than doubled. The estimated HEP for the novice under the stated conditions is .004, and the UCBs from Table 20-20, #5, are .0008 and .02. The HRA event tree for the novice operator is shown in Figure A-21.

The time estimates for the novice operator are listed below with their corresponding events.



$S_1 \simeq .99$ WITHOUT RECOVERY

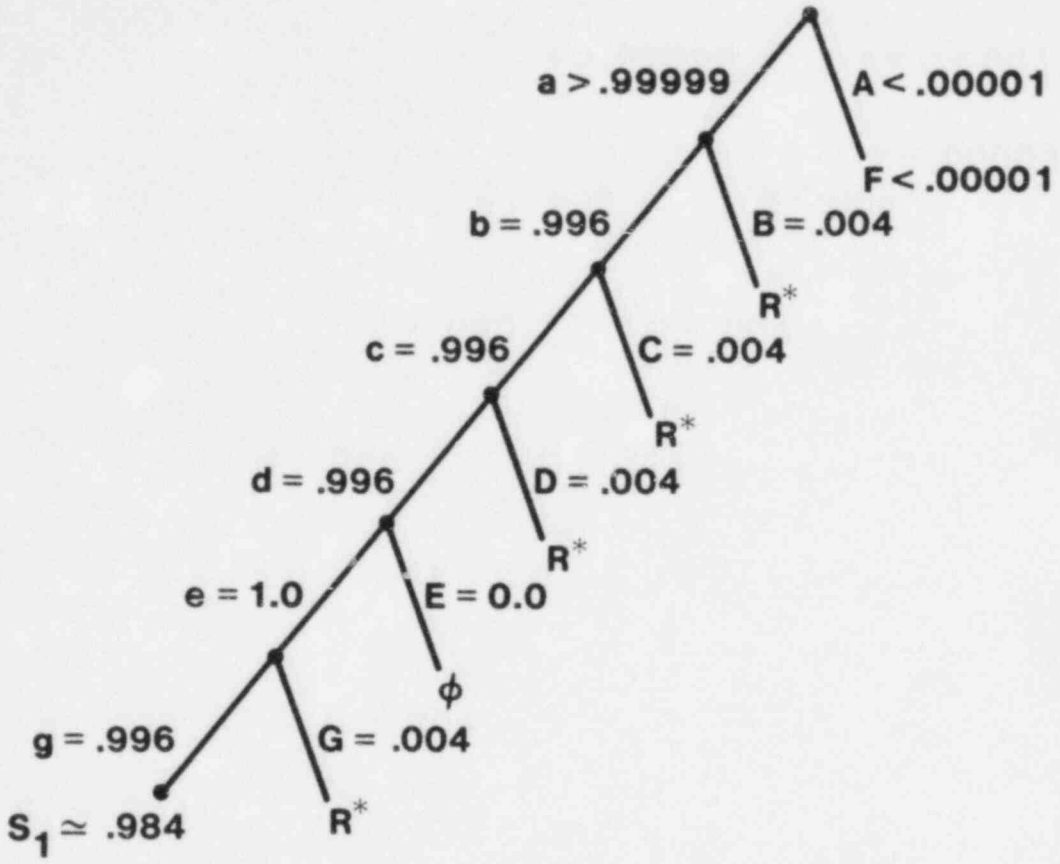
SINCE ALL ERROR LIMBS ARE FULLY RECOVERED,

$S_T = 1.0$

Event	HEP (UCBs)	Source
A = Failure to initiate task	Negligible	see text
B = Select wrong valve for CV-1337	.002 (.0004 to .01)	see text
C = Select wrong valve for CV-3202	.002 (.0004 to .01)	see text
D = Select wrong valve for CV-3215	.002 (.0004 to .01)	see text
E = Select wrong valve for CV-3215 (complete dependence)	0.0	see text
G = Select wrong valve for CV-3436	.002 (.0004 to .01)	see text

* R stands for Recovery Factor in this case. Feedback from the control room would alert the AO2 to having made a mistake. He could correct it on the spot.

Figure A-20 HRA event tree for experienced AO2 responding to station blackout.



$S_1 \simeq .984$ WITHOUT RECOVERY

SINCE ALL ERROR LIMBS ARE FULLY RECOVERED,

$S_T = 1.0$

Event	HEP (UCBs)	Source
A = Failing to initiate task (joint probability)	Negligible	see text
B = Select wrong valve for CV-1337	.004 (.0008 to .02)	see text
C = Select wrong valve for CV-3202	.004 (.0008 to .02)	see text
D = Select wrong valve for CV-3215	.004 (.0008 to .02)	see text
E = Select wrong valve for CV-3215 (complete dependence)	0.0	see text
G = Select wrong valve for CV-3436	.004 (.0008 to .02)	see text

* R stands for Recovery Factor in this case. Feedback from the control room would alert the AO2 to having made a mistake. He could correct it on the spot.

Figure A-21 HRA event tree for novice AO2 responding to station blackout.

Event	Time
Decision and travel time to control room (collect keys, receive instructions)	3 minutes
Travel time, control room to NPPR	6 minutes
Entry into NPPR	0.5 minute
Total time to initiation	9.5 minutes

In the operator interviews, it was determined that it would take a novice no appreciably greater amount of time to reach the NPPR than it would an experienced man. We judge that this is an overly optimistic assumption because it fails to account for the greater probability of indecision on the part of the novice. This plus the fact that the novice was out of control room at the time of the accident leads us to assume that he could hope to reach the NPPR in no fewer than 9.5 minutes. This is clearly unacceptable in terms of system requirements.

4.4 An Approach to Exercise #6

4.4.1 Solution to Problem 6a

Two of the Performance Shaping Factors described in this problem contribute to the low estimated probability (10^{-5}) of an unrecovered failure to restore the valve. First, the plant has a level 1 tagging system, as defined in Table 20-15 of the Handbook. Second, there is a pair of indicator lights in the control room indicating whether this locally operated valve is closed (green light) or open (red light). The detection of a control room indication of an inappropriate valve position during a shiftly inspection of the panels while using a checklist constitutes a recovery factor for an error of omission or commission in valve restoration after maintenance.

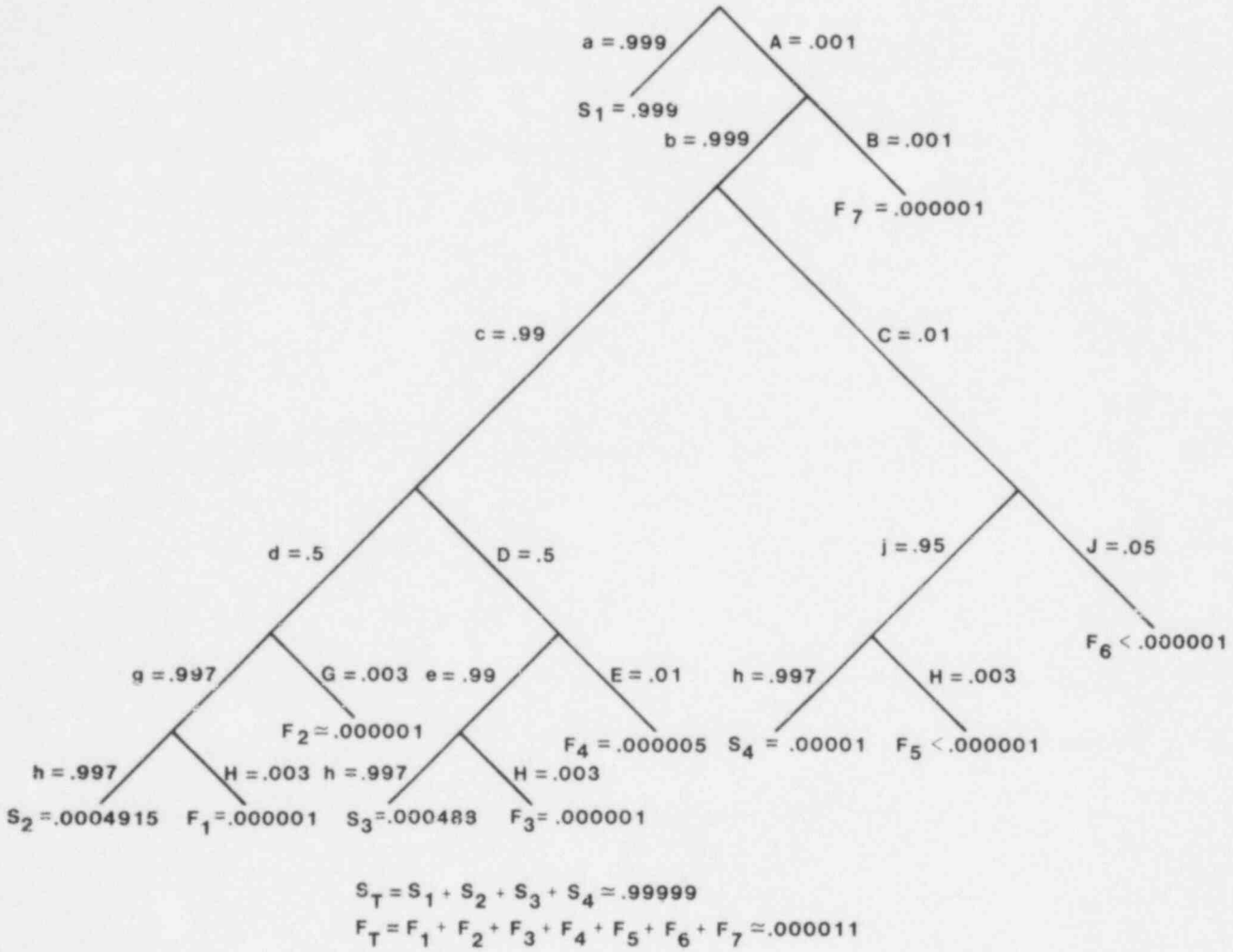
Considering the restoration of a specific component after maintenance on it or on related equipment, the question of interest is the detection of the deviant indicator corresponding to the misaligned component.

The HRA event tree associated with this solution of the problem is shown in Figure A-22 and the events are defined in Table A-2.

4.4.2 Solution to Problem 6b

This problem illustrates the degrading effect of eliminating the valve position indicator lights from the ESF panel. The only recovery factor in such a system is the walk-around inspection conducted during each shift.

For the conditions assumed in this problem, Table 20-27, #3 lists an estimated probability of .05 for failure to detect a deviant condition in 30 days or less for the case in which there are three persons available to rotate the walk-around inspection each shift, and there are three shifts per day.



$$S_T = S_1 + S_2 + S_3 + S_4 \simeq .99999$$

$$F_T = F_1 + F_2 + F_3 + F_4 + F_5 + F_6 + F_7 \simeq .000011$$

Figure A-22 HRA event tree for detection of failure to restore ESF valve after maintenance.

Table A-2 Definitions of events in Figure A-22 (page 1 of 2)

Event	HEP (UCBs)	Source
A = failure to remove the tag and restore the valve. This is an error of omission. It is the same as failing to initiate the restoration task.	.001 (.0003 to .003)	Table 20-8, #1
B = failure to initiate the shiftly inspection. The operator for any given shift may entirely forget to perform the check of the ESF panels. This is a failure of administrative control since this check is a standard plant procedure.	.001 (.0003 to .003)	Table 20-6, #2
C = failure to use written procedures. In this case, after deciding to perform the inspection, the operator chooses not to use the available written procedures.	.01 (.003 to .03)	Table 20-6, #5
D = failure to use the checklist properly. Given that the operator has decided to perform the check of the ESF panels, he may fail to use the checkoff provision of the checklist properly; i.e., checking then signing for one display at a time.	.5 (.1 to 1.0)	Table 20-6, #8
E = failure to check the status of the indicator in question, given that the checklist is used improperly. If a checklist with provision for checkoff is not used properly, no credit for the checkoff provision is assumed. Since the entire ESF system is checked, a long list is assumed.	.01 (.003 to .03)	Table 20-7, #4
G = failure to check the status of indicator in question, given that the checklist is used properly. This is the probability that any one item from a long list of items will be omitted when using a checklist with checkoff provision.	.003 (.001 to .01)	Table 20-7, #2

Event	HEP (UCBs)	Source
H = failure to detect an improper status cue of an indicator lamp. This is a reversal error in which the operator looks at the indicator to check its status but does not perceive that its status is incorrect. The general HEP for an error of commission is used.	.003 (.001 to .01)	Ch. 20, text
J = failure to check the status of the indicator in question, given that the written procedures are available but not used.	.05 (.01 to .25)	Table 20-7, #5

REFERENCES

1. Swain, A. D. and H. E. Guttmann, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Sandia National Laboratories, NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, DC, 1983 (in press).

2. NUREG-75/014, WASH-1400, Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, U.S. Nuclear Regulatory Commission, Washington, DC, October 1975.

3. NUREG-0801, Evaluation Criteria for Detailed Control Room Design Review, U.S. Nuclear Regulatory Commission, Washington, DC, October 1981.

4. MIL-STD-1472C, Military Standard, Human Engineering Design Criteria for Military Systems, Equipment and Facilities, U.S. Department of Defense, Washington, DC, 2 May 1981.

5. NUREG-0700, Guidelines for Control Room Reviews, U.S. Nuclear Regulatory Commission, Washington, DC, September 1981.

6. Stillwell, W.G., D. A. Seaver, and J. P. Schwartz, Expert Estimation of Human Error Probabilities in Nuclear Power Plant Operations: A Review of Probability Assessment and Scaling, Decision Science Consortium and Sandia National Laboratories, NUREG/CR-2255, U.S. Nuclear Regulatory Commission, Washington, DC, May 1982.

7. Seaver, D. A. and W. G. Stillwell, Procedures for Using Expert Judgment to Estimate Human Error Probabilities in Nuclear Power Plant Operations, Decision Science Consortium and Sandia National Laboratories, NUREG/CR-2743, U.S. Nuclear Regulatory Commission, Washington, DC, March 1983.

8. Brune, R. L. and M. Weinstein, Procedures Evaluation Checklist for Maintenance, Test, and Calibration Procedures, Human Performance Technologies, Inc. and Sandia National Laboratories, NUREG/CR-1369, Revision 1, U.S. Nuclear Regulatory Commission, Washington, DC, September 1982.

9. Brune, R. L. and M. Weinstein, Checklist for Evaluating Emergency Procedures Used in Nuclear Power Plants, Human Performance Technologies, Inc. and Sandia National Laboratories, NUREG/CR-2005, Revision 1, U.S. Nuclear Regulatory Commission, Washington, DC, April 1983.

10. INPO 82-017, Emergency Operating Procedures Writing Guideline (Preliminary), Institute of Nuclear Power Operations, Atlanta, GA, July 1982.

11. Brune, R. L., M. Weinstein, and M. E. Fitzwater, Peer Review Study of the Draft Handbook of Human Reliability Analyis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, Human Performance Technologies, Inc., SAND82-7056, Sandia National Laboratories, Albuquerque, NM, January 1983.

12. Haas, P. M. and T. F. Bott, Criteria for Safety-Related Nuclear Power Plant Operator Actions: A Preliminary Assessment of Available Data, Oak Ridge National Laboratory, NUREG/CR-0901, U.S. Nuclear Regulatory Commission, Washington, DC, July 1979.

ABBREVIATIONS

1278	--	NUREG/CR-1278
ABS	--	auxiliary building sump
ANN	--	annunciator
AO	--	auxiliary operator
BHEP	--	basic human error probability
BWST	--	borated water storage tank
CB	--	control board
CD	--	complete dependence
CP	--	control panel
CRT	--	cathode-ray tube
CV	--	control valve
DG	--	diesel generator
DH	--	decay heat
DHP	--	decay heat pump
ECCS	--	emergency core cooling system
EF	--	error factor
EFPR	--	emergency feedwater pump room
E.P.	--	emergency procedure
ES	--	emergency system
ESF	--	engineered safety feature
ERV	--	emergency relief valve
FW	--	feedwater
HD	--	high dependence
HEP	--	human error probability
HPI	--	high-pressure injection
HRA	--	human reliability analysis
INPO	--	Institute of Nuclear Power Operations
IREP	--	Interim Reliability Evaluation Program
LD	--	low dependence
LOCA	--	loss-of-coolant accident
LPI	--	low-pressure injection
MD	--	moderate dependence
MOV	--	motor-operated valve
MS	--	main steam

MU	--	make up
NaOH	--	sodium hydroxide
NPP	--	nuclear power plant
NPPR	--	north piping penetration room
NRC	--	Nuclear Regulatory Commission
NREP	--	National Reliability Evaluation Program
OP	--	operating procedure
OTSG	--	once-through steam generator
PRA	--	probabilistic risk assessment
PSF	--	performance shaping factor
psig	--	pounds per square inch, gage
RB	--	reactor building
RCP	--	reactor coolant pump
RCS	--	reactor coolant system
RF	--	recovery factor
TH	--	temperature hot leg
THERP	--	Technique for Human Error Rate Prediction
UCB	--	uncertainty bound
ZD	--	zero dependence

DISTRIBUTION

U.S. NRC Distribution Contractor
(CDSI) (2200)
7300 Pearl Street
Bethesda, MD 20014
400 copies for AN, RX
247 copies for Author-Selected Distribution

Kazuo Aoki
Mitsubishi Heavy Industries Ltd.
Pittsburgh Representative Office
% Westinghouse Elect. Corp.
Penn Center Bldg. 3
Room 600
Pittsburgh, PA 15230

Arne Anderson P3
Ringhalsverket
Varobadsa
Sweden

Dr. James L. Arnold
201 21st St., NE
Cedar Rapids, IA 52402

Dr. Kiyoji Asai
University of Osaka Prefecture
Mozu, Umemachi
Sakai, Osaka 591
Japan

Dr. William B. Askren
Logistics Res. Br.
USAF Human Resources Lab
AFHRL/LRL
Wright-Patterson AFB, OH 45433

Stuart Asselin
Technology for Energy Corp.
10770 Dutchtown Rd.
Knoxville, TN 37922

Ruta Axelsson
LUTAB
P.O. Box 52
S-161 26 Bromma
Sweden

Dr. Werner Bastl
GRS - Bereich Systeme
Forschungsgelande
8046 Garching
Federal Republic of Germany

Dr. Arthur N. Beare
General Physics Corp.
1 Northgate Park
Chattanooga, TN 37415

David Beattie
Ontario Hydro H-14
700 University Ave.
Toronto, ON M5G 1X6
Canada

B. J. Bell (10 copies)
Risk & Safety Analysis Section
Battelle's Columbus Lab.
505 King Ave.
Columbus, OH 43201

Dr. Jan Berkout
Psychology Dept.
Univ. of South Dakota
Vermillion, SD 57069

C. J. E. Beyers
Licensing Branch (Standards)
Atomic Energy Board
Private Bag X256
Pretoria 0001
Republic of South Africa

Dr. Robert E. Blanchard
M-8 Monticello St.
Del Mar, CA 92014

Terry F. Bott
Los Alamos Nat'l Lab.
Group Q6, Mail Stop K557
P. O. Box 1663
Los Alamos, NM 87545

Dr. Mark Brecht
4350 West 136 St.
Hawthorne, CA 90250

DISTRIBUTION (Continued)

Frank Briscoe
Safety & Reliability Directorate
UKAEA
Wigshaw Lane, Culcheth
Warrington WA3 4NE, Cheshire
England

Dr. Robert Budnitz
Future Resources Associates Inc.
734 The Alameda
Berkeley, CA 94707

T. E. Burnup
Safety & Reliability Directorate
UKAEA
Wigshaw Lane, Culcheth
Warrington WA3 4NE, Cheshire
England

Dr. Hugh Cahill
1585 James Town Drive
Cupertino, CA 95014

Lennart Carlsson
Swedish Nuclear Power Inspectorate
Box 27106
10252 Stockholm
Sweden

Betty P. Chao
Human Factors Lab
Dept. of Indust. Eng. & Opns. Resch.
Virginia Polytechnic Inst. & State U
Blacksburg, VA 24061

W. B. Cheney
Licensing Branch (Standards)
Atomic Energy Board
Private Bag X256
Pretoria 0001
Republic of South Africa

Dr. Julien M. Christensen
Human Factors Office
General Physics Corp.
1010 Woodman Dr. #240
Dayton, OH 45432

Bob Christie
Availability and Reliability Section
Nuclear Engineering Branch
Tennessee Valley Authority
W10C126
400 Commerce Ave.
Knoxville, TN 37902

R. J. Christie
c/o I. A. Watson
UKAEA Safety & Reliability Directorate
Culcheth, Warrington WA3 4NE
Cheshire, England

P. L. Clemens
Chief of Safety
Sverdrup/ARO Inc.
AEDC Division
Arnold AF Station, TN 37389

Dr. E. N. Corlett
Editor, Applied Ergonomics
Department of Engrg. Production
University of Birmingham
P. O. Box 363
Ergbaston, Birmingham B15 2TT
England

Dr. Vincent T. Covello
Office of Scientific, Tech, & Internat'l Affairs
National Science Fdn
1800 G St., NW
Washington, DC 20550

Dr. Michael Cullingford
International Atomic Energy Agency
P.O. Box 100
A-1400 Vienna
Austria

Orville Cypret
Arkansas Power & Light Co.
General Research & Development
P.O. Box 551
Little Rock, AR 72203

G. Dahl
Norsk Hydro
P.O. Box 110
N-3901 Porsgrunn
Norway

B. T. Davies
Dept. of Ergonomics
The University of Birmingham
P.O. Box 363
Birmingham B15 2TT
England

Harry L. Davis
Human Factors Group
Eastman Kodak Company
Kodak Park Division, B-56
Rochester, NY 14650

Alan Debiar (2 copies)
Av. Les Pins de Laurenzane
33170 Gradignan
France

Det norske Veritas
Human Factors (Ergonomics)
P.O. Box 300
N-1322 Høvik
Oslo, Norway

Ruth E. DeWald
7103 Gratiot Rd.
St. Clair, MI 48079

Ed. M. Dougherty, Jr.
Technology for Energy Corporation
10770 Dutchtown Road
Knoxville, TN 37922

Professor Keith Duncan
U.W.I.S.T.
Dept. of Appl. Psych.
Llwyn-y-Grant
Pnylan, Cardiff
South Glamorgan
Wales CF3 7UX

Sharen Eckert
487 Pearl St.
Berea, OH 44017

Dr. Elwyn Edwards
Dept. of Appl. Psychology
Univ. of Aston
Birmingham B4 7EK
England

Dr. Ward Edwards
Social Science Research Inst.
Univ. of Southern California
University Park
Los Angeles, CA 90007

Dr. David Embrey
Human Reliability Assocites Inc.
1 School House
Higher Lane, Dalton, Parbold
Lanc. WN8 7RP
England

Ente Nazionale per L'Energia
Elettrica
Centro Ricerca de Automatica
ENEL - CRA
Via Valv, Peroni, 77
20133 Milano
Italy

Dr. Ralph A. Evans
Editor, IEEE Transactions on Rel.
804 Vickers Ave.
Durham, NC 27701

Dr. Donald E. Farr
Science Applications, Inc.
1710 Goodridge Dr. T-6-1
McLean, VA 22102

L. Felkel
GRS - Bereich Systeme
Forschungsgelande
8046 Garching
Federal Republic of Germany

Dr. Mylen E. Fitzwater
Suite J
1000 Freemont Ave.
Los Altos, CA 94022

James A. Fletcher
12 Pinecrest Ct.
Greenbelt, MD 20770

DISTRIBUTION (Continued)

Drs. Joan and Patrick Foley
Dept. of Industrial Engineering
University of Toronto
Toronto, Ontario,
Canada M5S 1A4

Dr. John D. Folley, Jr.
Applied Science Assoc.
Box 158
Valencia, PA 16059

Haruo Fujimoto
Mitsubishi Atomic Power
Industry Inc.
4-1, Shibakouen 2-Chome
Minato-ku, Tokyo 105
Japan

Prof. Dr. I. Fukuyama
Dept. of Safety Engineering
Yokohama National University
156 Tokiwadai, Hodogaya-ku
Yokohama 240
Japan

Dr. J. B. Fussell
JBF Associates, Inc.
1630 Downtown West Blvd., Suite 108
Knoxville, TN 37919

Stein Gaarder
Veritas Research Div., Section 50
P.O. Box 300
1322 Høvik
Norway

Bernard Gachot
Electricité de France
Direction de l'Equipement
Region de'Equipement
Alpes-Marseille
140, Avenue Viton - B.P. 560
13275 Marseille Cedex 9
France

Paul Gagnolet
Electricité de France
Service de la Production hermique
Departement Surete Nucleaire
71 rue Miromesnil
F-75008 Paris
France

Dr. Brian R. Gaines
Centre for Man Computer Sciences
94 Shakespeare Tower
Barbican,
London EC2Y 8DR
England

J. P. Garde
26 rue Diaz
33000 Bordeaux
France

Dr. Kenneth Gardner
Applied Psychol. Unit
Admiralty Marine Tech.
Establishment
Teddington, Middlesex TW11OLN
England

Dr. B. John Garrick
Pickard, Lowe & Garrick, Inc.
1780 Skypark Blvd.
Irvine, CA 92714

Frank Gavigan
Department of Energy
Mail Stop F-305
Germantown, MD 20767

S. B. Gibson
Risk and Safety Analysis Section
Battelle's Columbus Laboratories
505 King Avenue
Columbus, OH 43201

Dr. R. A. Goldbeck
Ford Aerospace & Communications
Corp.
Engineering Service Div.
1260 Crossman Ave. MS S-33
Sunnyvale, CA 94086

Dr. Timothy Goldsmith
Dept. Psychology
University of New Mexico
Albuquerque, NM 87131

Prof. Etienne P. Grandjean
Dept. of Ergonomics
Swiss Federal Inst. of Tech.
21 Clausius St.
8092 Zurich CH
Switzerland

Hasim Gundagdu
Operations Research Div.
Marmara Scientific and Industrial
Research Institute
P.O. Box 21
Gebze-KOCAELI
Turkey

Dr. James C. Gutmann
Anacapa Sciences
901 Olive St.
Santa Barbara, CA 93102

Dr. G. W. Hannaman
NUS Corp., Suite 250
16885 W. Bernardo Dr.
San Diego, CA 92127

Dr. Douglas H. Harris
Anacapa Sciences, Inc.
P.O. Drawer Q
Santa Barbara, CA 93102

Tosaku Hattori
Industrial Designer
Naka Works
Hitachi Ltd.
882 I Chige
Katsuta, Ibaraki, 312
Japan

Prof. Yoshio Hayashi
Dept. of Administration Engineering
Keio University
3-14-1 Hiyoshi, Kohoku
Yokohama 223
Japan

Matti Heikkila
Institute of Radiation Protection
Department of Reactor Safety
P.O. Box 268
00202 Helsinki 10
Finland

Tor Heimly
Det norske Veritas
300, N-1322 Høvik
Norway

Prof. Carolyn Heising-Goodman
Nuclear Engineering Dept.
MIT
211 Massachusetts Ave.
Cambridge, MA 02139

Dr. O. H. Hellesøy
Mobil Exploration Norway Inc.
Kokstadflaten 9
5065 Blomsterdalen
Norway

C. Hensley
British Nuclear Fuels, Ltd.
Risley, Warrington
England WA3 6AS

E. M. Hinchley
Reactor Control & Safety Systems
Atomic Energy of Canada
Sheridan Park Research Community
Mississauga, ON L5K 1B2
Canada

Prof. Fritz Hjelte
Dept. of Aeronautics
The Royal Institute of Technology
S-100 44 Stockholm 70
Sweden

Prof. Robert R. Holt
Dept. of Psychology
6 Washington Pl., 4th Floor
New York, NY 10003

Eric Hollnagel
Institutt for Energiteknikk
OECD Halden Project
P.O. Box 173
N-1751 Halden
Norway

Dr. Robert Hooke
P.O. Box 1982
Pinehurst, NC 18374

B. C. Hopkins
MATSCO
4271 Bronze Way
Dallas, TX 75237

Dr. Helmut Hörtner
Systems Analysis Section
Gesellschaft fur Reaktorsicherheit (GRS) mbH
Forschungsgelande
8046 Garching
Federal Republic of Germany

Stephen B. Hottman
Systems Research Laboratories, Inc.
2800 Indian Ripple Rd.
Dayton, OH 45440

David M. Hunns
National Centre of Systems Reliability
United Kingdom Atomic Energy Authority
Wigshaw Land, Culcheth
Warrington WA3 4NE, Cheshire
England

Niall Hunt
Baltimore Gas & Electric
P.O. Box 1475
Fort Smallwood Rd. Complex
Baltimore, MD 21203

Dr. D. Ilberg, Head
Systems Safety and Accident Analysis Dept.
Licensing Division
Atomic Energy Commission
P.O. Box 17120
Tel-Aviv
61070 Israel

Rick Imig
Shell Oil Co.
P.O. Box 100
Deer Park, TX 77536

Dr. Tetsuro Itakura
Director, Eng. Dept.
The Japan Atomic Power Co.
Ohtemachi Bldg.
6-1, 1-Chome, Ohtemachi
Chiyoda-ku, Tokyo 100
Japan

Mutsumi Itoh
Control & Electrical Eng. Dept.
Nuclear Energy Group
Toshiba Corp.
13-12, MITA 3-Chome, Minato-ku
Tokyo 108
Japan

William G. Johnson
151 Shelter Cove Drive
Half Moon Bay, CA 94019

Dr. Daniel Kahneman
University of BC
Dept. of Psychology
#154 - 2053 Main Mall
University Campus
Vancouver, BC V6T 1Y7
Canada

Dr. Peter Kafka
Systems Analysis Section
Gesellschaft fur Reaktorsicherheit (GRS) mbH
Forschungsgelande
8046 Garching
Federal Republic of Germany

Dr. Stanley Kaplan
Pickard, Lowe & Garrick
1780 Skypark Blvd.
Irvine, CA 92714

Dr. Gyorgy Karmos (2 copies)
Institute of Psychology
Hungarian Academy of Science
Budapest, Hungary

Dr. Marcel Kinsbourne
Neurophysiology
Hospital for Sick Children
Univ. of Toronto
Canada M5S 1A4

Trevor A. Kletz
Petrochemicals & Plastics Div.
Imperial Chemical Industries Ltd.
P.O. Box 90
Wilton Middlesbrough
Cleveland TS6 8JE
England

George Klopp
Commonwealth Edison
Station Nuclear Engineering
Room 35W
P.O. Box 767
Chicago, IL 60690

Dr. William B. Knowles
School of Social & Behavioral Sciences
California State University, Northridge
Northridge, CA 91330

Dr. Jefferson M. Koonce
Lead Mine Hill Rd.
RFD #3
Amherst, MA 01002

Dr. Frank P. Lees
Department of Chemical Engineering
Loughborough University of Technology
Loughborough LE11 3TU
England

Fernand Leonard
Chef du Departement BR2
Centre d'Etude de l'Energie Nucleaire
Boeretang 200
B-2400 Mol
France

Saul Levine
NUS
4 Research Place
Rockville, MD 20850

Prof. Hal Lewis
Physics Department
University of California
Santa Barbara, CA 93106

Pierre M. Lienart
INPO
1800 Water Place
Atlanta, GA 30339

Bo Llwång
Swedish Nuclear Power Inspectorate
Box 27106
S-10252 Stockholm
Sweden

Linda O. Lund
Lund Consulting, Inc.
1200 Route 46
Clifton, NJ 07013

LUTAB
Attn: Library
P.O. Box 52
S-161 26 Bromma
Sweden

Dr. John Lyman
Eng. and Appl. Sci., UCLA
Los Angeles, CA 90024

James F. Mallay
Nuclear Safety Analysis Center
EPRI
P.O. Box 10412
Palo Alto, CA 94303

Dr. Thomas Mankamo
Technical Research Centre of Finland
VTT/Ltr
Otakaari 5
SF-02150 ESPOO 15
Finland

Dr. D. L. Marriott
22 Mechanical Engrg. Bldg.
Univ. of Ill. at Urbana-Champaign
Urbana, IL 61801

Dr. D. J. Martin
Atomic Energy Control Board
P.O. Box 1046
Ottawa, Canada
KIP 559

Dr. Harry F. Martz
LASL
P.O. Box 1663
Los Alamos, NM 87544

DISTRIBUTION (Continued)

Dr. M. Mazumdar
Dept. of Indus. Engin.
University of Pittsburgh
Pittsburgh, PA 15260

Robert Meyer
Professional Reactor Operator Society
Business & Technology Center
245 E. 6th St., Suite 816
St. Paul, MN 55010

Dr. Lorna A. Middendorf
1040 Berkshire
Grosse Point Park, MI 48230

Dr. C. O. Miller
7722 Bridle Path Lane
McLean, VA 22101

Dr. Robert B. Miller
Colonial House
South Road
Poughkeepsie, NY 12601

Jean-Jacques Mira
Electricité de France
Service de la Production Thermique
71, Rue de Miromesnil
75008 Paris
France

Prof. Richard A. Moll
Dept. of Eng. & Appl. Sci.
Univ. of Wisconsin--Extension
432 North Lake St.
Madison, WI 53706

Dr. Kazuo Monta
Nuclear Eng. Dept.
NAIG Nuclear Research Lab.
4-1, Ukishima-cho Kawasaki-ku,
Kawasaki-shi, Kanagwa-ken
210 Japan

Prof. J. Moraal
Institute for Perception
Soesterberg
Kampweg 5, Postbus 23
Holland

Dr. Ben B. Morgan
Center for Appli. Psych. Stds.
Old Dominion Univ.
Norfolk, VA 23508

G. Richard Mullee
Nuclear Services Dept.
General Electric Co.
175 Curtner Ave., M/C 853
San Jose, CA 92125

William M. Murphy
US Arms Control & Disarmament Agency
State Dept. Bldg.
21st & Virginia Ave., NW
Room 4947
Washington, DC 20451

Philippe Namy
Probabilistic & Risk Anal. Gp.
Framatome S.A.
Tour Fiat
1 Place de la Coupole
Cedex 16, F-92084 Courbevoie
France

Mohammad Nasim
Nuclear Safety & Licensing Div.
Pakistan Atomic Energy Comm.
P.O. Box 1114
Islamabad, Pakistan

Dr. David Navon
University of Haifa
Mount Carmel, Haifa 31999
Israel

Larry Noyes
Philadelphia Elec. Co.
2301 Market St., S12-1
Philadelphia, PA 19101

Nuclear Safety Research Association
Attn: Kazumori Matsuo
P.O. Box 1307
Falls Church, VA 22041

DISTRIBUTION (Continued)

Chuck Oh
Technology for Energy Corp.
10770 Dutchtown Rd.
Knoxville, TN 37922

Reidar Østvik
SINTEF
N7034 Trondheim
NTH
Norway

Magnus Øvreeide
Institutt for Energiteknikk
OECD Halden Reactor Project
P.O. Box 173
N-1751 Halden
Norway

Dr. Ray Parsick
Safeguards Evaluation Section
International Atomic Energy Agency
Wagrannerstrasse 5, P.O. Box 100
A-1400, Vienna
Austria

John Payne, Editor
Nuclear News
Amreican Nuclear Society, Inc.
555 N. Kensington Avenue
La Grange Park, IL 60525

Dr. M. Carr Payne
3035 Farmington Dr., NW
Atlanta, GA 30339

Prof. Charles Perrow
Dept. of Sociology
State Univ. of New York
at Stony Brook
Stony Brook, NY 11794

Dr. Dominique Pignon
Centre National de la Recherche
Scientifique
Laboratoire de Physique
Theoretique de l'Ecole
Normale Superieure
24, rue Lhomond 24
75231 Paris Cedex 05
France

Dr. E. C. Poulton
MRC Applied Psychology Unit
15 Chaucer Road
Cambridge, CB2 2EF
England

Leonard C. Pugh, Sr.
General Electric Co.
175 Curtner Avenue M/C 367
San Jose, CA 95125

Dr. Norman Rasmussen
Nuclear Engineering Dept.
Massachusetts Inst of Tech
Cambridge, MA 02139

T. J. Ravishanker
Ontario Hydro
700 University Ave.
Toronto, ON M5G 1X6
Canada

Prof. J. T. Reason
Dept. of Psychology
University of Manchester
Manchester, M1P 93L
England

Gunter Reichart
GRS - Bereich Systeme
Forschungsgelande
8046 Garching
Federal Republic of Germany

Dr. Frank Restle
Dept. of Psychology
Indiana Univ.
Bloomington, IN 47405

Dr. Kyou H. Rhyi
30, Gyurngi-Dong,
Jongro-ku
Seoul, Korea

Ausra Richards
NUS
4 Research Place
Rockville, MD 20850

DISTRIBUTION (Continued)

Robert C. Roberts
Babcock & Wilcox
P.O. Box 1260
Lynchburg, VA 24505

Prof. Gordon Robinson
Industrial Engineering Dept.
Univ. of Wisconsin
Madison, WI 53706

Louis H. Roddis, Jr.
PE, C Eng
110 Broad St.
Charleston, SC 29401

Prof. Dr. Jan Rosner
Polish Ergonomics Society
UL. Gornoslaska 20
00-484 Warszawa
Poland

Dr. William B. Rouse
1886 Vanderlyn Dr.
Dunwoody, GA 30338

John E. Rudolph
Division of Program Support
Office of Military Application
U.S. Dept. of Energy
Mail Stop A-362
Washington, DC 20545

Dr. Thomas G. Ryan (15 copies)
NRC-RES
DFO - Human Factors Branch
Nicholson Lane
Washington, DC 20555

Bo Rydnert
LUTAB
P.O. Box 52
S-161 26 Bromma
Sweden

Prof. Zeinab Sabri
Iowa State University
Ames, IA 50011

Dr. Mark S. Sanders
Dept. of Psychology
California State University,
Northridge
Northridge, CA 91330

Thomas O. Sargent
Conserv
3 Columbia St.
Hartford, CT 06106

Yusuke Sawaguchi
Nuclear Power Plant Operation
& Maint. Dept.
The Tokyo Electric Power Co.
NO 1-3, 1-Chome, Uchisaiwai-cho
Chiyoda-ku, Tokyo 100
Japan

M. Franz Schneider
Central Safety Services,
Ergonomics Unit
Ontario Hydro
757 MacKay Rd.
Pickering, ON L1W 3C8
Canada

Dr. Lothar Schroeder
Human Factors Group
UNC Nuclear Industries
P.O. Box 490
Richland, WA 99352

Dr. Donald L. Schurman
Applied Science Assoc.
741 Lakefield Rd., Suite C
Westlake Village, CA 91361

Science News
Behavioral Sciences Editor
1719 N Street, NW
Washington, DC 20036

Dr. David A. Seaver
The Maxima Corp.
7315 Wisconsin Ave.
Suite 900N
Bethesda, MD 20014

Dr. Mildred Shaw
Centre for Man Computer Sciences
94 Shakespeare Tower
Barbican,
London EC2Y 8DR, England

Dr. David Shinar
Ben-Gurion University of the Negev
Beer Sheva 84 120
P.O. Box 653
Israel

Wataru Shinoda
Plant Management Dept.
Japan Atomic Power Co.
Othemachi Bldg.
6-1,1-Chome, Othemachi
Chiyoda-ku, Tokyo 100
Japan

Dr. Arnold M. Small
2210 Domingo Rd.
Fullerton, CA 92635

John Spencer
Book Reviews Editor, Ergonomics
Department of Applied Psychology
University of Wales
Institute of Science and Technology
Penylan, Cardiff CP3 7UX
Wales

Dr. Michael Stamatelatos
GA Technologies
P.O. Box 81608
La Jolla, CA 92138

Dr. Larry Stark
University of California
Berkeley, CA 94720

Dr. Michael E. Stephens (10 copies)
Nuclear Safety Division
OECD Nuclear Energy Agency
38, Boulevard Suchet
F-75016 Paris
France

B. B. Stephenson
Con. Ed. Co.
Dresden Station
RR1
Morris, IL 60450

Tord Sterner
ASEA-ATOM
Box 53
S-721 04
Västerås,
Sweden

Catherine Stewart
TRW Human Factors
Mail Stop 523/313
Norton AFB
San Bernardino, CA 92402

Dr. William G. Stillwell
The Maxima Corp.
7315 Wisconsin Ave.
Suite 900N
Bethesda, MD 20014

Jean P. Stolz
Electricité de France
Service de la Production Thermique
71, Rue de Miromesnil
75008 Paris
France

Mitsuo Suzuki
Nuclear Power Division
The Federation of Power Companies
Keidanren Kai Kan Bldg.
9-4, 1-Chome, Ohte-Machi
Chiyoda-ku, Tokyo
Japan

Dr. Atsushi Takeda
Tokai Nuclear Generating Station #2
The Japan Atomic Power Co.
Tokai-mura, Ibaraki-ken
Japan

Dr. Toshihide Takesita
Inst. for Policy Services
Friend Bldg.
2-4-11 Nagata-cho, Chiyoda-ku
Tokyo 100
Japan

DISTRIBUTION (Continued)

Akira Tanabe
Reactor Design Eng. Dept.
Nuclear Energy Group
Toshiba Corp.
Isogo Engineering Center
8, Shinsugita-cho, Isogo-ku
Yokohama 235
Japan

Tomihiro Taniguchi
Nuclear Power Operation,
Administration Office
Agency of Natural Resources
Ministry of International Trade
& Industry
131 Kasumigaseki, Chiyoda-ku
Tokyo 100, Japan

Robert Taylor
Electronics Dept.
Risø National Laboratory
DK4000 Roskilde
Denmark

Dr. David A. Thompson
Industrial Engineering &
Engineering Management
Stanford University
Stanford, CA 94305

Toshiaki Tobioka
Reactor Safety Code Dev. Lab.
Div. of Reactor Safety Evaluation
Tokai Research Establishment, JAERI
Tokai-mura, Naka-gun, Ibaraki-ken
Japan

Dr. Donald A. Topmiller
1576 Burchwood Dr.
Fairborn, OH 45324

Dr. Anne Treisman
University of BC
Dept. of Psychology
#154 - 2053 Main Mall
University Campus
Vancouver BC V6T 1Y7
Canada

Ryosuke Tsutsumi
Nuclear Planning Div.
The Tokyo Electric Power Co.
No 1-3, 1-Chome, Uchisaiwai-cho
Chiyoda, Tokyo 100
Japan

Odd J. Tveit
Statoil
PO Box 300 Forus
4001 Stavanger
Norway

Hiroshi Ujita
Energy Research Laboratory
Hitchi Ltd.
1168 Moriyamacho, Hitachi,
Ibaragi 316 Japan

John D. Vandenberg
21 Moss Avenue
Westfield, NJ 07090

Jan Van Erp
Argonne National Lab.
9700 S. Cass Avenue
Argonne, IL 60439

G. Van Reijen
c/o I. A. Watson
UKAEA Safety & Reliability
Directorate
Culcheth, Warrington WA3 4NE
Cheshire, England

Dr. William E. Vesely, Jr.
Risk and Safety Analysis Section
Battelle's Columbus Laboratories
505 King Ave.
Columbus, OH 43201

W. Vinck
c/o I. A. Watson
UKAEA Safety & Reliability
Directorate
Culcheth, Warrington WA3 4NE
Cheshire, England

Prof. Giuseppe Volta
Euratoin Joint Research Center
ISPRA (VARESR)
Italy

DISTRIBUTION (Continued)

Jiro Wakabayaski
12-19, Shugakuin-Kitafukecho
Sakyo-ku, Kyoto 606
Japan

Dr. Ian B. Wall
ERPI
3412 Hillview Ave.
Palo Alto, CA 94303

Dr. Ray Waller
Los Alamos National Lab.
P.O. Box 1663
Los Alamos, NM 87545

Dr. Boardman C. Wang
Dept. of Anesthesia
New York Univ. Med. Center
560 First Ave.
New York, NY 10016

I. A. Watson
UKAEA
Safety & Reliability Directorate
Wigshaw Lane, Culcheth
Warrington, WA3 4NE Cheshire
England

Dr. Meyer Weinstein
7550 Rainbow Dr.
Cupertino, CA 95014

David Whitfield
Ergonomics Development Unit
The University of Aston
Gosta Green
Birmingham B4 7ET
England

Dr. Walter W. Wierwille
Dept. Indust. Eng. & Opns. Resch.
VPI&SU
Blacksburg, VA 24061

James R. Wilson
Safety Analyst
Exxon Nuclear Idaho, Box 2800
Idaho Falls, ID 83401

Jan Wirstad
Ergonomrad AB
Box 205
S-651 02 Karlstad
Sweden

Dr. David Worledge
EPRI
3412 Hillview Ave.
Palo Alto, CA 94303

John Wreathall
NUS
4 Research Place
Rockville, MD 20850

Jan Wright
Bronnoyvn 20
1315 Nesoya
Norway

Dr. Lawrence Young
M.I.T.
Aero and Astronautics Dept.
Room 32-207
Cambridge, MA 02139

Prof. Takeo Yukimachi
Dept. of Administrative Engineering
Keio University
Hiyoshi, Yokohama
223 Japan

Sandia National Laboratories:

3141 L. Erickson (5)
3151 W. L. Garner (3)
3440 L. M. Jercinovic
3442 D. L. Rost
3530 L. V. Rigby
7200 J. M. Wiesen
7210 A. J. Clark, Jr.
7220 R. R. Prairie
7222 G. T. Merren
7223 R. G. Easterling
7223 B. H. Finley
7223 H. E. Guttmann
7223 D. P. Miller
7223 A. D. Swain (3)
7223 L. M. Weston
7230 W. L. Stevens
7250 W. C. Kraft

DISTRIBUTION (Continued)

7260 R. H. Schultz
8100 D. M. Olson
8214 M. A. Pound
8322 F. J. Murar
8329 O. Schreiber
9268 C. E. Olson
9400 A. W. Synder
9410 D. J. McCloskey
9411 A. S. Benjamin
9411 S. W. Hatch
9412 J. W. Hickman
9412 N. L. Brisbin
9412 W. R. Cramond
9412 F. T. Harper
9412 A. M. Kolaczkowski
9412 G. J. Kolb
9412 S. H. McAhren
9412 A. C. Payne, Jr.
9412 R. G. Spulak
9412 T. A. Wheeler
9413 N. R. Ortiz
9414 G. B. Varnado
9415 D. C. Aldrich
9416 L. D. Chapman
9416 B. J. Roscue
9420 J. V. Walker
9440 D. A. Dahlgren
9443 D. C. Carlson

NRC FORM 335 (7 77)

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER *(Assigned by DDC)*
NUREG/CR-2254, SAND81-1655
Final Report

4. TITLE AND SUBTITLE *(Add Volume No., if appropriate)*
A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants

2. *(Leave blank)*

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S)
Barbara Jean Bell and Alan D. Swain

5. DATE REPORT COMPLETED
MONTH: April | YEAR: 1983

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
Sandia National Laboratories
Statistics, Computing and Human Factors
Division (7223)
Albuquerque, NM 87185

DATE REPORT ISSUED
MONTH | YEAR

6. *(Leave blank)*

8. *(Leave blank)*

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
Office of Nuclear Regulatory Research
(Division of Facility Operations)
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

10. PROJECT/TASK/WORK UNIT NO.

11. CONTRACT NO.
A-1188

13. TYPE OF REPORT
Final Report (replaces Draft for Interim Use and Comment dtd December 1981

PERIOD COVERED *(Inclusive dates)*
January 1982 - May 1983

15. SUPPLEMENTARY NOTES

14. *(Leave blank)*

16. ABSTRACT *(200 words or less)*

This document describes in detail a procedure to be followed in conducting a human reliability analysis as part of a probabilistic risk assessment when such an analysis is performed according to the methods described in NUREG/CR-1278, "Handbook for Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications". An overview of the procedure describing the major elements of a human reliability analysis is presented along with a detailed description of each element and an example of an actual analysis. An appendix consists of some sample human reliability analysis problems for further study.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

probabilistic risk assessment
human reliability analysis
human factors
nuclear power

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT
Unlimited

19. SECURITY CLASS *(This report)*
Unclassified

21. NO. OF PAGES
127

20. SECURITY CLASS *(This page)*
Unclassified

22. PRICE
$

NRC FORM 335 (7 77)

☆ U.S. GOVERNMENT PRINTING OFFICE: 1983-0-676-027/562

Org Bldg Name Rec'd by Org Bldg Name Rec'd by

120555078877 1 1AN1RX
US NRC
ADM-DIV OF TIDC
POLICY & PUB MGT BR-PDR NUREG
W-501
WASHINGTON DC 20555