



GOVERNMENT OF INDIA

TEC. DOC. NO. AERB/NPP/TD/O-2

**AERB TECHNICAL DOCUMENT**

**HUMAN RELIABILITY ANALYSIS : A COMPENDIUM  
OF  
METHODS, DATA AND EVENT STUDIES  
FOR  
NUCLEAR POWER PLANTS**



**ATOMIC ENERGY REGULATORY BOARD**

**AERB TECHNICAL DOCUMENT NO. AERB/NPP/TD/O-2**

**HUMAN RELIABILITY ANALYSIS : A COMPENDIUM  
OF  
METHODS, DATA AND EVENT STUDIES  
FOR  
NUCLEAR POWER PLANTS**

**Atomic Energy Regulatory Board  
Mumbai 400 094  
India**

**March 2008**

**Price:**

**Orders for this technical documents should be addressed to:**

**The Administrative Officer  
Atomic Energy Regulatory Board  
Niyamak Bhavan  
Anushaktinagar  
Mumbai - 400 094  
India**

## FOREWORD

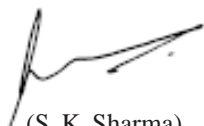
The Atomic Energy Regulatory Board (AERB) constituted by the Government of India via Statutory Order No. 4772 dated November 15, 1983 is entrusted with the responsibility of enforcing safety and carrying out regulatory functions envisaged under the Atomic Energy Act, 1962. AERB is responsible for enforcing safety in all atomic energy related activities within India as well as for enforcing the provisions of the Factories Act, 1948 in the units of the Department of Atomic Energy (DAE), that are under the purview of AERB. In discharging these responsibilities, AERB has been drawing up codes, standards, guides, manuals and other safety related technical documents to facilitate the concerned organisations in implementing the relevant safety regulations.

AERB is in the process of developing a manual to provide guidelines for the performance and review of Probabilistic Safety Assessment (PSA) of nuclear power plants and other nuclear facilities. It was also realised that many of the significant events in nuclear power plants are due to less than adequate human performance or incorrect human action, and that there is a need to incorporate Human Reliability Analysis (HRA) in PSA by applying human reliability methods and data. Towards this end, AERB commissioned this study and preparation of a technical document on HRA. This technical document is intended to support analysts in performing or reviewing human reliability analysis and assessment studies and supplement the safety manual on guidelines for probabilistic safety assessment.

This document has been primarily written to fulfil the existing need of analysts, for a document on HRA having specific reference to the Indian context. The document therefore presents HRA methods and data most useful for application in HRA studies for Indian NPPs. Examples of case studies for Indian NPPs have been given to better illustrate the application of HRA methods. Experience in developing a human reliability database for Indian NPPs, and results of analysis of the data collected, are presented. Data from some published sources are also given in the report.

A review and analysis of plant events due to human error and incorrect human performance can yield valuable insight into ways for improving human reliability and safety in plant operation. This document details a study of some such events in KAPS. The human error related event data has been analysed and human error probabilities are evaluated. As case studies, HRA has been carried out for two of the events.

This document has been prepared by Shri K. Subramaniam, Former Head, Operator Support Systems and Instrumentation Section, Reactor Safety Division, BARC. Subsequently, it was reviewed by the PSA Committee of AERB and experts in this field from various units of DAE. AERB thanks all the individuals who helped in the drafting and finalisation of this technical document.



(S. K. Sharma)  
Chairman, AERB

## DEFINITIONS

### **Accident**

An unplanned event resulting in (or having potential to result in) personal injury or damage to equipment, which may or may not cause release of unacceptable quantities of radioactive material or toxic/hazardous chemicals.

### **Common Cause Failures (CCF)**

The failure of a number of devices or components to perform their functions as a result of a single specific event or cause.

### **Confidence Limit**

A number that delimits a parameter with some amount of confidence.

### **Emergency**

A situation which endangers or is likely to endanger safety of the site personnel, the nuclear/radiation facility, or the public and the environment.

### **Error of Commission**

An error, that amounts to an unintended action excluding inaction. It includes selection error, error of sequence, time error and qualitative error.

### **Error of Omission**

An error that amounts to omitting a part or entire task.

### **Event**

Occurrence of an unplanned activity or deviations from normalcy. It may be one single occurrence or a sequence of related occurrences. Depending on the severity in deviations and consequences, the event may be classified as an anomaly, an incident or an accident in ascending order.

### **Event Tree**

Inductive logic model that orderly represents event sequence branches leading to end state arising from success or failure of mitigating actions required for each group of initiating events.

### **Fault Tree**

Deductive model which starts with a most undesired event (system unavailability) known as 'top event' and proceeds downwards till all the credible combinations of basic events leading to the top event are depicted.

### **Hazard**

Situation or source, which is potentially dangerous for human, society and/or the environment.

### **Human Behaviour**

The performance, i.e., action or response of human operator to occurrence of event (s).

### **Human Reliability**

The probability that a human operator will perform a required mission under given conditions in a given time interval.

### **Human Reliability Assessment/Analysis**

Assessment concentrating on the human errors liable to be committed by the operator having a mission to fulfill on a system.

**Incident**

Events that are distinguished from accidents in terms of being less severe. The incident, although not directly or immediately affecting plant safety, has the potential of leading to accident conditions with further failure of safety system(s).

**Initiating Event/Initiator**

An identified event that leads to anticipated operational occurrences or accident conditions and challenges safety functions.

**Postulated Initiating Events (PIEs)**

Identified events during design that lead to anticipated operational occurrences or accident conditions, and their consequential failure effects.

**Probabilistic Risk Assessment (PRA)/Probabilistic Safety Assessment (PSA)**

A comprehensive structured approach to identifying failure scenarios constituting a conceptual and mathematical tool for deriving numerical estimates of risk. The terms PRA and PSA are interchangeably used.

**Redundancy**

Provision of alternative structures, systems, components of identical attributes, so that any one can perform the required function, regardless of the state of operation or failure of the other.

**Reliability**

The probability that a structure, system, component or facility will perform its intended (specified) function satisfactorily for a specified period under the specified conditions.

**Response Time**

The time required for a system component instrumentation to achieve a specified output state from the time it receives a signal.

**Root Cause**

The fundamental cause of an event, which, if corrected, will prevent its recurrence, i.e. the failure to detect and correct the relevant latent weakness (es) (undetected degradation of an element of safety layer) and the reasons for the failure.

**Sensitivity Analysis**

A quantitative examination of how the behaviour of a system varies with change, usually in the values of governing parameters.

**Uncertainty Analysis**

An analysis to estimate the uncertainties and error bounds of the quantities involved in, and the results from, the solution of a problem.

**Walkdown**

A step or process during which data is gathered, assumptions on component capabilities are checked and analysis is performed (e.g. walkdown for PSA with respect to component capability assessment).

## LIST OF ABBREVIATIONS

AFS	- Auxiliary Feedwater System
AO	- Auxiliary Operator
AOT	- Allowed Outage Time
ASDV	- Atmospheric Steam Discharge Valve
ASEP	- Accident Sequence Evaluation Programme
ATHEANA	- A Technique of Human Error Analysis
BDBA	- Beyond Design Basis Accident
BE	- Basic Event
BHEP	- Basic Human Error Probability
CAM	- Controlled Addition Mode
CCF	- Common Cause Failure
CD	- Complete Dependence
CDF	- Core Damage Frequency
CEP	- Cognitive Error Potential
CHEP	- Conditional Human Error Probability
CICA	- Caracterisque Importante de la Conduite Accidentale, i.e. Important Feature for Emergency Operation
CMF	- Common Mode Failure
COCOM	- Contextual Control Model
CPC	- Common Performance Condition
CR	- Control Room
CREAM	- Cognitive Reliability and Error Analysis Method
CRO	- Control Room Operator
CSDV	- Condenser Steam Dump Valve
CSNI	- Committee on Safety of Nuclear Installations
EDF	- Electricite de France
EEM	- External Error Mode
EF	- Error Factor
EFC	- Error Forcing Condition/Error Forcing Context
EOP	- Emergency Operating Procedure
EOS	- Emergency Operation System
ER	- Event Report
ERA	- Error Reduction Analysis
ERM	- Error Reduction Measure
ET	- Event Tree
FCO	- Fuel Change Order

FP	- Failure Probability
FT	- Fault Tree
HCI	- Human Computer Interaction
HCR	- Human Cognitive Reliability
HD	- High Dependence
HE	- Human Error
HEA	- Human Error Analysis
HED	- Human Engineering Deficiency
HEP	- Human Error Probability
HER	- Human Error Rate
HERF	- Human Error Reporting Form
HF	- Human Factor
HFE	- Human Failure Event
HI	- Human Interaction
HMI	- Human Machine Interface
HPES	- Human Performance Evaluation System
HRA	- Human Reliability Analysis/Human Reliability Assessment
HRAET	- Human Reliability Analysis Event Tree
HRMS	- Human Reliability Management System
IF	- Influence Factor
KBB	- Knowledge Based Behaviour
LB	- Lower Bound
LC	- Local Control
LD	- Low Dependence
LER	- Licensee Event Report
LO	- Local Operator
LOCA	- Loss of Coolant Accident
MAPPS	- Maintenance Analysis of Personnel Performance Simulation
MCR	- Main Control Room
MD	- Moderate Dependence
MERMOS	- Methode d'Evaluation de la Realisation des Missions Operateur La Surete, i.e. Method for Assessing Performance of Human Factor Missions for Safety
MMI	- Man Machine Interface
MOV	- Motor Operated Valve
NHEP	- Nominal Human Error Probability
NKSC	- Narora Kakrapar Safety Committee
NPP	- Nuclear Power Plant
NUCLARR	- Nuclear Computerised Library for Assessing Reactor Reliability



OAT	- Operator Action Tree
ORE	- Operator Reliability Experiment
PC	- Paired Comparisons
PEM	- Psychological Error Mechanism
PRA	- Probabilistic Risk Assessment
PSA	- Probabilistic Safety Assessment
PSF	- Performance Shaping Factor
PWR	- Pressurised Water Reactor
RBB	- Rule Based Behaviour
RCAC	- Root Cause Analysis Committee
RCS	- Reactor Coolant System
RF	- Recovery Factor
SAD	- Strategy Action Diagnosis (Model)
SBB	- Skill Based Behaviour
SER	- Significant Event Report
SG	- Steam Generator
SGTR	- Steam Generator Tube Rupture
SHARP	- Systematic Human Action Reliability Procedure
SLIM-MAUD	- Success Likelihood Index Methodology using Multi Attribute Utility Decomposition
SLIM-SARAH	- Success Likelihood Index Methodology using Systematic Approach to Reliability Assessment of Humans
SMoC	- Simple Model of Cognition
SORC	- Station Operation Review Committee
SPDS	- Safety Parameter Display System
SRK	- Skill, Rule, Knowledge (Levels)
SRUOR	- Safety Related Unusual Occurrence Report
SS	- Shift Supervisor
TA	- Task Analysis
TFP	- Total Failure Probability
THERP	- Technique for Human Error Rate Prediction
TMI	- Three Mile Island
TRC	- Time Reliability Curve/Time Reliability Correlation
TRF	- Total Recovery Factor
UB	- Upper Bound
UCB	- Uncertainty Bound
UOR	- Unusual Occurrence Report
ZD	- Zero Dependence

# CONTENTS

FOREWORD .....	i
DEFINITIONS .....	ii
LIST OF ABBREVIATIONS .....	iv
1. INTRODUCTION .....	1
1.1 General .....	1
1.2 Objectives .....	1
1.3 Scope .....	1
1.4 Structure .....	1
2. HUMAN RELIABILITY CONCEPTS .....	3
2.1 Introduction to Human Reliability Analysis (HRA) .....	3
2.2 The HRA Process .....	3
2.3 Frameworks for Integration of HRA into PSA .....	11
3. METHODS AND MODELS FOR QUANTIFICATION OF HUMAN RELIABILITY .....	18
3.1 Introduction .....	18
3.2 Technique for Human Error Rate Prediction (THERP) .....	19
3.3 Accident Sequence Evaluation Programme (ASEP) .....	24
3.4 Human Cognitive Reliability (HCR) Method .....	38
3.5 Expert Elicitation Methods .....	40
3.6 An Overview of the State of HRA and Development of Second Generation HRA methods .....	43
3.7 A Technique for Human Error ANALysis (ATHEANA) .....	48
3.8 Cognitive Reliability and Error Analysis Method (CREAM) .....	50
3.9 MERMOS (Method for Assessment of Performance of Human Factor Missions for Safety) .....	55
3.10 Guidance on Selection and Use of Human Reliability Assessment Methods .....	62
3.11 Further Needs of HRA .....	68
4. DATA FOR HUMAN RELIABILITY ANALYSIS .....	70
4.1 Types, Uses and Sources of Data .....	70
4.2 Generic and Specific Data .....	70
4.3 Data from Plant Operating Experience .....	71
4.4 Data Collection Systems .....	72
4.5 Human Error Probability Data .....	72
4.6 Data Collection in Indian Nuclear Power Plants .....	73
4.7 Currently Used Databases .....	80
5. APPLICATION OF HRA DATA AND METHODOLOGIES TO CASE STUDIES IN HRA .....	87
5.1 Application of HRA Data .....	87
5.2 Case Studies in HRA .....	87
6. STUDIES OF PLANT EVENTS TO IMPROVE SAFETY IN A REFERENCE NUCLEAR POWER PLANT (KAPS) .....	130
6.1 Introduction .....	130

6.2	Collection and Tabulation of Data on Human Errors in Significant Events in KAPS .....	130
6.3	Case Studies of Detailed HRA for Two Human Performance Related Events which occurred in KAPS .....	145
APPENDIX - 1	CLASSIFICATION OF HRA METHODS .....	150
APPENDIX - 2.1	OUTLINE OF HUMAN ERROR TAXONOMY .....	151
APPENDIX - 2.2	HUMAN ERROR REPORTING FORM FOR NUCLEAR POWER PLANT .....	154
APPENDIX - 2.3	COMPLETED HUMAN ERROR REPORTING FORM FOR TYPICAL PLANT EVENT .....	159
APPENDIX - 3.1	TABULAR FORMAT USED FOR ORGANISING HUMAN ERROR/HUMAN PERFORMANCE EVENT DATA .....	162
APPENDIX - 3.2	SUMMARY OF RESULTS OF ANALYSIS OF PLANT EVENT DATA .....	164
APPENDIX - 4	PLANT SPECIFIC HUMAN ERROR PROBABILITIES .....	167
APPENDIX - 5	THERP HANDBOOK.....	168
APPENDIX - 6	ACCIDENT SEQUENCE EVALUATION PROGRAMME (ASEP) SCREENING AND NOMINAL DIAGNOSIS MODELS AND HEP TABLES, HCR CORRELATION AND EDF TIME RELIABILITY CURVES .....	186
APPENDIX - 7	TABLE OF COGNITIVE FAILURE PROBABILITIES - NOMINAL VALUES AND UNCERTAINTY BOUNDS FOR COGNITIVE FUNCTION FAILURES .....	194
ANNEXURE - 1	NUCLEAR COMPUTERISED LIBRARY FOR ASSESSING REACTOR RELIABILITY (NUCLARR)- SAMPLE DATA TABLES .....	195
ANNEXURE - 2	TABLE OF DATA FOR PRELIMINARY QUANTIFICATION OF SIMPLE HUMAN INTERACTIONS IN PICKERING GENERATING STATION HRA .....	197
ANNEXURE - 3	MATRIX OF HEP DATA FOR PRELIMINARY POST-IE QUANTIFICATION IN CANDU HRA .....	198
REFERENCES	.....	199
BIBLIOGRAPHY	.....	201
LIST OF PARTICIPANTS	.....	202
COMMITTEE ON PSA FOR NUCLEAR FACILITIES	.....	202
PROVISIONAL LIST OF AERB SAFETY CODES, GUIDES, MANUALS AND TECHNICAL DOCUMENTS ON OPERATION OF NUCLEAR POWER PLANTS .....		203

# 1. INTRODUCTION

## 1.1 General

Human errors are identified from event analyses as a major contributor to risk of accidents in nuclear power plants. Estimates of the fraction of system failures arising due to human failures vary, but many analysts have indicated that it can be as high as 50 % for full power operation and 70 % for low power and shutdown operations. It is therefore important in Probabilistic Safety Assessments (PSAs) to identify human errors, quantify their likelihood in terms of Human Error Probabilities (HEPs) and correctly incorporate the HEPs in the assessment of risk. It is also important to analyse each human error event that occurs in an operating plant, arrive at its root cause and implement suitable design or operational changes, in order to reduce likelihood of error. All these functions are achievable through Human Reliability Analysis (HRA).

HRA has been primarily applied in PSA to quantify human reliability in event trees and fault trees to assess its impact on plant risk, e.g. system unavailability, Core Damage Frequency (CDF) and radioactivity release frequency. However, human reliability in areas like design and construction activities also needs to be evaluated.

The application of HRA in PSA requires quality data on human error/human reliability. Data collection schemes and databases for component and system failures are well organised and quite well implemented in a comparative sense, but the same for human errors/failure probabilities are not. Hence, there is a need to develop improved human reliability databases through systematic collection, review, classification recording and analysis of human error and human reliability data. There is also a need to analyse plant events associated with errors in human actions and to recommend appropriate measures for effecting improvements to safety in plant operation.

A majority of HRA methods were developed in the eighties, but many in practice were not sufficiently effective and the need for substantial improvements was gradually realised. HRA had been developed to fulfil the need to describe incorrect human actions in the context of PSA and produce the human action probabilities it needed. The drawbacks of the methods used however, were brought to the fore in 1990, and subsequently led to the development of new HRA methods. These methods, commonly called second-generation HRA methods, have attempted to achieve a better integration of HRA practices and behavioural/cognitive science theory.

## 1.2 Objectives

The primary objective of this document is to provide a compendium on human reliability methods, data and applications that would better enable human reliability analysts to perform and review human reliability analysis and assessment studies and make available to management adequate insights to decision making related to minimising human error probabilities and enhancing human performance and plant safety.

In view of the more recent developments in the field, the document also includes a study of second-generation HRA methods. Other objectives are to detail the systematic collection, review, classification, recording and analysis of human error data for Indian NPPs and derivation of plant specific HEPs, and present studies on plant event data analyses to improve safety in operation, for an Indian nuclear power plant.

## 1.3 Scope

The document will be primarily applicable to nuclear power plants and research reactors. However the contents of the document will be useful in HRA of other nuclear and non-nuclear facilities.

## 1.4 Structure

The document comprises six sections, seven appendices and three annexures.

Section 1 is the introductory section covering general information, objectives, scope and the structure of the document.

Section 2 presents the basic concepts of human reliability and human error, describes the steps involved in the HRA process and discusses two main frameworks, SHARP and IAEA, used to structure the HRA process and integrate it into PSA.

Section 3 covers different methods and models for quantification of human reliability. These include the Technique for Human Error Rate Prediction (THERP), Accident Sequence Evaluation Programme (ASEP), Human Cognitive Reliability (HCR) methods and an expert elicitation method; Success Likelihood Index Methodology (SLIM). This is followed by an overview of the present state of HRA and a discussion on the new (second generation) HRA methods being developed. Three different second-generation HRA approaches are introduced and their main features are described.

Section 4 discusses the subject of data for HRA. The chapter covers types of data, data sources and data collection from operating experience. Data collection from Indian NPPs, using plant event reports as a data source, is presented. Currently used HRA databases are discussed and a section on databases for review and analysis of HRA studies is included.

Section 5 presents eight case studies on the application of HRA. Of these, four case studies pertain to Indian NPPs. The remaining four case studies have been drawn from textbooks or papers authored by experts in the field and are included to show how HRA methods are used. Three of these studies present the application of commonly used first generation HRA methods. The fourth case study from the literature shows how the second-generation HRA method “Cognitive Reliability and Error Analysis Method (CREAM)” is applied to an accident management task in PWR.

Section 6 presents a detailed study of significant plant events that relate to human error/human performance for KAPS. The study has been carried out with a view to improving human performance and operational safety in the plant. Human error probabilities are evaluated for the human errors observed in the events. This is done by directly using handbook and other published data available. In addition, for two plant events, more detailed stepwise HRA has been carried out including the evaluation of HEPs for the human errors made in handling the events. These are also presented

Appendix-1 gives a classification of HRA methods. Appendix-2 presents a human error taxonomy, the Human Error Reporting Form (HERF) used in data collection from plant events, as well as a completed HERF for an actual plant event. Appendix-3 gives the summary of results of analysis of event data pertaining to RAPS and MAPS. Appendix-4 gives a table of plant specific HEPs calculated from RAPS and MAPS data. Appendix-5 gives an extract of Chapter 20 from the Technique for Human Error Rate Prediction (THERP) Handbook [25]. It comprises 27 tables of data. Appendix-6 presents data from Accident Sequence Evaluation Programme (ASEP) HRA Procedure [26] including the Screening and Nominal Diagnosis curves, Human Cognitive Reliability (HCR) and Electricite de France (EDF) Time Reliability Correlations (TRCs). Appendix-7 gives a table of nominal values and uncertainty bounds for cognitive function failures from Hollnagel [8].

Annexure-1 presents sample data from Nuclear Computerised Library for Assessing Reactor Reliability (NUCLARR) database. Annexure-2 gives a table of data used for preliminary quantification of simple (pre-initiating event) interactions in Pickering Generating Station and Annexure-3 gives a matrix of HEP data used for quantification of post-initiating event human interactions in early CANDU HRA.

## 2. HUMAN RELIABILITY CONCEPTS

### 2.1 Introduction to Human Reliability Analysis (HRA)

Human error, which is defined as a departure of human behaviour from what it should be, is identified from event analyses, as a major contributor to significant events in nuclear power plants. Human operators can exacerbate initiating events or even be their initiators. But they can also effect restoration and recovery when serious events occur. The human contribution to safety of nuclear power plants can be best studied, understood, assessed and quantified using techniques of Human Reliability Analysis (HRA). HRA has become an essential part of every Probabilistic Safety Assessment (PSA) and is used to identify human errors, quantify their likelihood in terms of Human Error Probabilities (HEPs) and correctly incorporate the HEPs in the assessment of risk.

HRA in a PSA therefore has a threefold purpose.

- Identifying the critical human interactions in the system and how they can fail.
- Quantifying their probabilities of failure in terms of HEPs.
- Determining how to improve human reliability, if performance needs improvement (i.e. when PSA calculated risk is high and if human performance or potential human error is contributing significantly to risk).

In operating nuclear power plants, each event is analysed and its root cause is arrived at through Root Cause Analysis. In addition, it is also important to analyse each human error event using the methods of human reliability analysis and implement suitable design or operational changes to reduce the likelihood of human error.

### 2.2 The HRA Process

#### 2.2.1 General Introduction to Human Error, Performance Shaping Factors and Error Taxonomy

Humans make errors due to a variety of causes. Some of the causes are internal to the individual, e.g. operator unable to concentrate due to insufficient sleep the previous night, and some are external to the individual, e.g. equipment controls not easily and comfortably accessible.

The human's performance in a work situation is influenced by factors called Performance Shaping Factors (PSFs). A PSF is any factor that shapes (influences) human performance, making it reliable or error prone. The factors can be hypothesised as external factors (relating to situational and equipment characteristics), stressor factors (relating to psychological and physiological characteristics) and internal factors (characteristics of people resulting from internal and external influences). In other words, PSFs are divided into External PSFs, Internal PSFs and Stressor PSFs. The set of PSFs present in the work situation can greatly affect how safely or otherwise a system is operated.

External PSFs include factors like work environment (ambient temperature, lighting and air quality), quality of the Human Machine Interface (HMI) and quality of procedures. Internal PSFs include factors like motivation, emotional state and the physical condition of the individual. Stressor PSFs are generally overlooked as they are difficult to understand, but their influence is considerable, particularly in hazardous situations. A stressor is a stress on the human while performing a task. The origin of stress can be psychological (suddenness of onset of a disturbance, task overload, pressure of time, fear of failure, repetitive meaningless work, long uneventful periods during monitoring and distractions that affect attentiveness) or physiological (fatigue, discomfort, vibration and disruption of the sleep/wake cycle). The interplay of PSFs has a net negative, positive, or mixed impact on human performance. Human error occurs when the operator and the task are mismatched. PSFs influence the degree to which the two are matched (A poorly designed system is setup for human error/failure).

The identification of potential human errors is an important step in HRA. Errors, which alone or in conjunction with hardware/software failures, can lead to degraded system state, are to be identified. A

classification or taxonomy of human errors will aid human error identification and analysis. A typical taxonomy for observable manifestation of human error (external error mode) and psychological error mechanism (operator's internal failure mode) would be as follows.

#### External error mode (EEM) taxonomy

- |                     |   |
|---------------------|---|
| Error of omission   | Omits entire task<br>Omits a step in the task   |
| Error of commission | Selection error <ul style="list-style-type: none"><li>• selects wrong control (e.g. transposition error)</li><li>• mispositions control (e.g. reversal error)</li><li>• issues wrong command or information (e.g. communication error)</li></ul> Sequence error <ul style="list-style-type: none"><li>• incorrect sequencing of actions</li></ul> Time error <ul style="list-style-type: none"><li>• action too early</li><li>• action too late</li></ul> Quantitative error <ul style="list-style-type: none"><li>• action incorrectly performed (e.g. too much or too little)</li></ul> |

#### Extraneous acts rule violation

#### Psychological error mechanism (PEM) taxonomy

##### Attention failure/distraction

##### Perception failure

- misperception
- out of sight bias

Misdiagnosis, where diagnosis is the capacity or mechanism to understand what is perceived and realise the implications of a perceived situation.

- misinterpretation, miscuing
- signal discrimination failure

##### Memory failure

- failure to recall/memory lapse
- inaccurate recall (mistake among alternatives)

Incorrect/incomplete mental model (a model being a representation of the description of the phenomena and interactions of a real system used to predict or assess its behaviour under specified, often hypothetical conditions).

- level of knowledge inadequate for recognition of plant state

##### Misjudgement/misinferencing

Stereotype takeover

- assumptions
- mindset

Indecision

- lack of knowledge

Uncertainty

Cognitive overload (where cognition is the capacity or mechanism that leads to knowledge).

- observation failure

Invoking a shortcut

- pressure of time

Spatial misorientation

- operator mistakes the control panel for another one, which has a similar layout

Risk recognition failure

- overconfidence/oversimplification
- risk taking

In addition to the EEM and PEM taxonomies, it is possible to classify human error with respect to type of behaviour. For PSA purposes, Rasmussen's Step Ladder Model [11] provides a generally accepted framework to identify different types of behaviour and associated error mechanisms. The model identifies three kinds of behaviour, which are explained below.

Skill based behaviour

A skill is an ingrained ability (or capacity) to perform a specific action, which may be innate or learned. In skill based behaviour, there is a close coupling between the sensory input and response action. Skill based behaviour does not depend on the complexity of the task, but rather on the level of training and extent of practice in performing the task.

Rule based behaviour

It is a (hypothesised) mode of behaviour that amounts to following situation action pairs, or behaviour that is governed by a set of rules or associations, which are well known and followed. A major difference between rule based and skill based behaviour stems from the degree of practice.

Knowledge based behaviour

When symptoms are ambiguous or complex, state of plant is complicated by multiple failures or unusual events, or the instruments give only indirect readings of parameter values, the operator has to rely on his knowledge and understanding and his behaviour is determined by more complex cognitive processes

Following the skill, rule and knowledge model, errors may also be identified as arising in one of three cognitive levels of human behaviour and denoted as skill based, rule based and knowledge based (diagnosis and decision) errors. The error mechanisms associated with Rasmussen's model of human behaviour are of two kinds; slips and mistakes.

Slip: A slip is an error in implementing a set goal-plan, decision or intention; say, intention correct but execution failed, e.g. a failure to open a valve. A type of slip is lapse; an omission, e.g. forgetting to open a valve.



Mistake : A mistake is an error in establishing a course of action, e.g. an error in diagnosis, decision making or planning. A mistake occurs when a correct and necessary action is performed on a wrong system (wrong system is selected) or an erroneous action (wrong action is selected) is performed on the right system.

Both slips and mistakes are observable by their external effects, i.e. EEMs. Thus, inadvertent closure of the wrong valve (say, valve B is closed when operator intended to close valve A) is a slip error with its external error mode an error of commission. The external error mode of a lapse, a type of slip error is an error of omission (e.g. operator intended to open valve A, but does not do so). A mistake, such as an erroneous action executed on the right equipment, manifests itself as an error of commission.

Slips are more likely to occur during the execution of skill based actions. Mistakes can be made when rule based and knowledge based actions are planned and involve more serious error mechanisms that lead to incorrect understanding of a situation followed by an incorrect plan of action. Mistakes can also occur by an inappropriate selection (based on incomplete information) of familiar rules or procedures.

Slips usually arise in following the intended protocol or executing the intended procedure and occur in a less time-constrained environment (i.e. a situation in which there is no constraint on time available for performing the intended task). Therefore their error probabilities would be less time dependent. Mistakes, on the other hand, occur in a time-constrained environment and are more time dependent (it takes time to think of an appropriate response in an unfamiliar situation).

Any task may in general consist of 'slip likely' and 'mistake likely' subtasks, and all subtasks take time to perform. The time dependency therefore needs to be taken into account in the overall approach to quantification.

In HRA for PSA, the potential for error recovery for different errors is to be duly considered. Recovery is defined to be the accommodation of a failure or otherwise undesired performance in hardware or software by restoring the failed hardware or software or finding an alternative to achieving the function of the hardware or software error recovery is a recovery from one's own or another's error. Slips and lapses can usually be recovered from fairly quickly provided there are appropriate feedbacks and plant behaviour is reversible. Mistakes are less easily recovered from in the short term - 'mindset' problems can make operators persist with an inappropriate plan even in the face of contradictory information. Recovery actions have to be positive and powerful to be reliable e.g. based on key alarms and backed up by adequate operator training in execution of the recovery actions.

### 2.2.2 HRA in the Framework of PSA

In a PSA, accident sequences (i.e. event sequences leading to accident) are modelled using logic structures. The sequences start with an initiating event and progress through plant responses and mitigating actions to success or failure state. Accident sequence models consider the following.

- the initiators (initiating events or faults);
- the demanded safety functions and additional failures that occur after the initiating event; and
- the unreliability or unavailability of equipment/systems required to operate after event initiation.

Logic structures used for PSA modelling include event trees and fault trees. The event sequence is represented as a binary (success/failure) event tree. In the cases where an event involves a human interaction or intervention, HRA is required to provide the appropriate HEP value. To do this the human interaction is modelled as an HRA Event Tree (HRAET) or an Operator Action Tree (OAT).

Manual actions/interventions (e.g. switching off a pump or opening a valve) in an event sequence are distinct and end in success or failure. They are represented as nodes in the event tree. However, for a human interaction, which involves cognitive functions, the approach in PSA has been to decompose the human interaction into its assumed components and describe the relations between these components by means of a small event tree. For example, such human interactions can be broken down into four

segments; diagnosis, decision, execution and (possibly) recovery. A result of this kind of decomposition is that it becomes necessary to find error probability data for each segment (i.e. diagnosis, decision, execution and recovery). However, models used in some of the newer second-generation HRA approaches, are seen to reduce or even do away with the need for specific sets of data for the segments mentioned above [9].

PSAs are performed for a variety of reasons, from meeting safety-goal regulations to effecting improvements in the plant, and requirements of HRA are defined by the purpose of the PSA. In the broader perspective humans are involved not only in operation of a process but also design, construction and management. HRA carried out in the framework of PSA will generally be limited to human reliability in operation and maintenance. In addition to developing models for human interaction in operation, it is necessary to develop models for human interactions involving higher-level cognitive functions. The second generation HRA approaches study human action in the broader context taking the cognitive functions involved in operator response into consideration.

### 2.2.3 Categorisation of Human Interactions in PSA

Three categories of human interactions can be defined to facilitate the incorporation of HRA into the PSA structure. The three categories are as follows [11].

#### Category A : Pre-initiators

Pre-initiators consist of those human interactions associated with maintenance, testing and calibration, which on account of the errors made during their performance, can cause equipment/systems becoming unavailable, when required post-fault. System availability could be degraded because the human interactions may cause failure of a component/component group or may leave components in an inoperable state.

Especially important are errors that result in concurrent failure of multiple channels of safety related systems. This unavailability is added to other failure contributions for components or systems, at the fault tree level. In these human interactions, the time available for action is not a major constraint, i.e. time related stress is not a significant influence factor. Further, pre-initiator errors usually occur prior to an Initiating Event (IE) and can remain latent. Recovery action for such human errors could follow error alarm, post-maintenance testing or post-maintenance inspection with checks and may be modelled as applicable at the quantification stage.

#### Category B : Initiators

Initiators are those human interactions that contribute to IEs or plant transients. They are usually implicit in the selection of IEs and contribute to total IE frequency. Errors in these actions, either by themselves or in combination with other failures (other than human errors) can cause initiating events. Most important are errors that not only precipitate an accident sequence but which also concurrently cause failure of safety/safety related systems. Such 'common cause initiators' need to be specially emphasised in HRA.

#### Category C : Post-initiators

These are post-incident human interactions comprising the actions performed after an initiating event, with the intent to bring the plant to safe state. Errors in these interactions can exacerbate the fault sequence. These human interactions can be separated into three different types.

##### Type 1 : Procedural safety actions

These actions involve success/failure in following established procedures in response to an accident sequence and are incorporated explicitly into event trees. These include EOP responses and other manual reinforcement actions.

#### Type 2 : Aggravating actions/errors

These actions/errors occur post-fault following an initiating event and significantly exacerbate the accident progression. They are the most difficult to identify and model. One type of such an error occurs when the operator's mental image of the plant differs from actual plant state, causing the operator to perform the 'supposedly right' action for the event, which however has been 'wrongly interpreted'. Such an error also occurs when the operator correctly diagnoses an event but adopts a less than optimal strategy for dealing with it. Once the actions and their significant consequences are identified they can be incorporated explicitly into the event/fault tree.

#### Type 3 : Improvisations and recovery/repair actions

These consist of recovery actions, which are included in accident sequences that would otherwise dominate risk profiles. They may include the recovery of previously unavailable equipment or the use of non-standard procedures (improvisations) to mitigate accident conditions. These can be incorporated into the PSA as recovery actions in the accident sequence event trees.

Some diagnosis is required for Type 1, Type 2 and Type 3 actions and time is usually a limiting factor. The general approach for dealing with Type 1 and Type 3 actions is the same and the two can be treated as one single category. For convenience, Type 2 actions are also included in this category, although specific measures are usually outlined for dealing with them.

### 2.2.4 Conducting HRA - Steps in the HRA Process

The HRA process is shown in Figure 2.1 and is sourced from Kirwan [14]. The steps in the process are outlined below.

#### (a) Problem definition

The scope of the HRA is determined in the problem definition phase. Points to be considered include whether the HRA is PSA driven (i.e. scenarios to be analysed are determined by the PSA) or a stand-alone assessment, the tasks and errors to be examined, whether a quantified estimate is required, goals and criteria for risk assessment and the general vulnerability of the system to human error.

#### (b) Critical task identification

HRA is required to focus on tasks involved in maintenance, test and calibration operations, normal operation and emergency response. The tasks contributing significantly to overall plant risk are the critical tasks to be included in the HRA. The critical tasks are identified from the PSA preliminary system analysis wherein all major events/faults that affect system safety and integrity are compiled. As the PSA and HRA proceed, new human interactions may be identified and these, if significant, are added to the list of critical tasks for HRA.

#### (c) Task analysis

Human-System Interactions are described and analysed using task analysis methods. The roles of operators are defined in detail. The step-by-step interactions of the operator with the system, involving reading of displays, deciding on a course of action, operating controls and checking for response feedback, are delineated. A Task Analysis structures operator tasks and results in a more reliable HRA.

#### (d) Human error identification and analysis

Human error identification is a critical part of the HRA process. Important human errors are identified on the basis of their consequences on system performance. To guide the search, it will be useful to use an error taxonomy/classification, so that errors belonging to different categories may be identified.

HRAs may not model human errors explicitly but model human contribution to risk at the task level, as only task failure probabilities are needed to evaluate risk in a PSA. Potential errors can be identified by examining the relevant operating, maintenance and test procedures.

Seeking out extraneous errors (rule violations) is more difficult. The actions operators may come up with in complex scenarios (situations already disturbed by previous errors) are difficult to foresee. One way is to see how operators have behaved in similar situations in similar plants i.e. through operating experience feedback. Another way is by simulating the scenarios on a simulator.

It is necessary to gather all information, which will allow the estimation of the probability of each error. This qualitative analysis is not just a preliminary to quantification. It also allows the analyst to bring out which performance shaping factors contribute to the occurrence of errors.

(e) Human error representation

Once identified, errors need to be evaluated to ascertain the importance of each, and so that the combined probabilities of all failures and combinations of failures (hardware, software, human and environmental) can be summed to derive the total system risk. This is done, by representing the human errors, along with other failures, in fault trees and event trees. Analysis gives an indication of the degree of importance of each individual event to total risk.

In addition to the above, it is necessary to model and evaluate 'dependencies' between different tasks/human errors. Dependency is a relationship between two events in which one causally follows the other (e.g. failure to notice an alarm and another event, say the failure of the alarm). A case of direct dependence between two tasks can occur in response to a first alarm and response to a second alarm. If the same operator is involved in both actions then errors associated with the two events are unlikely to be independent.

Dependence on this level can be dealt with by using a dependence model. Kirwan [13] explains the use conditional probabilities, which involves adjusting the HEP in those situations where human intervention is possible at two or more points in the event sequence. For example, when checking is carried out by both operator and supervisor. HEP (of say 0.02) is applied for check by operator and conditional HEP (of say 0.01) is applied for check by supervisor, conditional on failure of check by operator, because supervisor may implicitly assume that operator has correctly performed his task, and also that responsibility for performance of the task rests with the operator.

Another example of dependence is the dependence between the different actions of an operator who is calibrating a set of gas detectors. If the operator made a random error in calibrating a single detector, then the error would not be expected to occur in other detectors. If, however, the operator mishears or misreads the common setting for the detectors, then every detector may be erroneously set as a result. It is important when representing error in this scenario, to take dependence into account for correct estimation of HEP for many detectors being wrongly set. It is important to look for common points between errors, such as actions using the same information, the same means of control or the same reasoning or diagnosis [13].

'Screening' is another area of concern in Representation. Screening can be used in large PSAs where a correspondingly large number of errors have been identified, and where, as a result, considerable resources have to be expended to quantify the probabilities of all the errors. Errors are 'screened' by assigning each error a highly pessimistic probability in the initial run of a PSA logic tree evaluation, in order to determine whether a detailed and more accurate quantification is appropriate on an error-by-error basis.

(f) Human error quantification

After representing the human error potential, the next step is to quantify the likelihood of errors

involved and determine the overall effect of human error on system safety or reliability. Human reliability quantification techniques quantify human errors in terms of Human Error Probabilities (HEPs). HEP, which is measured as the ratio of the number of errors that occurred to the number of opportunities for the error to occur, is the measure or metric of human reliability. Recorded HEPs are relatively few in number. Moreover, they are highly context dependent. The main reasons for the scarcity of recorded HEP data are as follows.

- Difficulty in estimating the opportunity for error in many tasks.
- General unwillingness and restraint in disclosing data that reveals poor human performance.
- Lack of realisation of the benefits of such data.

When HEP data are scarce, HRA resorts to quantification based on expert judgement or a combination of data and models that evaluate the effects of influences on human performance. The development of techniques of human reliability quantification has always been an area of significant activity. Important techniques are Technique for Human Error Rate Prediction (THERP), Accident Sequence Evaluation Programme (ASEP), Human Cognitive Reliability (HCR), Expert Judgement and newer techniques like Cognitive Reliability and Error Analysis Method (CREAM) and A Technique for Human Error Analysis (ATHEANA). These are presented in detail later in this document.

Uncertainty in data is to be addressed. A method commonly used is the error distribution approach, in which uncertainty is expressed as a continuous probability distribution surrounding the chosen point estimate. If a lognormal distribution is used, uncertainty is expressed as the error factor, which is the ratio of the ninetyfifth percentile value to the median value.

(g) Impact assessment

Once the errors have been quantified and represented in the risk assessment logic trees, the overall system risk can be evaluated. If the calculated risk is unacceptably high, then the risk must be reduced to acceptable value. Impact assessment involves determining not only whether the risk is acceptably low, but also which events (human, hardware, software or environmental, or combinations of these) contribute most to the calculated risk.

If the risk is found to be unacceptably high, then these events/combinations of events are subjected to in-depth investigation. If one or more human errors contribute significantly to risk, then these would be targeted for error reduction analysis.

(h) Error reduction analysis

If critical human errors are found from impact/sensitivity analysis, then Error Reduction Analysis is carried out to determine the error reduction approaches to be applied. The error reduction approaches generally taken include consequence reduction (by shielding the operator from radiation exposure or by automation), error pathway blocking (e.g. by designing interlocks), enhancement of error recovery (e.g. by introducing an additional level of supervision) and PSF based error reduction (e.g. by reducing the negative impact of PSFs on human performance).

The specific Error Reduction Measures (ERMs) required may be worked out in a number of ways; from the root causes of the error identified during the error identification and analysis stage, from the Performance Shaping Factors (PSFs) contributing to HEP, usually identified during the quantification stage, or from an assessment of the task in the work context using ergonomics guidelines/engineering judgement.

Common ERMs include provision of additional displays, imparting training to operators for 'self recovery' and introducing procedural checks and 'check off' sheets. If ERMs are devised, the quantification is done again to recalculate the HEPs for the system, as it would perform with

the ERMs implemented. In some cases several iterations through the impact assessment, error reduction and re-quantification stages may be required before risk goals and criteria are met.

(i) Quality assurance and documentation

Quality Assurance in HRA involves two main aspects. These are 1. Assurance that a quality HRA has been carried out and the objectives have been achieved within the scope of the project and without error and 2. Assurance that the ERMs are effectively implemented and the assumptions relating to improvements in human reliability made in analysis are still valid. Quality Assurance essentially means ensuring that performance is as required and documentation is proper.

The purpose of documentation is to provide at all stages of the HRA, a traceable account of the analysis and results, in order to facilitate any additional analysis (that may be required at a later date) and application of results, and also communicate a clear perception of the impact of the human element on plant safety. The documentation may best be organised as per the task steps in the HRA framework, clearly delineating the inputs, outputs and assumptions made. The results should address quantitative impacts on CDF and other risk measures, key sensitivities and the major findings and insights derived. The latter may include recommendations for improvements to procedures, training or HMI and the influence of human error on the relative ranking of dominant sequences.

All documents should be referenced and supporting information on task analyses, operator interviews and expert opinions should be documented as a basis for judgements made during the analysis. Although the HRA process is presented in terms of discrete tasks, it may be noted that it is usually iterative between the tasks.

## 2.3 Frameworks for Integration of HRA into PSA

### 2.3.1 General

Different frameworks are used for introducing and integrating HRA into PSA. A commonly used framework is Systematic Human Action Reliability Procedure (SHARP) developed by Electric Power Research Institute, U.S.A [7]. Other frameworks are “A Guide for General Principles of Human Action Reliability Analysis for Nuclear Power Generation Studies”, known as the IEEE Standard P1082/D7 and the U.S. NRC sponsored “Task Analysis Linked Evaluation Technique (TALENT)” for implementing human factors expertise into PRA [5].

The International Atomic Energy Agency (IAEA) has established guidelines to facilitate the use of PSA. To support these PSA Guidelines, a number of other documents have been written to provide detailed guidance in specific areas. One such technical document (IAEA, 1995) gives a procedure for conducting Human Reliability Analysis (HRA) in PSA [11]. Two commonly used frameworks, EPRI SHARP and the IAEA procedure are discussed in the following sections.

### 2.3.2 Systematic Human Action Reliability Procedure (SHARP)

The SHARP framework systematically incorporates human-system interactions into PSAs by distinguishing five types of human interactions with the system [15].

#### 2.3.2.1 Types of Human Interactions in SHARP

The types of human interactions according to SHARP are as follows:

Type 1: Prior to an initiating event, plant personnel can affect safety and availability by inadvertently disabling equipment during testing or maintenance. They could also improve the availability of systems by restoring failed equipment through corrective maintenance and testing.

Type 2: By committing some error, plant personnel can initiate an accident.

Type 3: By following procedures during the course of an event, plant personnel can operate standby equipment and terminate or mitigate an event.

Type 4: Plant personnel, while attempting to follow procedures during the course of an event, can make a mistake that aggravates the situation or fails to terminate the event.

Type 5: By improvising, plant personnel can restore and operate initially unavailable equipment to terminate an event.

The SHARP categorisation is basically identical to the categorisation given in section 2.2.3 with Type 1 corresponding to Category A, Type 2 to Category B and Type 3, Type 4 and Type 5 together corresponding to Category C.

### 2.3.2.2 Seven Steps of SHARP

In his detailed review of HRA performed for GRS, Germany, Swain presents the following seven steps from SHARP. Each step has defined objectives, inputs and outputs, activities and rules. The links between the steps and key decision points are shown in Figure 2.2. The goals for each step are as given below.

- (1) Definition: To ensure that all types of human interactions are adequately considered in the study.
- (2) Screening: To identify the human interactions that are significant to operation and safety of the plant.
- (3) Breakdown: To develop a detailed description of key human interactions in the form of tasks and subtasks. Include any performance write-ups from other plants as well as plant specific write-ups, if any.
- (4) Representation: To select and apply techniques for modelling important human interactions in logic structures. Such methods help to identify additional significant human actions that might impact the system logic trees.
- (5) Impact assessment: To assess the impact of significant human actions on the system logic trees.
- (6) Quantification: To apply appropriate data and/or quantification methods to assign error probabilities for the various interactions examined, determine sensitivities and establish uncertainty bounds.
- (7) Documentation: To include all necessary information for the assessment to be traceable, understandable and reproducible.

The activities to be carried out in the seven steps are delineated below:

#### Step 1: Definition

The basic logic trees developed by system analysts from the functional descriptions of the plant are enhanced to clearly and fully describe human interactions. This is to ensure that that all the different human interactions are adequately considered in the study.

Important are human actions for operations, including maintenance and testing, human initiators, isolation and mitigation actions, actions that might exacerbate a situation and potential improvisations to existing procedures. Various source documents (including those covering emergency, maintenance and test procedures) may be referenced.

#### Step 2: Screening

The logic trees, enhanced with human interactions, are screened to rank and select human interactions that are key to safe operation (i.e. those actions which if improperly performed lead to increase in CDF). Screening can be based on the following:

- judgement (e.g. location in the logic tree)
- coarse screening (e.g. by evaluation of the human impact in minimal cutsets)
- fine screening (e.g. by quantifying human interactions based on the type of behaviour – skill, rule and knowledge).

#### Step 3 : Breakdown

Each key interaction is subdivided into tasks and subtasks associated with specific equipment procedures, to enable a more detailed consideration of factors which affect performance. Tasks and subtasks are enhanced by descriptions of significant cues (alarms and signals), behaviour type, time allowed for task, motor actions required, controls to be operated, response feedbacks, and other influence factors like stress and ergonomics of the human-machine interface. These descriptions serve as a basis for selection of a model or representation for the human interaction.

#### Step 4 : Representation

The key human interactions are explicitly modelled to include all possible alternatives and a representation is selected (for example, the HRA Event Tree or Operator Action Tree-OAT), taking into account the availability of data and/or expert opinion to support the selected representation. For the selected representation, a specific description is generated covering alternate choices or mistakes possible in the human interactions.

#### Step 5 : Impact assessment

This step is essentially one of recapitulation and review to allow the analyst to incorporate the insights gained from the breakdown and representation stages. The possibilities for initiating events, recovery actions and common cause failures and also the impact on quantification are reviewed. Also reviewed are the possible sequence initiating events, e.g. the initiating event for an event sequence could be ‘operating the pushbutton’ or ‘taking the wrong channel out for maintenance’. The step also includes a review of whether actions can be combined for the purpose of analysis. Such tasks are to be judiciously combined.

#### Step 6 : Quantification

The probability of success or failure of key human interactions is quantified for incorporation into the PSA study accident sequence quantification. This includes the evaluation of sensitivities and uncertainties associated with the data. The most appropriate database is to be selected and might include time reliability curves, published data, data obtained from experiments and human reliability models and opinions of experts. SHARP suggests a number of techniques and is somewhat specific. However, procedurally the use of any particular technique is not precluded.

#### Step 7 : Documentation

All documentation relating to the PSA must be traceable. The documentation must accurately describe the process used to develop the quantification including assumptions made in respect of data and actions in event trees, models and quantification techniques as well as the rationale for action times or dependencies assumed. Any modification made to an existing method is to be clearly stated and a quantitative statement as to the impact of human actions on CDF is to be given. Quantitative evidence is to be included as proof for actions concluded to be risk dominant for a particular sequence. Procedures for preparation of the documentation are available in the U.S. NRC Procedures Guide, NUREG/CR-2300 [28].

#### 2.3.2.3 Benchmark and Evaluation Studies on SHARP [5]

A benchmark study, the hypothetical loss of main feedwater induced Anticipated Transient Without Scram (ATWS), was conducted and documented by EPRI in 1987 to determine the consistency of a number of analysts in using SHARP. Analysts were positive in their evaluation of SHARP.



Swain reviewed SHARP with a set of evaluation criteria for human reliability in the form of a checklist [Comparative Evaluation of Methods for Human Reliability Analysis, GRS-71, April 1989]. The checklist is an evaluation of HRA methods. SHARP received a favourable review for usability. According to Swain, it provides a quantitative output meaningful to PRA and ensures that qualitative information is catalogued. No benchmark application has proven SHARP difficult to apply or yielded inconsistent findings.

### 2.3.3 IAEA's Procedure for Conducting Human Reliability Analysis in PSA [15]

The IAEA procedure aims to provide a practical and nearly standardised approach and terminology for PSA and describe a framework in which different types of human actions are related to specific parts of PSA. Acceptable methods and data sources for analysing human actions are discussed and the integration of HRA into PSA is detailed. In the IAEA Procedure, human interactions are grouped into three categories (A, B and C), as described in Section 2.2.3.

There are six main components in an HRA study, which comprises a qualitative assessment phase and a quantitative assessment phase. The components are:

- (i) Task definition/understanding
- (ii) Task analysis
- (iii) Identification of errors
- (iv) Error recovery potential and mechanisms
- (v) Identification of additional constraints
- (vi) Quantification

The process of incorporating the HRA into PSA can be separated into seven basic tasks. Each task has inputs, activities and outputs. The tasks required for each of the three categories of human interactions have the same form. The seven tasks are as follows:

- (1) Definition: To ensure that all candidate human interactions of the three categories are adequately considered in the study
- (2) Screening: To identify human interactions that are significant to operation and safety of the plant, with a view to minimising the resources required.
- (3) Qualitative analysis: To develop a detailed stepwise description of important human interactions, identifying key influence factors necessary for completing the modelling.
- (4) Representation: To select and apply techniques for depicting human interactions in logic structures.
- (5) Model integration: To describe how the significant human actions are integrated into the plant and the system models of PSA.
- (6) Quantification: To apply appropriate data or quantification methods to assign probabilities for various interactions examined, determine sensitivities and establish uncertainty ranges.
- (7) Documentation: To include all necessary information for the assessment to be traceable, understandable and reproducible.

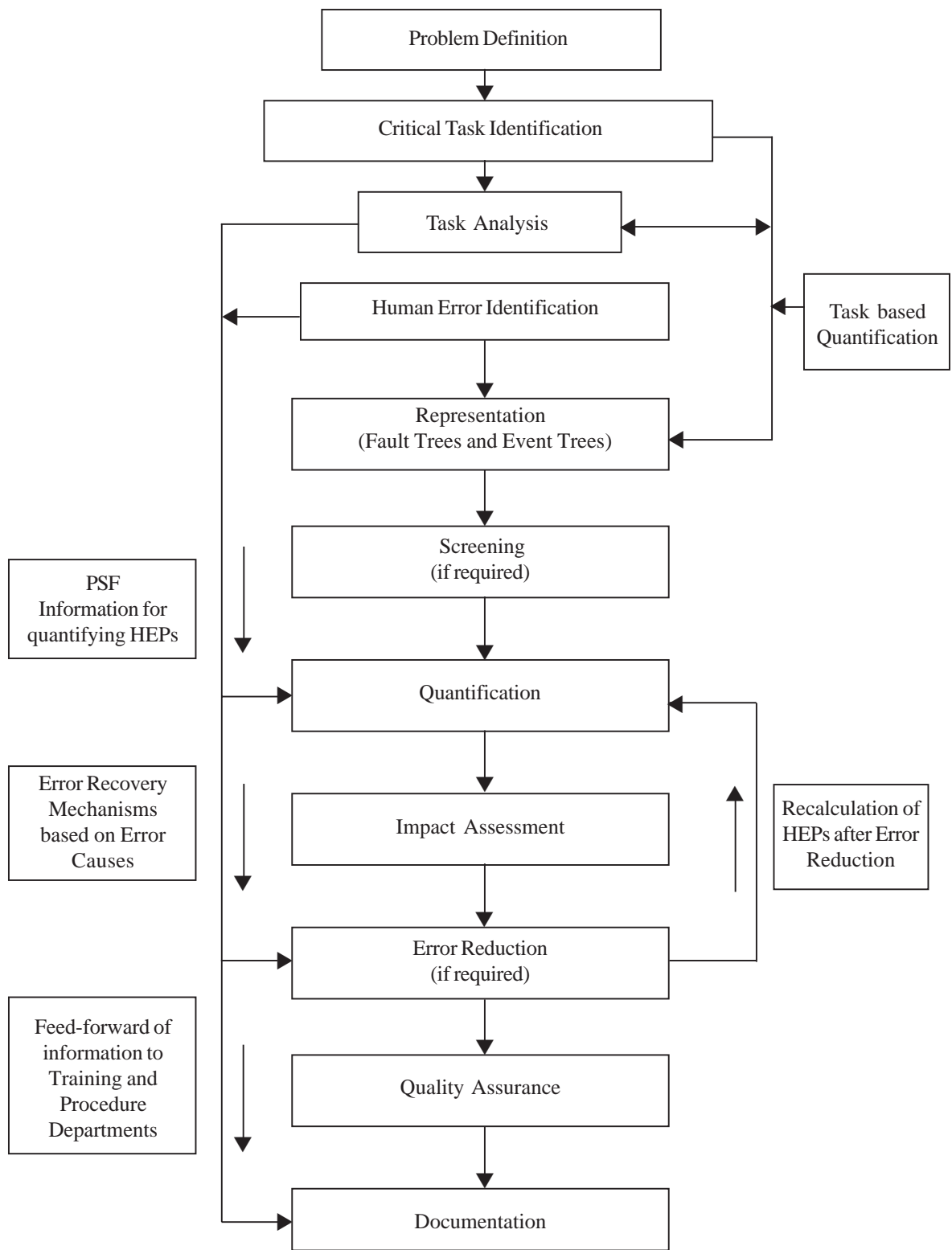
### 2.3.4 Comparison of SHARP and IAEA Frameworks

Both SHARP and IAEA Procedure provide an organised framework for the steps in the HRA process. While SHARP distinguishes 5 types of human interactions, the IAEA Procedure defines 3 categories of human interactions, with Category C essentially covering Type 3, Type 4 and Type 5 of SHARP. The

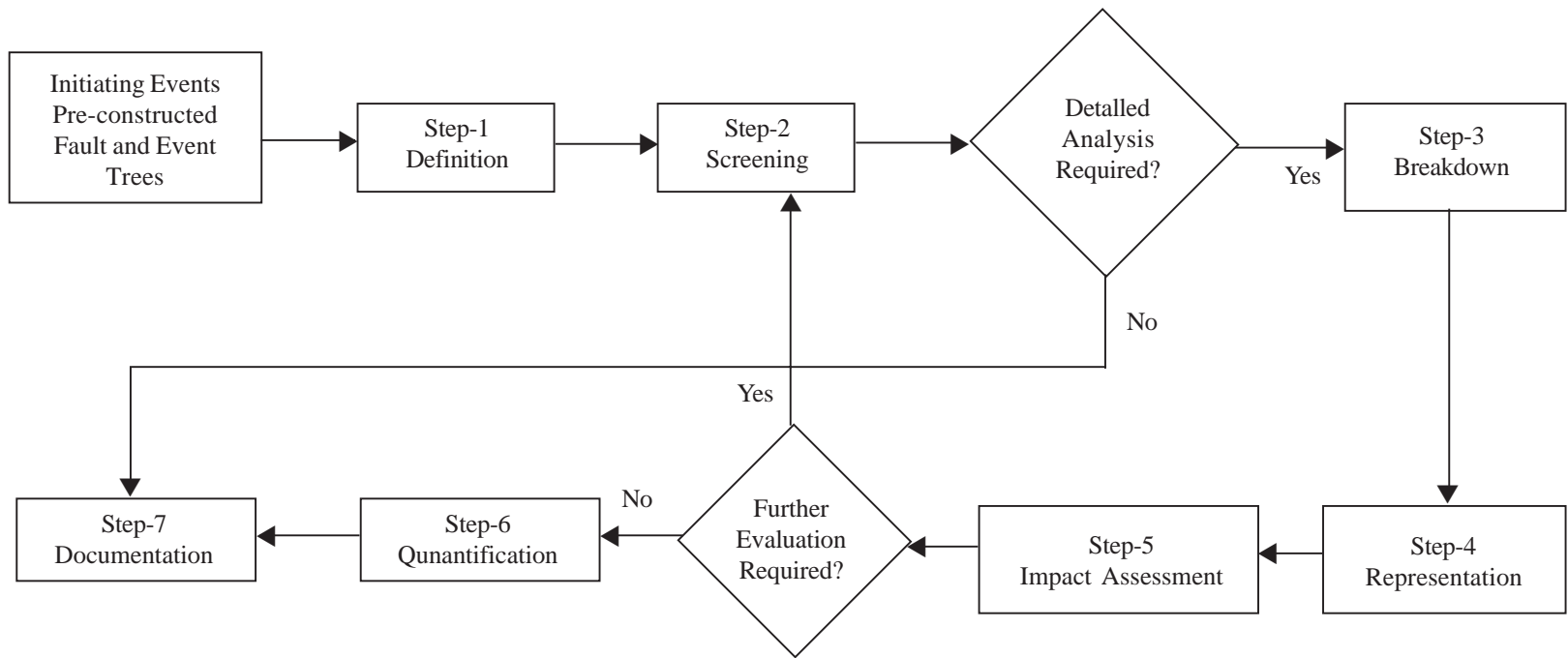
seven steps of SHARP are similar to the seven basic tasks of the IAEA procedure. One notable difference between the two is the absence of an explicit step for impact assessment in the IAEA procedure. The impact assessment is presumably to be carried out as part of the quantification task.

### 2.3.5 Points to Consider in Integration of HRA into PSA

The extent and attributes of the HRA will depend ultimately on the objectives of the PSA. The effective integration of HRA into the PSA requires knowledge of both HRA and PSA. A human reliability analyst with an understanding of basic PSA methods and NPP operations can coordinate the integration. Close interaction with plant personnel is necessary to ensure that both the PSA model and the HRA evaluations within it reflect actual plant operations and practices. If the PSA is being performed at the design stage, then the human reliability analyst needs to consult knowledgeable personnel from other operating stations to ensure that the assumptions made in respect of operating practices, procedures and training are reasonable.



**FIGURE 2.1 : THE HRA PROCESS [14]**



**FIGURE 2.2 : SHARP FRAMEWORK**

### 3. METHODS AND MODELS FOR QUANTIFICATION OF HUMAN RELIABILITY

#### 3.1 Introduction

Some of the methods and models used in HRA are given in Table 3.1 below.

**TABLE 3.1 : HRA METHODS**

1. ANALYTICAL METHODS 1.1 Time dependent activities (a) Pre-accident (Normal) activities: THERP, HCR. (b) Post-accident activities: THERP, OATS, HCR, CM. 1.2 Time independent activities (a) Pre-accident activities <ul style="list-style-type: none"> <li>• Component specific errors. These are usually included in equipment failure rates, e.g. human errors in repairing a pump.</li> <li>• Configuration errors, e.g. restoration errors. These are usually incorporated into fault trees.</li> </ul> (b) Post-accident activities : THERP
2. EXPERT ELICITATION/JUDGEMENT METHODS 2.1 Direct numerical estimation (absolute probability judgement) 2.2 SLIM-MAUD 2.3 STAHR (influence diagram approach)
3. FAST SIMULATION MODELS 3.1 MAPPS 3.2 SAINT
4. OTHER METHODS 4.1 Sandia recovery model (SRM) 4.2 Operator reliability calculation and assessment (ORCA)

Key to abbreviations :

- THERP       - Technique for human error rate prediction
- HCR         - Human cognitive reliability
- OATS        - Operator action tree sequence
- CM          - Confusion matrix
- SLIM-MAUD - Success likelihood index method-multi-attribute utility decomposition
- STAHR      - Socio-technical assessment of human reliability
- MAPPS      - Maintenance personnel performance simulation
- SAINT      - Systems analysis of integrated networks of tasks

The following sections present in detail the methods most useful for HRA in PSAs of Nuclear Power Plants.

## 3.2 Technique for Human Error Rate Prediction (THERP)

### 3.2.1 Overview of THERP

THERP was developed for the US Nuclear Regulatory Commission [25] and is an in-depth and widely used method for modelling and quantifying human reliability. Of the many methods available, it is the only complete method because it provides mechanisms for both modelling and quantifying. THERP is the source of the HRA event tree, the basic tool used to model tasks and task sequences in HRA. The method is based on performing a task analysis that describes the tasks to be performed by the operations or maintenance crew.

While describing the individual tasks, information on the different PSFs is collected to modify the error probabilities. The procedural steps in the tasks are graphically described in the form of HRA event trees. THERP allows for the modelling of task dependence and also recovery from less-than-adequate performance.

Event trees are quantified by the use of lookup tables which contain probability estimates. Factors such as dependence, stress, experience, training, procedure quality and the adequacy of human-machine interfaces are used to modify the base HEPs. The resulting probabilities are then placed on the HRA event trees and summed to provide values for input to PSA.

### 3.2.2 The THERP Approach - Qualitative Analysis

Human reliability analysts applying THERP should make use of the qualitative and quantitative approach given in NUREG/CR-1278. The approach comprises the following steps.

- (i) Perform a task analysis and identify all significant interactions involving personnel. This includes the consideration of the interfaces between personnel and procedures, personnel and hardware, personnel to personnel communications and decision making.
- (ii) Analyse the interfaces and determine if the PSFs are adequate and favourable/unfavourable to the performance of required tasks.
- (iii) Identify potential problem areas, with respect to procedures, equipment design, lighting, ventilation, plant policies and practices and the motor skills and mental effort that are required of personnel, which may lead to human error.
- (iv) Determine which problems have potential impact and which necessitate changes in equipment or extant practices.
- (v) Develop solutions to the problems. Human factor problems are resolved through job redesign, use of mechanical interlocks, administrative controls and implementation of training and certification requirements.
- (vi) Review the consequences of the changes with respect to availability, reliability and costs (through costs-benefits analysis). Consider the degree of hazard to personnel, risk of damage to equipment, implementation schedules, the ability of the modified system to operate under the range of environmental constraints normally encountered and the ability to maintain the system in the new configuration in a tradeoff study.

### 3.2.3 Task Descriptions in THERP

Tasks in THERP are classified as either dynamic or step-by-step. Dynamic tasks refer to instances where interpretation and diagnosis of a situation is required. The diagnosis of an infrequently occurring event without the aid of procedures would be a dynamic task. A regular task, which is considered as a sequence of actions, such as the planned shutdown of a NPP unit is a step-by-step task.

### 3.2.4 Error Likely Situations

Error likely situations can be determined through structured interviews with plant personnel, together with evaluation of the systems against available guidelines and standards. Errors in general can arise in

any situation where the abilities required for task performance do not match those of the personnel concerned. Error likely situations exist when the distinctive cues to be used by the operators to assess a situation are not apparent. Similarly, the lack of clear unambiguous feedback to operators most often indicates a potential error likely situation. The lack of cues or lack of feedback, are best determined by plant walkthroughs.

### 3.2.5 Dependence

When THERP is used to estimate the frequency of human error (or HEP), the degree of interaction or dependence that is present is to be decided upon. This is done, by first decomposing the tasks into smaller elements for which there are reference HEP data and then evaluating the dependence between tasks for these elements. The failure rates for the smaller units are adjusted for the degree (zero, low, moderate, high, complete) of task dependence present. Highly dependent tasks would have somewhat higher failure rates. The HEPs for the smaller units are finally combined using the denoted set of rules in THERP and an overall HEP is determined. THERP further allows the failure rates to be modified for operator/crew stress levels.

Dependence can also occur between persons as when several technicians perform a task together or when a second person checks the actions performed by the first, in the form of an inspection. Dependence can also occur within an individual as several tasks are performed.

### 3.2.6 Recovery

When an error likely event is discovered, recovery by operator/crew is modelled and quantified. Quantification of non-recovery gives a joint probability (i.e. the probability that an error will occur and will not be recovered).

### 3.2.7 Integrating Human Failure Rate Information into PSA

The steps to be followed by the analysts using THERP to integrate failure rate information into PSA are as follows.

- (i) In conjunction with the system analyst and the PSA analyst, define the system failures of interest, including system functions that can be influenced by human error.
- (ii) Perform the task analysis necessary to list and adequately analyse the human operations.
- (iii) Estimate the relevant error probabilities.
- (iv) Estimate the influence of human error on system failure events.
- (v) Recommend changes to the system and recalculate the system failure probabilities. Both sensitivity analysis and uncertainty analysis are to be performed.

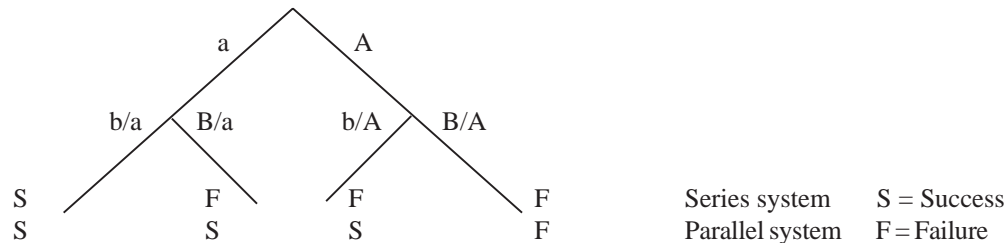
To complete the above five steps, the analyst goes through four phases, which are delineated below.

- (i) Familiarisation phase: Information gathering and plant visit, understanding plant specific and event specific data and databases, review of administrative and operating procedures and drawings.
- (ii) Qualitative assessment phase: Determining performance requirements, evaluating the performance situation, modelling human performance and determining potential errors.
- (iii) Quantitative assessment phase: Determining probabilities of human errors, quantifying the influence of the effects of performance shaping factors on human failure rates, accounting for probabilities of recovery from errors and calculating the human error contribution to probability of system failure.
- (iv) Incorporation or integration phase: Incorporation of human factors and HRA findings in the estimation of risk (e.g. CDF), performing sensitivity and uncertainty analysis.

### 3.2.8 The HRA Event Tree Model in THERP

The HRA event tree, which is a formal representation of the sequence of actions, is unique to THERP. The tree starts at any convenient point in an activity sequence and works forward in time. Decision processes are modelled in binary success or failure fashion, with the sum of their probabilities always equal to 1. All human activities depicted by the tree have a conditional probability, except for those in the first branching.

HRA event tree



Task 'A' The first task

Task 'B' The second task

- a = Probability of successful performance of Task 'A'
- A = Probability of unsuccessful performance of Task 'A'
- b/a = Probability of successful performance of task 'B', given a.
- B/a = Probability of unsuccessful performance of task 'B', given a.
- b/A = Probability of successful performance of task 'B', given A
- B/A = Probability of unsuccessful performance of task 'B', given A

For series system

$$\Pr [S] = a(b/a)$$

$$\Pr [F] = 1 - a(b/a) = a(B/a) + A(b/A) + A(B/A)$$

For parallel system

$$\Pr [S] = 1 - A(B/A) = a(b/a) + a(B/a) + A(b/A)$$

$$\Pr [F] = A(B/A)$$

If the first branching represents a carry-over from some other tree, or a task based on likelihood of a previous event, it too will be a conditional probability. In the event tree shown above, because Task 'A' is always performed first, the probabilities associated with Task 'B' are all conditional on the outcome of 'A'. b/a, B/a, b/A, and B/A represent the interdependence of the tasks A and B.

A series system has total success only if both Task 'A' and Task 'B' are successful. A parallel system succeeds if either task is successful and fails only when both fail. The sum of individual path Pr[S] gives the total success probability. Because Pr[S] = 1 - Pr[F] and vice versa, only success or failure probability need be calculated for the system.

### 3.2.9 THERP Data and Types of HEPs

THERP is based on a database of HEPs summarised in chapter 20 of the THERP Handbook [25]. These data were derived from objective field judgements by the authors of the technique. The Handbook also contains human performance models explaining how to modify the data for changes in performance shaping factors and guidelines on how to convert independent failure probabilities into conditional failure probabilities.



Although modelling of tasks with event trees and using conventional reliability mathematics to derive task success probabilities are straightforward tasks, the assignment of HEPs to individual task element failure branches of the event trees calls for considerable judgement on the part of the analyst. Data acquired from the specific plant situation under analysis would give the best estimate of error for the task. As such human error data are not often available; sources like the Handbook have to be used.

The applicable HEP data found in THERP are referred to as Nominal HEPs. These represent the probability of human error without considering the influence of plant specific and task specific PSFs. Once these are taken into account a basic HEP is obtained. The basic HEP (BHEP) is the HEP with PSFs considered, without considering the influence of other tasks, i.e. the task is considered in isolation. A conditional HEP (CHEP) is a modification of the basic HEP to account for the influences of other tasks or events that may include the preceding task elements/tasks and the number of personnel performing the task.

### 3.2.10 The THERP Dependence Model

THERP distinguishes five levels of dependence, equations for the conditional HEP of failure, given failure of the previous task and  $P_o$  as its independent HEP value, are given in the Table 3.2 below.

**TABLE 3.2 : LEVELS OF DEPENDENCE**

Dependence Level	HEP
Zero	$P_o$
Low	$(1 + 19P_o) / 20$
Moderate	$(1 + 6P_o) / 7$
High	$(1 + P_o) / 2$
Complete	1

### 3.2.11 Data Tables in THERP Handbook

There are 27 data tables in THERP handbook (Appendix-5), and all of them are referred to in the stepwise procedure for determining HEP values, presented in Section 3.2.12. The database considers only the most frequently observed tasks in a NPP. Therefore, when a task is being evaluated for which there are no tabled HEPs, a value of 0.003 is assigned as the nominal HEP for a general error of omission or commission, if it is judged that there is some probability of either type of error. In abnormal events, those tasks for which the tables indicate the HEP to be 'negligible', are assigned a nominal HEP of 0.001 to allow for the effects of stress that is associated with abnormal events. Most of the tables list the error factors (EFs) or the uncertainty bounds (UCBs) for the HEPs. For cases in which the EFs or UCBs are not listed, guidelines for estimating them are given in Table 20.

### 3.2.12 Determining HEP Values in THERP

The stepwise procedure for determining an appropriate HEP value from the tables in chapter 20 of the Handbook (NUREG/CR-1278), given in Appendix-5, is as follows:

- (a) If, to begin with, it is required to carry out a screening analysis (involving the assignment of very high failure probabilities), then follow directions given for selecting screening values for the performance of diagnosis and for subsequent rule based actions using the Tables 1 and 2.
- (b) If screening analysis is not required, then check whether nominal diagnosis is required. In most PSAs, nominal HEPs for diagnosis are of interest. The HEPs for the nominal diagnosis model (Table 3) are used to estimate the probability of control room personnel failing to diagnose one

or more abnormal events within the time constraints given by system analysts. To consider the effects of personnel interaction in modifying the nominal HEPs for post-event activities (e.g. rule based actions), one uses the table listing control room staffing assumptions (Table 4) as a function of time.

- (c) Following the above, if rule based actions are required to be carried out, then first determine whether errors of omission, or errors of commission, or both, are involved. A set of ten tables (Tables 5-14) lists the HEPs for errors in rule based tasks.
- (d) If errors of omission are involved, then determine whether the use of written material is mandated for the task. Written material includes formal procedures, ad hoc procedures and oral instructions that are written down by the recipient as he receives them. If yes, then the three tables (Tables 5,6,7) giving HEPs for errors (including commission errors) in preparation of written material, for errors in the initiation of a task and use of procedures (administrative controls) and for omission of items in procedures when using written material, are to be used.
- (e) If no written material is involved and the operator is relying on memory, then the appropriate HEPs are selected from Table 6 giving HEPs for errors in initiation of task and the Table 8 giving HEPs for errors in carrying out oral instructions as a function of the number of items to be remembered.
- (f) If errors of commission are involved, first determine whether the interface used is logically categorized as a display, a control, a switch for motor operated valve (MOV) or a switch for locally operated valve and then select the appropriate HEPs. If displays are used, then chose HEPs from the tables for errors in selection of displays (Table 9), the table for errors in reading and recording quantitative information from displays (Table 10) and errors arising due to the poor ergonomics of displays (Table 11). If a control or a switch for a MOV is used, then Table 12 giving HEPs for errors made in the selection and use of switches and other manual controls is referred to. If a locally operated valve is operated, then refer to the table giving HEPs for errors in selection of locally operated valve (Table 13) and/or the table giving HEPs for errors in recognizing that a valve is not fully open or closed because it is stuck (Table 14).
- (g) After selecting the nominal failure rate for the omission or commission error, the analyst must review PSF information to establish a BHEP. The PSF should be evaluated according to the tables given for taking into account tagging, stress and experience and dependence types (Tables 15-19).
- (h) At this stage, the analyst performs a preliminary quantification to get the total failure probability. Also, if there are human error terms that have no significant impact on system failure events, they may be dropped from further consideration.
- (i) Determine the uncertainty bounds (cubs) or error factors (eves) for estimated HEPs using the guidelines given in Table 20. Cubs for conditional HEPs based on the dependence model are given in Table 21. The total failure probability plus cubs constitutes the system analyst's input to overall PSA.
- (j) At this stage in the HRA, recovery factors will be considered. Recovery from deviations in actions under normal operating conditions may depend on the checking of actions performed by an individual; by another individual, the checker. HEPs for errors of omission and commission in the checker's task are given in Table 22. Recovery may also be based on inspections of plant indications by walkthroughs. Recovery cues may be annunciated. Table 23 lists HEPs for errors in initiation of corrective action in response to one or more enunciators and Table 24 lists HEPs for errors in remembering to respond to an enunciator that is steady on, after an interruption or in noticing an important 'steady on' enunciator during the initial audit, or during subsequent hourly scans.

In the absence of recovery cues, plant practice may mandate special status check of individual

equipment. If not, checking is more of a general inspection. In respect of these, Table 6 lists HEPs relating to initiation of a scheduled checking or inspection function, Table 25 lists HEPs for detection of deviant annunciated indications on different types of displays during the initial audit and on subsequent hourly scans, Table 26 gives modified HEPs for more than one display (a maximum of 5) showing the presence of deviant conditions and Table 27 lists HEPs for failure of the basic walk-around inspection to detect annunciated deviant indications of equipment within 30 days.

- (k) Appropriate modifications of the recovery factors by PSFs are next considered. This is followed by sensitivity analysis, which though may be done at other stages in the HRA. The sensitivity analysis is a means of ascertaining, whether the different assumptions and estimates made significantly affect PSA results. Any of the assumptions or HEPs may be modified after the sensitivity analysis and the effects of changes assessed to confirm that probabilistic safety goals/criteria are met.

### **3.3 Accident Sequence Evaluation Programme (ASEP)**

#### **3.3.1 Introduction**

The accident sequence evaluation programme (ASEP) HRA procedure detailed in NUREG/CR - 4772 [26] is the latest update of THERP. The intent of the ASEP HRA procedure was to enable systems analysts to make estimates of HEPs and human performance characteristics (sufficiently accurate for PSA), with minimal support from experts in HRA. The report includes some consideration of decision-based errors, clarification of task and operator dependence and guidance in respect of post-accident HEPs. It also provides guidance for memorized immediate emergency actions and a means of carrying out HRA with less effort. The results obtained with ASEP are in many cases more conservative than those obtained when applying THERP.

The ASEP document (Swain, 1987) is particularly valuable for providing guidance for post-accident HRA not found in the THERP document. It enables the analyst to assess the effect of emergency operating procedures (epos) and of memorised immediate emergency actions. As with THERP, the assumptions with regard to crew response are based on the time reliability curve/correlation (TRC) approach. The TRC is a relationship of the probability of the (failure of) occurrence of an event to the time over which the event could occur.

The basic approach taken in the development of the ASEP HRA procedure was to select certain generic HEPs for certain sets of tasks and employ easy-to-understand procedures for using these HEPs and for estimating the effects of dependence and recovery factors. The aim was to have a rule based procedure that could be employed with considerably less judgement than is the case with the more complete THERP HRA procedure.

The ASEP procedure consists of a pre-accident screening HRA, a pre-accident nominal HRA, a post-accident screening HRA and a post-accident nominal HRA. The screening analysis uses conservative estimates of HEPs, response time, dependence levels and other human performance characteristics. It is less complicated than nominal analysis and does not produce upper confidence bounds, as the analysis itself is sufficiently conservative.

#### **3.3.2 Pre-accident and Post-accident Tasks**

Pre-accident tasks of interest consist of maintenance (routine and corrective), calibration, surveillance, testing and restoration tasks. The opening or closing of manual or motor operated valves following repair or test, in order to restore these valves to their normal operating position/status, is an example of a restoration task.

Pre-accident tasks are tasks usually performed by operations personnel, instrumentation and control personnel and maintenance personnel, under non-accident conditions. Pre-accident tasks, if incorrectly performed, can affect the availability of safety systems that are required to mitigate an accident sequence.

To evaluate pre-accident tasks for an existing plant design, the calibration, test and maintenance procedures are reviewed for each front-line and support system. This review identifies critical instrumentation for which miscalibration could prevent system function, and components that could be removed from service and inadvertently left in an inoperable or incorrect state in maintenance or testing.

Pre-accident tasks may include elements of skill-based, rule-based or knowledge-based behaviour. However, normally only rule-based behaviour is modelled for PSA purposes, while assessing pre-accident tasks.

Post-accident tasks pertain to activities that are performed by control room operating crew and take place after the onset and annunciation of an initiating event. Post-accident tasks are divided into diagnosis (meaning perception, discrimination, interpretation, diagnosis and decision making) and post-diagnosis (execution) tasks, which are required in the implementation of mitigation measures for ensuring or maintaining the reactor in a safe state.

Post-accident operator actions are required in the following cases:

- failure of automatic actuation of the mitigating systems.
- successful automatic actuation of a mitigating system, with a requirement for operator actions to ensure its continued operation.
- the absence of design features for automatic mitigating action.

Diagnosis is the identification and evaluation of an abnormal event to the level that enables the operators to pin-point those systems or components whose status can be changed to mitigate or terminate the problem situation. Diagnosis therefore implies the determination of appropriate actions on recognising an abnormal event, within the allowable time constraints. Diagnosis includes interpretation and when necessary, decision making. Diagnosis also involves knowledge-based behaviour, i.e. behaviour that is applied in unfamiliar situations in which personnel have to interpret, diagnose or accomplish some level of decision making.

Post-diagnosis actions are activities that are indicated by, and logically follow a correct diagnosis of the abnormal event. These actions involve skill-based, rule-based and/or knowledge-based behaviour, and must be performed correctly within allowable time constraints.

### 3.3.3 Pre-accident HRA Methodology in ASEP

#### 3.3.3.1 Modelling of Pre-accident Tasks.

Pre-accident human errors are modelled at lower levels in the individual fault trees, usually at the basic event level. Typically a human error is modelled alongside its corresponding hardware failure. Both error types input to an 'OR' logic gate as contributors to the specified undesirable state of the component. Each human error basic event so modeled in the fault tree is labelled so that operator errors can easily be identified in cutset analysis and sorted for separate event reporting.

#### 3.3.3.2 Steps in Analysis

- (i) Obtain information for pre-accident HRA.

This is accomplished by carrying out the following steps.

- (a) Visit plant to gather information on maintenance, calibration, surveillance tests and restoration tasks. Review plant policies and practices. Discuss with plant personnel.
- (b) Observe plant personnel carrying out pre-accident tasks (calibration, maintenance and testing). Ask plant personnel to talkthrough the pre-accident procedures, as they are being carried out.

(c) Collect relevant written procedures and documents, including administrative procedures, system descriptions, layout drawings and technical specifications.

(ii) Identify the critical human-machine interfaces (HMIs).

All the relevant HMIs are evaluated to ensure that no potential failures due to human error are overlooked.

(iii) Define the critical systems and associated tasks and activities.

Document under: System name, Task (what is being done/not done by the human) and Activities (specific actions that are required to be performed to complete the task and restore the system to the required configuration).

(iv) Assign basic human error probability (BHEP).

The ASEP HRA procedure presents a simple model of human behaviour for pre-accident tasks. The model includes a generic BHEP that can be used for all pre-accident tasks, as well as rules to adjust this BHEP for the effects of dependence and recovery factors. The BHEP is conservatively selected as 0.03. Based on HRAs and reviews of pre-accident procedures at La Salle NPP, USA, it is taken as the HEP value for pre-accident actions, exclusive of recovery factors.

Therefore, for each key action that must be accomplished, e.g. the restoration of a valve to its normal operating position after maintenance or the performance of a critical step in a calibration procedure, a total BHEP of 0.03 is used. This value is based on the assumption of average quality written instructions and restoration procedures and associated administrative control.

The BHEP of 0.03 represents a combination of a generic HEP of 0.02 assessed for an error of omission and a generic HEP of 0.01 assessed for an error of commission, with the conservative assumption that an error of commission is always possible if an error of omission does not occur. The values 0.03, 0.02 and 0.01 are larger than many of the BHEPs related to pre-accident tasks, as given in NUREG/CR - 1278 [25].

Performance shaping factors (PSFs) other than recovery factors, dependence effects and radiation are implicitly included in the BHEP and assume average or better human factors or conditions. The effects of PSFs are also implicitly taken into account in the uncertainty bounds for the various HEPs. If considered necessary, the BHEP of 0.03 may be re-assessed upward (made larger) on the basis of a more detailed analysis of administrative procedures and their method of implementation. However, no downward adjustment of the BHEP of 0.03 should be made.

Radiation is explicitly considered as a PSF in pre-accident screening HRA. In AECL HRA [6] for CANDU reactors when a human action takes place in a radiation area, the probability of human failure is doubled; i.e. the basic HEPs are doubled.

(v) Identify recovery factors (RFs) and assess their effects

Recovery factor (RF) is a factor that prevents or limits the undesirable consequences of a human error. One of the most common RFs is human redundancy. Other RFs are applicable to the effects on human performance of control room component status displays (especially those that are annunciator), of post-maintenance or post-calibration tests and of periodic inspections (particularly those involving the use of written checklists). These RFs it may be noted are not part of post-accident recovery analysis discussed in Section 3.3.4.7.

In ASEP HRA procedure for pre-accident tasks, no RF credit is given for the use of written checklists, unless users of these checklists have been instructed to checkoff the equipment items one by one, once the prescribed check is completed. In HRA therefore, RFs will be

credited for written checklists, on the assumption that these checklists are available and are required to be checked off.

A conservative approach is taken, with a limited number of RFs being considered in the methodology. First, each RF is applied to the BHEP value (0.03) rather than being applied separately for errors of omission and errors of commission. Second, if there is more than one component to be checked in a group of components being treated as a system for analysis purposes, the relevant RFs are applied to components as a group and not to each component individually. This means that each RF is treated independently of the number of components in the system; each RF is counted only once to be conservative, and also to account for the possibility that not all RFs will be employed on each occasion in which they should be employed. The recovery factor includes the effects of between-person dependence (i.e. dependence between task performer and the second person or other RF performer). Dependence between the tasks performed by one person is included in the dependency effects determination.

The recovery factors (RFs) considered in human reliability assessment would comprise the following.

- (a) Compelling signals - for activities associated with compelling (attention getting) signals, errors are assessed to be fully recoverable. One or more annunciators that must be compulsorily cleared on completion of a maintenance or calibration task or resumption of normal operation would constitute an example.
- (b) Post-maintenance or post-calibration test - in these activities, errors are recoverable if the tests are correctly performed.
- (c) Written verification - in activities with written checkoff provisions, errors can be recovered from. For example, when a second person is required to verify the actions of the original task performer or when the original task performer is required to make a check at a different time and place from the original.
- (d) Written daily check or per-shift check - a daily or per shift check of component status using a checklist.

#### Credit for recovery factors

A condition where the RF is absent is called 'basic'. When the RF is present, the condition is 'optimum'. Each 'basic' condition has its complementary 'optimum' condition. For each activity, it is necessary to determine the 'basic' and 'optimum' conditions (with respect to RFs) that apply. For the case when 'basic' condition is applicable for all RFs, a BHEP of 0.03 is assessed for human caused failure of a critical safety component or system that is unavailable. As an error of commission is always possible even if an error of omission does not occur, each critical action is assigned a BHEP of 0.03.

For the case when 'optimum' condition is applicable for all RFs, the failure probability is negligible because of the multiplicity of RFs available. For intermediate conditions, procedures are provided. The cases that are applicable to the concerned task/activity are found in Table 3-3 below and the corresponding values are used in the HRA.

**TABLE 3.3 : BASIC AND OPTIMUM CONDITIONS**

	<b>Recovery Factor (RF)</b>	<b>Basic Condition (BC)</b>	<b>Optimum Condition (OC)</b>	<b>Recovery Factor Failure Probability or Non-Recovery Probability</b>
1.	Compelling signal available indicating component unavailable status	None	Present	The RF is excellent in this case. So the failure probability is taken to be 1 E - 5.
2	Post- maintenance, Post- calibration tests	There is no verification of component status.	Verification of component status is present. There is full recovery if it is done correctly.	1 E - 2 for failure to do it correctly
3	Written verification	There is no written verification.	Written verification is present.	1 E - 1 for failure of the RF to catch error made by the original task performer. RF is presumed inoperative if the PM/PC test is not done correctly.
4	Written daily or per-shift check of component status (in and outside control room)	There is no written daily or per-shift check	Written daily or per-shift check is present.	1 E - 1 for failure of check to detect unavailable status. #

# For initial Nominal HRA (NHRA), this RF may be used only once per error. If this leads to significant effect of a task on the results, give credit, as in THERP, in a detailed analysis.

When basic condition applies to all RFs (i.e. no RFs available), assess BHEP = 0.03 with EF to be equal to 5. When optimal condition applies to all RFs (all RFs available), assess the HEP to be equal to 1 E - 5.

Considering all the possible combinations of recovery factors that can be associated with an activity, nine cases applicable to critical activities are delineated in ASEP HRA Procedure. For each, the Total Failure Probability (TFP) is listed with its error factor in parenthesis. The TFP is the product of the basic HEP of 0.03 and the probabilities of failure of the relevant RFs. Table 3.4 presents the nine applicable cases and is consulted, using the basic and optimum conditions associated with each activity, in order to determine which of the nine cases applies to the activity under review. The appropriate TFP value is taken from the table and used in the HRA.

The data given in Table 3.4 is taken from Table 5.3 in ASEP HRA Procedure [26]. The Error Factors (EFs) given in the document referred to are calculated using the propagation method for Uncertainty Bounds (UCBs) given in Appendix A of the Handbook [25]. It is an algebraic equivalent of the Monte Carlo procedure. Because this procedure is onerous, a programme for this UCB propagation method in Fortran is given in Appendix B of ASEP HRA Procedure.

(vi) Determine dependence effects and modify BHEP

The dependence between two tasks or activities refers to the situation in which the probability of failure for one task is influenced by the success or failure that has occurred for the other

**TABLE 3.4 : CRITICAL ACTIVITIES IN PRE-ACCIDENT HRA CASES APPLICABLE [26, B3]**

TFP = BHEP x FP of RFs, where BHEP = 0.03. EF = Upper UCB/Lower UCB, where UCB is Uncertainty Bound

No.	RF: Compelling Signal -1	RF: Post-Maintenance (PM), Post-Calibration (PC) Test-2	RF: Written Verification-3	RF: Daily or Per-Shift Check-4	Applicable BCs and OCs	HEP (EF)
1.	Nil	Not effective	Not Used	Not used	All BCs apply	BHEP = 0.03 (5)
2.	Nil	Not effective	Used	Used	BCs : 1,2 OCs : 3,4	$0.03 \times 0.1 \times 0.1 = 0.0003$ (~ 16)
3.	Nil	Not effective	Second person/ other immediate RF is used	Not used	BCs : 1, 2, 4 OCs : 3	$0.03 \times 0.1 = 0.003$ (~10)
4.	Nil	Not effective	Not used	Used	BCs : 1,2,3 OCs : 4	$0.03 \times 0.1 = 0.003$ (~10)
5.	Available (annunciation)	Availability of these RFs does not matter			OCs : 1	Very small, assess upper bound of 0.00001
6.	Not Used	Effective if correctly done	Not used	Not used	BCs : 1,3,4 OCs :	Probability of not or incorrectly performing PM/PC Test = 0.01 $0.03 \times 0.01 = 0.0003$ (~10)
7.	Nil	No credit if not done or incorrectly done	Used	Used	BCs : 1 OCs : 2,3,4	$0.03 \times 0.01 \times 1.0 \times 0.1$ $= 0.00003$ (~16). The 1.0 means no recovery credit is given for OC 3 if PM/ PC test is not done or done correctly as per OC 2.
8.	Nil	Effective if correctly done	Second person/ other immediate RF used	Not used	BCs : 1,4 OCs : 2,3	$0.03 \times 0.01 \times 1.0 = 0.0003$ (~10). The 1.0 means no recovery credit is given for OC 3 if PM/PC Test is not done or done correctly as per OC 2.
9.	Nil	Effective if correctly done	Not used	Periodic check is made	BCs : 1,3 OCs : 2,4	$0.03 \times 0.01 \times 0.1 = 0.00003$ (~16)



task. The dependence may exist between two tasks performed by the same person (within-person dependence), or between the same two tasks performed by different persons (between-person dependence). For the same pair of activities, the level of dependence for errors of commission may differ from that for errors of omission.

The BHEP of 0.03 is modified for effects of dependence. Between-person dependence is already included in the HEPs for RFs. Within-person dependence is considered in this section. In ASEP Procedure, dependence effects for RFs and original task performance are treated differently. For RFs, dependence effects are not specifically considered because of the rule which states that each RF will be applied only once, and because in the exceptions (e.g. for periodic checks), independence can be assumed. For original task performance, dependence effects for series systems and parallel systems are treated differently.

#### Levels of dependence

Though dependence is a continuum, for practical reasons it is separated into distinct levels, varying from three levels (zero dependence, high dependence and complete dependence) in ASEP HRA Procedure to five discrete levels in THERP. However, a conservative simplification would be to separate it into four levels; zero dependence (ZD), moderate dependence (MD), high dependence (HD) and complete dependence CD).

The information to be collected to determine dependence effects includes the following.

- (a) Time reference - The relative times of performing the activities is determined. Two activities are said to occur closely in time if the between-activities time interval is less than two minutes. This time interval is a modification of the one minute guideline in THERP.
- (b) Location reference - Two components are considered to be in the same visual frame of reference of the operator if, while performing an action on one, the operator can see the other. Same frame of reference implies that the components are within four feet of each other.
- (c) Written requirements - For those components not in the same visual frame of reference, determine whether the operator is required to record some information about each or only initial/make a check mark.
- (d) General location - For components not within the same visual frame of reference and with no requirements for writing some information for each, determine whether they are in the same general area (i.e. within four feet of each other).

The treatment of dependence effects differs for series and parallel systems.

- (a) Series system - In respect of activities on different components of a series system, zero dependence (ZD) is assessed for both errors of commission and errors of omission.
- (b) Parallel system - In respect of activities on different components of a parallel system, zero dependence (ZD) is assessed for errors of commission.

Three levels of dependence for errors of omission are considered in Table 3-5 given below.

**TABLE 3.5 : DEPENDENCE ASSESSMENT OF ERRORS OF OMISSION**

Zero dependence (ZD)	If activities do not occur within the same time reference (2 minutes) OR activities occur within the same time reference but components are not in the same visual frame of reference (4 feet) and operator is required to record information.
Complete dependence (CD)	If activities occur within the same time and visual frame of reference.
High dependence (HD)	If activities occur within the same time reference but not in the same visual frame of reference and the operator is not required to record information.

Assessment of dependence

For pre-accident errors, the modelling of dependent errors in the fault trees is affected by the level of dependence that is assigned between the errors. Equations for the calculation of conditional failure probabilities that are associated with the levels of dependence are given below. These equations are taken from the THERP handbook. Dependencies are analysed only at the system level and not at the sequence level, so that the cutset truncation limit is  $10^{-10}$ .

Conditional failure probability (CFP) equations

Level of dependence	Equation of conditional failure probability	Approximate value #
Zero dependence	$P [b/a ZD] = P[b]$	$P[b]$
High dependence	$P [b/a HD] = ( 1 + P[b] ) / 2$	0.5
Complete dependence	$P [b/a CD] = 1.0$	1.0

- (a) Task A is the first task and Task B is the second task.
- (b) Table gives CFP for Task B, given failure of previous task (Task A), for three levels of dependence.
- (c)  $P[b]$  is the probability of failure of Task B, assessed independently.
- (d)  $P [b/a]$  is the probability of failure of Task B, given failure of the immediately preceding task (Task A).
- (e) # when  $P[b] = 0.1$

For each level of dependence, the logic structure of the fault tree is modified if necessary, as given below.

- (i) Zero dependence (ZD) - All human actions that are identified as being completely independent (zero dependence) are modelled in the fault trees as individual basic events, each with its own unique label. In general for the case of zero dependence, the original fault tree will not require modification.
- (ii) High dependence (HD) - Where each dependent event appears, an additional dependent failure event is added to the fault tree in a way similar to the addition of a CCF event for hardware failures. For two tasks A and B, the probability for the dependent event ( $P_d$ ) modelled in the fault tree, is a product of the probability of the independent event  $P_a$  and the conditional probability  $P[b/a]$ , i.e.  $P_d = P_a \times P[b/a]$ .
- (iii) Complete dependence (CD) - All errors identified to be completely dependent are modelled by using the same basic event label in the fault tree. The fault tree analysis software then treats the dependent errors as the same error.

- (vii) Carry out quantification and determine the nominal HEPs.

In this step, the failure probabilities of category A (Pre-accident) human actions, including the influence of RFs and within-person dependence for multiple errors, are assessed. The RFs already include between-person dependence. The steps used to determine nominal HEP are detailed below.

Base information

- (a) Number of components in the system = n.
- (b) BHEP: Total BHEP is assigned for each critical action = 0.03; 0.02 for error of commission and 0.01 for error of omission.
- (c) PSFs: The only explicit PSF, excluding RFs and dependence effects, that is to be considered in the calculation of pre-accident NHEP is radiation (In AECL HRA, if the critical action is performed in a radiation area, then the BHEP is multiplied by a factor of 2).
- (d) RFs : Credit is assigned for all permissible RFs.
- (e) Both series and parallel systems are considered.
- (f) Dependence effects - NHEPs are calculated as shown below.
- (g) Upper bound (UB) and lower bound (LB): Calculated by multiplying and dividing the NHEPs by the EFs.

Calculation of nominal human error probabilities (NHEPs)

- (i) Series system (ZD)

Zero dependence (ZD) is assessed for the critical human actions that are related to series systems. ZD is assessed for errors of omission and errors of commission. For this case, the NHEP is approximated by the following equation:

$$NHEP = n [BHEP \times TRF] = n [0.03 \times TRF]$$

where BHEP = 0.03 (0.02 for error of omission and 0.01 for error of commission for one component), Total Recovery Factor (TRF) is the product of all recovery factors that are to be credited and n is the number of components in the system. The RF values are as given in Table 3.3.

- (ii) Parallel system

Zero dependence (ZD) - If zero dependence is assessed for the critical human actions in a parallel system, the NHEP is approximated by the following equation.

$$NHEP = [0.03 \times TRF]^n.$$

Complete dependence (CD) - For complete dependence between critical human actions in a parallel system, the NHEP is approximated by the following equation.

$$NHEP = 0.03 \times TRF \times [1.0]^{n-1} = 0.03 \times TRF$$

where 1.0 is the conditional HEP, assuming complete dependence, for the second or subsequent human actions.

High dependence (HD) - For high dependence between the critical human actions in a parallel system, the NHEP is approximated by the following equation.

$$NHEP = 0.03 \times TRF \times [0.5]^{n-1}$$

where 0.5 is the conditional HEP assuming high dependence, for the second or subsequent human actions.

### 3.3.4 Post-accident HRA Methodology in ASEP

#### 3.3.4.1 Modelling Post-accident Tasks

Post-accident operator actions are usually modelled in the event trees as separate decision branch points (header events) and are usually placed just before the top event of the associated system that requires manual initiation. In some cases, post-accident operator actions are modelled in the system fault trees. This is usually restricted to those cases where only one system or subsystem is affected by the operator action.

Therefore, for the systematic identification of post-accident human actions, the accident sequence event trees for each initiating event are required to be developed. In addition the analyst reviews the emergency procedures associated with each accident sequence, accident analyses reports and other relevant information. A list of operator actions to be performed for each system and sequence is then compiled.

Both diagnosis errors and execution errors are modelled for the post-accident operator actions. In some situations, even after correct diagnosis, execution errors or system failure may occur. This means that the success criteria for the particular operator action are not met. The operator then is assumed to correctly monitor the state of the plant and realise the occurrence of a failure. For the subsequent operator action in this case, a new diagnosis HEP will be considered, unless this failure possibility is already included in the procedure being followed by the operator, which clearly specifies the action next required.

#### 3.3.4.2 Time Relationship Between Diagnosis and Execution Tasks

A simplification that is employed in the post-accident screening analysis is to divide the total estimated time available for coping with an abnormal event into two artificially independent parts. The total allowable time for coping with an abnormal event is specified by the systems analyst and is divided into an allowable diagnosis time and an allowable execution (post-diagnosis) time. The procedure for estimating diagnosis time is described below.

First, assuming that a correct diagnosis has been made, the time to perform the execution of tasks required in response to the initiating event is estimated. Then this time is subtracted from the total allowable system response time estimated by the systems analyst. The time that is left is the allowable diagnosis time.

$$T_d = T_m - T_a$$

where:

$T_m$  is the estimated maximum allowable time for correct diagnosis of the abnormal event and completion of the required post-diagnosis actions (execution tasks) to meet system success criteria established by the system analyst.

$T_d$  is the estimated allowable time for a correct diagnosis, with sufficient time to perform the post-diagnosis actions within the maximum allowable system response time  $T_m$ .

$T_a$  is the estimated time to get to the appropriate locations and perform the required post-diagnosis actions, following a correct diagnosis.

#### 3.3.4.3 Human Error Probability for Diagnosis Tasks

The HEPs for diagnosis tasks are given below as a function of the available diagnosis time. In assessing diagnosis time, the time starts from the receipt of first alarms and indications of the off-normal conditions and specifically excludes the time taken to execute the specific corrective action required. The diagnosis model (ASEP nominal model) represents the performance of a typical team (crew) expected to be in the control room following an abnormal event. The nominal diagnosis curve from which the following table (Table 3-6) is derived is given in Appendix-6 (Figure AP 6-2).

**TABLE 3.6 : ASEP - NOMINAL DIAGNOSIS MODEL**

Item	T (minutes after To)	Median Joint HEP (Control Room Team)	Error Factor
1	1	1.0	-
2	10	0.1	5
3	20	0.01	10
4	30	0.001	10
5	60	0.0001	30
6	1500 (~ 1 day)	0.00001	30

To is the time at which a compelling signal of an abnormal situation is registered and is usually taken as a pattern of annunciators. A probability of 1.0 is assumed for observing that there is some abnormal situation.

#### 3.3.4.4 Human Error Probability for Execution Tasks

The operator's response in coping with an abnormal event may be classified as either dynamic or step-by-step. A step-by-step task is a routine, procedurally guided set of steps that is performed one step at a time, without a requirement to divide the operator's attention between the task in question and other tasks. Post-accident step-by-step tasks are generally classified as Category C-Type 1 (procedural safety actions). However with practice and high level of skill, a step-by-step task may be performed reliably, without recourse to written procedures. A dynamic task is one that requires a higher degree of interaction between personnel and equipment than step-by-step procedurally guided tasks. Dynamic tasks may include decision-making, monitoring and/or control of several functions or any combination of these. Tasks belonging to Category C-Type 3 (Recovery/Repair and Improvisation Actions) are generally classified as dynamic tasks.

Post-diagnosis actions are also classified as being performed under moderately high stress or extremely high stress levels. A moderately high stress level is a level of disruptive stress that will result in a moderate deterioration of performance effectiveness of most people. The onset of an abnormal event that is indicated by annunciators or other compelling signals, is usually considered as causing at least a moderate level of stress.

An extremely high stress level is defined as a level of disruptive stress that causes the performance of most people to deteriorate rapidly. The occurrence of a large LOCA is assessed as resulting in extremely high stress to operating personnel. Extremely high stress is assessed for the operator under one or more of the following conditions (NUREG/CR-4550).

- (a) maximum time available is less than two hours,
- (b) a single channel tube blockage occurs, or
- (c) more than two safety related systems fail.

NHEPs for post-accident execution errors are quantified using ASEP Procedure. Median values of HEP, which include the effects of stress and complexity of the task, are used to determine the NHEPs. HEPs assessed for the type of task and stress level are given in Table 3.7 (from CANDU generic PSA/HRA) below. This table draws upon the information given in two tables, one from the ASEP document (NUREG/CR - 4772) and another from NUREG/CR- 4550 (a U.S. NRC report entitled 'Analysis of core Damage Frequency: Internal events methodology'). The original performer (OP1) is the operator performing the task.

In the case when recovery of error made by OP1 is still possible at the point of error action, the HEP for the related task and stress categories for the second person in the operating crew (OP2) are to be used. Also, a third person can be credited for verifying the emergency actions and for taking recovery actions during an abnormal state of the plant.

If there are Recovery Factors other than human redundancy (checkers), then the influence of these will be separately assessed. Credit for the second and/or third operator (checker) can be given. The HEP for the third operator (checker) is the same as that of the second operator (checker) given in the table.

Credit for the second and third operator is also conditioned by the following criteria.

For the tasks performed in the main control room:

- (a) If the time allowed is greater than 30 minutes, credit for the second operator is given.
- (b) If the allowed time is greater than 60 minutes, then credit for the second and third operator is usually given.

For the tasks performed in the field:

- (a) If the allowed time is less than 60 minutes, then credit for the second operator is not given.
- (b) If the allowed time is greater than 60 minutes, then credit for the second and third operator is given.

**TABLE 3.7 : ASSESSMENT OF NOMINAL HUMAN ERROR PROBABILITIES BY TASK AND STRESS LEVEL**

Post-Diagnosis Actions (Execution)	Original Performer (OP1)		Second Operator [Checker] (OP2)	
	HEP	EF	HEP	EF
Step-by-step task (Moderate stress)	0.02	5	0.02	5
Step-by-step task (Extreme stress)	0.02	5	0.50	5
Dynamic task (Moderate stress)	0.02	5	0.50	5
Dynamic task (Extreme stress)	0.25	5	0.50	5

Notes:

- (a) The HEPs are for independent tasks or independent sets of tasks, in which the actions that make up the set can be judged to be completely dependent.
- (b) A HEP of 1.0 is assessed for the total failure probability of the post-diagnosis task (diagnosis + execution), if no written procedures are available for a critical skill based /rule based action.
- (c) The HEPs and EFs are taken from the table entitled Assessment of Nominal HEPs for Post-Accident Post-Diagnosis Actions, from the ASEP HRA document.
- (d) Credit to the Second and/or Third Operator (Checker) can be given. The HEP for the third operator is the same as that for the second operator (checker).

The total failure probability of the execution task is the product of the HEPs for OP1, OP2 and OP3. The HEP values for each activity are then added for each task. This yields the total HEP for the task under

investigation. For the tasks, for which there is insufficient time to execute the task, the operator is not credited ( $HEP = 1$ ).

#### 3.3.4.5 Dependencies for Post-accident Actions

For zero dependence, consecutive operator actions are simply assigned the calculated HEPs. For complete dependence, the second and subsequent operator actions (branch points) are assigned a probability of 1.0 (certain failure) on the failure branch of the first operator action, and are generally not modelled in the event tree. For high dependence, the conditional failure probability equation is given in Section 3.3.3.2 (vi) on page 35.

#### 3.3.4.6 Quantification of Post-accident Actions

The total failure probability for a post-accident operator action is taken as the failure of the operator to correctly diagnose the event 'OR'ed with the failure to correctly execute the actions that must be taken within the total allowable time. Thus the total failure probability for the combined diagnosis and execution tasks is given in the following equation.

$$P_t = P_d + P_e - (P_d \times P_e)$$

where:

$P_t$  = total post-accident failure probability

$P_d$  = probability of diagnosis error

$P_e$  = probability of execution error

$P_d \times P_e$  can be conservatively considered to be small, compared with  $P_d + P_e$ , such that the combined failure probability is

$$P_t = P_d + P_e$$

#### 3.3.4.7 Recovery Analysis

Recovery analysis deals with the probabilistic evaluation of recovery actions, and is usually performed after accident sequence quantification at the cutset level. Recovery analysis will be performed on sequence cutsets<sup>@</sup> for a possible damage state, if the probability of that core damage state is higher than acceptable. The operator actions that are credited during recovery analysis are based usually on component/equipment failure at the cutset level.

The following steps are involved in recovery analysis.

- (a) Obtain information for post-accident analysis
- (b) Identify recovery actions that are included in event trees and fault trees.
- (c) Develop accident sequence descriptions.
- (d) Select the dominant cutsets.
- (e) Identify potential recovery actions.
- (f) Determine the available operator time.
- (g) Determine the operator performance time.
- (h) Select viable operator actions.
- (i) Determine the HEP.

<sup>@</sup> A cutset is a combination of basic events resulting in the undesirable event.

The nine steps involved in recovery analysis are detailed below.

- (a) Obtain information for post-accident analysis  
Information for the recovery analysis is based on the plant response that is modelled in the accident sequence event tree analysis.
- (b) Identify recovery actions included in event trees, fault trees.  
Post-accident operator actions are generally modelled in the event trees. In some cases, post-accident operator actions are modelled in the system fault trees. This is usually limited to cases where only one system or subsystem is affected by operator action.
- (c) Develop accident sequence descriptions  
The accident sequences that are relevant for the recovery analysis are identified and the following information is recorded.
  - initiating event and event tree number,
  - event tree sequence number,
  - sequence designator, and
  - accident type and subsequent plant damage state.
- (d) Select the dominant cutsets  
The accident sequence is defined by the initiating event and the set of system successes and failures leading to plant damage. The dominant cutsets are chosen for recovery analysis. In generic CANDU PSA/HRA, the dominant cutsets for the recovery analysis are chosen among those having a frequency that is generally three orders of magnitude lower than the accepted frequency of core damage. For the selected sequence, the mission time is determined.
- (e) Identify potential recovery actions  
The potential recovery actions in the cutset are determined among the component failures in the cutset. These potential recovery actions are usually applicable to one specific failure in the cutset.
- (f) Determine available operator time  
The time available to perform a recovery action is the amount of time from the point at which the affected component has failed, to the time at which plant damage occurs. For various sequences, the available action time can range from tens of minutes to a few hours.
- (g) Determine operator performance time  
This is the time required by the operator to execute the recovery action. If this is a simple action performed in the main control room, it may require only a few minutes. If the action is to be performed on the supplementary control panel, then another 15 minutes are to be added to the operator action time.
- (h) Select viable operator actions  
A recovery action is considered to be viable if the time required to perform the action ( $T_a = T_m - T_d$ ) is less than the time available to perform it. If more than one operator action is required, then the order of initiation of actions is to be stated.
- (i) Determine human error probability (HEP)  
HEPs for recovery actions include the contribution of diagnosis errors and execution errors, which are calculated as per the methodology for quantification of post-accident operator



errors, given in section 3.3.4.6. HEPs for recovery actions during seismic or fire events should consider also the factors delineated in (g) and (h), respectively.

The dominant sequences, with operator errors in recovery actions, may be re-evaluated using THERP or an expert judgement method to calculate the HEP.

### 3.4 Human Cognitive Reliability (HCR) Method

The HCR model quantifies the time dependent nonresponse probability of control room operators performing tasks. The model does not strictly produce a HEP, although analysts use it as such. The method uses the terminology developed by Rasmussen to describe the levels of cognitive processing and also PSFs that may influence task performance.

The notion of success and failure (or correct and incorrect response) intrinsic to the time-reliability correlation is extended by the HCR by adding a third category of 'no response'. The 'no response' can be seen as a result of 'slow cognition', i.e. when the operator uses more time than allowed.

The basis for the HCR model is a normalised time reliability curve, the shape of which is determined by the dominant human cognitive processes associated with the task being performed (skill based, rule based or knowledge based behaviour). The human reliability analyst determines the type of cognitive process, estimates the median crew response time and the time available to the crew, and uses the HCR model to quantify the non-response probability. The extent to which a task is correctly analysed to be rule based versus knowledge based depends on the competence of the analyst. Further, if not enough simulator trials are available to establish a median crew response, then the analyst's judgement is required. The time available to the crew for response is determined on the basis of thermal hydraulic calculations. The HCR curve is given in Appendix-6 (Figure AP 6-3).

The HCR model is applicable to settings other than nuclear control rooms provided that the crew performance times can be determined and the accident phenomenon is known well enough to predict the time available to the crew for their response.

For example, one could model the progression of a fire or flood event at a process plant, until consequences occur. The time required for the fire brigade to come to the site and mitigate the fire or flood could be calculated. The ratio of the time until the fire is contained to the time before the consequences of the fire are realised offsite provides the basis for running the HCR model. Data is best validated by running drills from the fire house to the site and running models of fire dispersion. In nuclear applications, the time reflects the time before either fuel damage or core damage occurs. In process industries, time available may be time until toxic release/explosion.

PSFs, specifically stress, experience and the quality of the HMI are accounted for by adjusting the median time. This is, however, done in a purely quantitative fashion without considering the possible information processing mechanisms that the Skill-Rule-Knowledge (SRK) Framework, as given in Table 3-8, might imply. There is no consideration of how the PSFs influence operator performance. PSFs are assumed to affect the response probability by changing the crew median response time (representing distribution location) and not the variability in response times (representing distribution shape).

The normalised time reliability curves used in the model have been derived from simulator data and small scale tests. The shape of the curves is approximated by three-parameter Weibull distributions. Each distribution corresponds to a category of cognitive behaviour. The three parameter Weibull function has the form

$$P(t) = \exp - \left[ \left\{ \left( \frac{t}{T_m} \right) - B_i \right\} / A_i \right]^{c_i}$$

where

P(t) is the crew non-response probability for a given system time window t, i.e. the time allowed by the system for crews to complete actions before a change in plant state.

$T_m$  is the estimated median time taken by the crew to complete action(s) or task(s).

$A_i$ ,  $B_i$  and  $C_i$  are the coefficients associated with the predominantly  $i$ -th type of mental processing, e.g. skill, rule or knowledge which can be calibrated using simulator data.

Interim values of the parameters  $A_i$ ,  $B_i$ , and  $C_i$  [10] are as given below:

Cognitive Process Type	$A_i$	$B_i$	$C_i$
Skill	0.407	0.7	1.2
Rule	0.601	0.6	0.9
Knowledge	0.791	0.5	0.8

Procedure for using the HCR model

- (i) Identify the actions to be analysed using for example, a task analysis method. Determine the type of cognitive processing used by the crew on the basis of task characteristics and operator training.
- (ii) Obtain estimates of the median response time ( $T_m$ ) for crews to complete the tasks, from sources such as simulator data, expert judgement or task analysis.
- (iii) Modify the median response time to account for the PSFs of stress, crew experience, procedures and the Human Machine Interface.

**TABLE 3.8 : CHARACTERISTICS OF OPERATOR BEHAVIOURS**

Skill Based Behaviour	Rule Based Behaviour	Knowledge Based Behaviour
Reflexive and well rehearsed motor skill behaviours. Some cognitive behaviour and craft skills may also be so classified.	Rules and procedures are always involved.	Situations for which no procedures exist and crews experience and internal supposed to operate. Response to BDB events and respond based on their heuristics for how a plant is situations where operators must correct inaccurate procedures involves knowledge based behaviour.

- (iv) Determine the system time window ( $t$ ), which is the time between the initial plant situation and the time by which the crew must act in order to halt the progression of the accident sequence.
- (v) Calculate the normalised time ( $t/T_m$ ) based on the ratio of the system time window to the estimated adjusted median time.

The parameter values determined from Table 3.9 above are applied as inputs to the normalised crew non-response probability distribution relation to yield a probability of non-response  $P(t)$  for the accident situation of interest. The time taken by the crews to perform a given task ( $t$ ) is normalised by dividing the actual task performance time by the median time ( $t/T_m$ ).  $T_m$  is obtained from simulator measurements, task analysis or expert judgement. The resulting failure probability can then be input to an event tree or fault tree in the PSA.

The HCR model does not include uncertainty distribution for either the Weibull parameters or the median response time. It can however be easily used for sensitivity analyses by varying the time

window, median response time and the inputs of the PSFs. The inputs for PSFs can be changed to reflect the effect of improvements made in the PSFs (procedures, training and the like). Positive changes in PSFs reduce and negative changes increase the performance time.

**TABLE 3.9 : INTERIM HCR MODEL PERFORMANCE SHAPING FACTORS AND RELATED COEFFICIENTS [10]**

Performance Shaping Factor	Coefficients
OPERATOR EXPERIENCE (K1)	
1. Expert, well trained	-0.22
2. Average knowledge, training	0.00
3. Novice, minimum training	0.44
STRESS LEVEL (K2)	
1. Situation of grave emergency	0.44
2. Situation of potential emergency	0.28
3. Active, no emergency	0.00
4. Low activity, low vigilance	0.28
QUALITY OF THE HMI (K3)	
1. Excellent	-0.22
2. Good	0.00
3. Fair	0.44
4. Poor	0.78
5. Extremely poor	0.92

$$T_{ma} = T_m (1 + K1) (1 + K2) (1 + K3)$$

where  $T_{ma}$  = Adjusted Median Time for the PSFs K1, K2, K3.

### 3.5 Expert Elicitation Methods

There are a number of techniques using expert elicitation/judgement to estimate human error probabilities. These include Direct Numerical Estimation (DNE), Paired Comparison (PC) and Success Likelihood Index Method (SLIM). Expert elicitation method SLIM is presented here.

Success likelihood index method (SLIM) [4,5]

Success Likelihood Index Method (SLIM) originates from the field of decision analysis. Its applicability to the assessment of human reliability arises from the consideration that human performance is affected by many factors and therefore it can be quantified by summing up the effects of these factors on human response. Factors like time available, quality of procedures, level of training and experience, etc., are considered to be the Performance Shaping Factors (PSFs). A systematic approach is used to identify these PSFs for a specific set of tasks. The relative importance (weights) of the PSFs are derived by structured expert judgement.

The method comprises two modules: SLIM-MAUD (Multi-Attribute Utility Decomposition), for quantifying the effects of various factors on human reliability, using expert judgements for deriving the relative likelihood of success for a set of tasks; and SLIM-SARAH (Systematic Approach to Reliability Assessment of Humans), for transforming the relative likelihoods into absolute probabilities, using log-linear calibration relationships.

The SLIM procedure comprises ten steps. The first eight steps are performed in the SLIM-MAUD

module and the remaining two by SLIM-SARAH. The approach, described in NUREG/CR-3518 [4], is given below. SLIM assessments usually require multiple judges but they can work alone or together in a group. The method assumes a logarithmic relationship because of the wide range of HEPs (1E-5 to 1.0), which is generally considered. Two tasks, for which the probabilities of success are known, are required, and in order to estimate an HEP, the success probabilities must be subtracted from 1.0

The steps for using the SLIM are as follows.

- (a) Selection of experts - Experts competent to review the task and its requirement of plant personnel are identified.
- (b) Identification of errors - Experts discuss the task and define the ways in which errors could occur. They are supported by making available task analysis and walkdown information, video tapes of performance, administrative and operating procedures, and photographs of equipment that show the quality of the interface.
- (c) Elicitation of PSFs - Experts elicit the PSFs that influence the various potential error modes.
- (d) Documentation - Experts document PSF definitions and descriptions.
- (e) Weighting of PSFs - Experts assess the relative importance (weights) for the PSFs. A simple method, suggested by Ember [4] is to identify the most important PSF and assign it a weight of 100. PSFs of lesser importance are assigned weights in some proportion to it. The weights assigned are normalised by dividing each weight by the sum for all the PSFs.
- (f) Rating of PSFs - The rating indicates how good or how bad a PSF is for the task. Experts rate the PSFs by assigning a numerical value on a scale of 0.0 to 100.0. In this step, experts consider the situation as it exists for a task and take account of it in assigning the PSF ratings.
- (g) Calculation of success likelihood index (SLI) - For each PSF, the product of its rating (how good/bad the PSF is for the success of the task) and its associated weight (how important the PSF is for the success of the task) is evaluated. The sum of the products (for all the PSFs) gives the SLI.
- (h) Conversion of SLIs to probabilities - The SLIs generated are relative measures of the likelihood of success of each of the tasks considered. To transform these to probabilities, it is necessary to calibrate the SLI scale for each set of tasks considered. The relationship assumed in SLIM is:  $\text{Log}(\text{success probability}) = a \text{SLI} + b$ , where  $a$  and  $b$  are constants.  
  
The determination of the values of the constants  $a$  and  $b$  requires that at least two tasks for which success (or failure) probabilities are known are included in the set of tasks and that the SLIs for these tasks are assessed. This produces two equations from which the constants  $a$ ,  $b$  can be calculated. SLIM users select the anchor values from an external source of data. For example, users may want to select a high value and a low value from THERP data tables, which will serve as upper and lower bound respectively for the SLIM session.
- (i) Generation of uncertainty bounds - Experts directly estimate upper and lower bounds, by consensus if they work as a group. If they work independently, then the geometric mean of the estimates for upper and lower bounds should be used.
- (j) Cost-benefit analysis - The SARAH module allows relatively dominant cost-benefit design issues to be resolved quantitatively, so that the impact of a design change on the human reliability of a task can be quickly calculated.

The method for calculation of SLI is based on good theoretical background in decision theory and the easily managed interactivity in the computerised version of SLIM (i.e. SLIM-MAUD) makes the method readily verifiable. The evaluation is easily and rapidly made, once the detailed database has been established. SLIM-MAUD does not require detailed decomposition of the task to an elemental level (as THERP does) but is capable of quantifying human reliability at a higher or more holistic level of task description. A major drawback of SLIM is that it makes extensive use of expert judgement requiring a small group of (e.g. four) experts.

A variation of SLIM [2]

This variation of SLIM is aimed at placing SLIM within the risk assessment framework. The experts' task is made easier by prescribing seven PSFs for use in sessions.

- (i) Plant interface - The degree to which conditions assist or hinder required actions.
- (ii) Significant preceding and concurrent actions - Addresses the situational context in terms of whether there might be lack of attention or a surprise.
- (iii) Complexity of task - Accounts for the effect of multiple requirements in task performance, e.g. accessing multiple locations and communications requirements
- (iv) Procedures - Accounts for the procedure's ability to aid operator/crew actions.
- (v) Training and experience - Accounts for the crew's familiarity and confidence in respect of performing the task.
- (vi) Time available - Adequacy of time available to perform the task (time to decide plus time to carry out the actions, all calculated from the first indication that task is required to be performed).
- (vii) Stress - Acts positively as an incentive or negatively as a reluctance or inability to take action.

The method captures core PSFs that appear with a high degree of regularity. A suggestion made by Chien et al. is to use a rating scale that increases as the likelihood of failure increases. The rating scale supports a failure likelihood index (FLI). FLI parallels the SLI equation.

$$SLI = \sum_{i=1}^j w_i \cdot r_i \quad FLI = \sum_{i=1}^j w_i \cdot r_i \quad \text{where } w_i \text{ is the weight and } r_i \text{ the rating of PSF}_i$$

Another suggestion by Chien et al. is that assessment teams consist of operators and PSA team members, who work together to evaluate the actions under review. The assessment team is provided with a ten-point scale (one for each PSF) as a guide. As an example, the scale for the PSF 'significant preceding and concurrent actions' is given in Table 3.10.

**TABLE 3.10 : SCALING GUIDANCE FOR PSF “SIGNIFICANT PRECEDING AND CONCURRENT ACTIONS”**

0	Previous actions focus operators on the urgent need to act.
1	No distractions from the action and action subject to supervision and follow-up.
2	[No scaling guidance given].
3	Operators are alerted to the need for possible action and are expecting it
4	Another step in standard or procedure based response.
5	Action does not come as a surprise, but previous actions create some competition for the operators' attention.
6	[No scaling guidance given].
7	One of many concurrent actions and so could be overlooked. Operator is involved in recovery actions pertaining to one or two previous problems.
8	Operators are busy with other work or operators are in normal shift operations, and this is an unexpected, unusual transient
9	Previous operator problems create an unusual situation.
10	The need to accomplish this action is unexpected and inconsistent with previous actions.

Individual scores - Assessments made individual members of the assessment team:  
Consensus score - Assessment of the team arrived at by consensus among members:

Rating scales for all seven PSFs assume that 1 is a positive rating, 5 is a neutral rating and 10 is a negative rating.

As in SLIM, the assessment team selects calibration tasks with known HEPs and the authors use a spreadsheet approach instead of the MAUD software used by Embrey. A contribution made by Chien et al. lies in the forms used to document the consensus process and the consistency likely to result in the long term.

### **3.6 An Overview of the State of HRA and Development of Second Generation HRA Methods**

#### **3.6.1 Introduction**

HRA methods were developed to describe incorrect human actions in the context of PSA. The basic premises for HRA were:

- (i) It must function within the framework of PSA and
- (ii) It must produce the human action failure probabilities needed.

In PSAs, accident sequences are generally represented by event trees. The nodes in the event sequence represent the function of a component/system or operator-system interaction and can have a success/failure outcome. For PSA it is necessary to know whether an event ends in success/failure and further determine the probability of failure. For components, failure probability is calculated from engineering knowledge and plant data. For operator-system interactions, HRA provides the basis for calculating HEP.

From the beginning HRA used procedures similar to those used in established reliability analysis. Human tasks were substituted for equipment failures and modifications were made to account for the greater variability and interdependence of human performance. HEP for a human interaction was first obtained from available databases, human reliability models or expert judgement. This HEP was then modified by a numerical factor to account for the influence of PSFs, i.e. task, environment and work situation and other characteristics.

In using the above approach, two assumptions of consequence have been made. These are as follows.

- (i) The probability of failure can be determined for specific types of action independent of the context.
- (ii) The effects of context are additive. In other words, the performance conditions (like quality of interface, levels of stress and training and complexity of task) do not influence one another.

Neither of the two assumptions can be justified and either assumption alone implies a deficiency in the approach to HRA.

#### **3.6.2 First Generation HRA and Its Shortcomings**

The HRA methods described thus far, namely, THERP, ASEP, HCR and SLIM are considered to be first generation HRA methods. In practice, these methods were not very effective and the need for improvements was recognised early on. The shortcomings were summarised by Dougherty in 1990 in an important paper [3] that established the distinction between first-generation (traditional) and second-generation (modern) HRA approaches. The first-generation HRA approaches were more concerned with whether humans met with success or failure than with what they are likely to do.

The shortcomings delineated by Dougherty were:

- (i) Insufficient data to support the quantification of human performance in complex systems.
- (ii) Expert Judgement is used in place of empirical data but there is lack of consensus in the use of

expert judgement methods. There is a lack of accuracy in predictions and no consistency among experts.

- (iii) Simulator data can be used in place of empirical (i.e. observation/experience based) data but calibration to plant situations is not adequate. The applicability of the data has not been convincingly demonstrated for reasons like the stress situation being different and operators being well aware that they are not in the real plant. These biases that are inherent in the use of a simulator make calibration to field data difficult.
- (iv) Accuracy of prediction by HRA methods has not been proved particularly for non-routine tasks (e.g. tasks involving time constrained diagnosis and misdiagnosis).
- (v) Many models and approaches are based on the assumptions made in respect of human behaviour. These may not be valid from the view point of psychology and behavioural science.
- (vi) The treatment of important PSFs is inadequate. There is little emphasis on PSFs relating to management methods and attitudes, organisational factors, culture and irrational behaviour.

In the view of Alan D. Swain, a pioneer in the field, the above inadequacies have led HRA analysts to deliberately assess higher estimates of HEPs and UCBs to compensate for those probabilities. Knowing that such an approach is inappropriate, HRA researchers initiated the development of improved HRA methods that could overcome the above shortcomings.

### 3.6.3 Improving HRA - Context and Cognition

The shortcomings of HRA pointed to the problems of Context and Cognition. In the above, 1, 2, 3 and 6 relate to Context and 4 and 5 relate to Cognition. Human performance takes place in a context, i.e. the situation or framework in which a human functions. Context includes not only the actual performance conditions but also the operators' perception or understanding of the conditions. The actions of a human are the result of cognition, i.e. his/her perception, reasoning, understanding and also his/her beliefs. The actions are therefore not simple responses to events. Beliefs further may be shaped and shared by the crew as a whole.

The consequence of recognising the importance of context is that analysts need to analyse human actions not separately, but as parts of a whole. Further, 'human error' should be looked upon as a way in which erroneous actions can occur in a specific context.

### 3.6.4 Operator Models [8, 9]

#### 3.6.4.1 Main Groups of Operator Models

Many classes of operator models have been used in describing and understanding the failure of human actions. However, the different classes can be grouped together to form three main groups. The three groups of operator models are as follows.

- (a) Behavioural or human factor models.

Behavioural models concentrate on error modes or simple manifestations of error. Error modes are generally described as omissions, commissions and extraneous events. A classical behavioural model is the Stimulus-Organism-Response (SOR) Model, which was initially used in THERP. The methods associated with these models aim to derive the probability that a specific mode/manifestation will occur. Cause-effect representation is either very simple or non-existent. It is therefore not possible to use a behavioural model for predicting performance failure. Behavioural models are therefore also weak in accounting for the influence of the context.

- (b) Information processing models

Information Processing (IP) models concentrate on internal human information processing mechanisms, e.g. interpretation, evaluation, planning and decision-making. The Operator Action

Tree (OAT) model considers information processing mechanisms. OAT divides operator response into observation, diagnosis and response phases, but only considers error in diagnosis. The methods associated with IP models aim to explain cause-effect flow through the models. Cause-effect representations are therefore often complex, but have limited capability for failure prediction and little concern for quantification of human reliability. Context is considered at most as input to operator. IP models are better suited for retrospective analysis.

(c) Cognitive models.

Cognitive models concentrate on the relation between error modes and causes in the socio-technical environment as a whole. Cognitive models are used in some new HRA approaches. The methods associated with cognitive models consider human performance as resulting from the interaction between the demands from the monitored process and the organisational environment in which it exists and the resources and constraints of the working environment. The resources and constraints are explicitly provided by the organisational framework, say in terms of procedures, rules, limits and tools. Cognitive models are simple and context is explicitly represented. The models are suitable for both retrospective and predictive HRA

### 3.6.4.2 Operator Models: Fine Distinctions [8, 9]

Some fine distinctions between the three classes of operator models are explained below.

- (a) The S-O-R concept dominated behavioural psychology in the early days of HRA. Error events were described in terms of behavioural components, which emphasised the perceptual-motor aspects rather than the cognitive aspects of human action. The “O” in the S-O-R model was the human component, which was viewed as a “black box” processor. In the original THERP, which used this model, “Stimulus” was the Input, “Organism” was the description of the human component (what goes on in the human mind) in terms of “Mediating Activities and Processes” and “Response” was the Output.
- (b) Machines and processes had from the beginning been described in terms of flows of information and control. Therefore, the introduction of information processing psychology made it possible to describe the operator in the same way. The “O” in the S-O-R model was therefore extended by the information processing approach by adopting Rasmussen’s Step Ladder Model. Human performance was analysed from an information-processing perspective to trace the flow of information through the cognitive stages that are presumed to mediate between a stimulus and a response.
- (c) Early cognitive psychology found the divide between known descriptions of brain functions and descriptions of cognitive functions to be too large. Models therefore made use of a Human Information Processor (HIP) in the brain serving as a link between the level of brain function and the level of cognition. Human cognition was assumed to be information processing and by this assumption, models of cognition had to be information processing models.
- (d) As a result of assuming the presence of a HIP in the brain, it became necessary to assume that cognition is sequential and also assume the existence of context free processes. However both these assumptions could not be justified.
- (e) In reality it was found that cognitive models need not account for cognitive processes as a set of steps/stages executed one by one. A well-ordered flow of actions is required only with the HIP model concept. In fact, the actual sequence of actions is a result of the complex coupling between processes internal and external to the human, between a person’s control of the situation and conditions that existed at that time. It is not due to a built-in dependency among cognitive functions. Although the sequence in Rasmussen’s Decision Model, from ‘observation’, through ‘integration’, ‘interpretation’, ‘evaluation and ‘planning’, to ‘action’, appears to be taking place in an orderly manner, in reality it is not.
- (f) As regards the assumption of existence of context free processes, while information processing



in technological systems can be described in a context free manner in terms of elementary functions (e.g. arithmetic, logic and control), it does not make sense to describe basic human processes in the same way. Cognition is not an epiphenomenon of information processing, i.e. it is not a secondary phenomenon accompanying information processing and caused by it.

- (g) In the light of the arguments in e and f above, cognition and cognitive processes are to be studied within a context and to model it the approach must be functional rather than structural, i.e. it must be described in terms of what the actions accomplish than in terms of assumed mental mechanisms that may be involved. Cognition is assumed to be the basis of how humans adapt to the changing circumstances and cope with complexity.
- (h) To sum up, the cognitive systems engineering perspective relies on two important assumptions regarding the analysis of human performance in a work setting. Firstly, it assumes that the interactions between human and system are best viewed in terms of a joint (human-system) cognitive system and secondly, it advocates that the behaviour of the human operator (and therefore possible erroneous actions) are primarily shaped by the socio-technical context in which the behaviour occurs, rather than the characteristics of an internal information processing system. Additionally, in the joint cognitive system perspective, the use of advanced computers in control systems is taken into account, by considering the machine system too to be a cognitive element with the ability to make decisions in respect of the current state of the process. Such systems can for instance, respond to certain classes of process events, without the need for active intervention by the operator.
- (i) The notion of the joint cognitive system implies that, both process (or machine) and operator should be modelled and that coupling the two models is necessary to analyse the details of their interactions. This means that the modelling of the human operator as a system is in itself not sufficient and this is the basic reason why classical information processing models are inadequate for analyses of human erroneous action. Although the situation or context is present as input data, the representation does not capture the dynamics and complexity of the interaction. This can only be achieved by providing a coupled model of the human-machine system.
- (j) In contrast to the information processing view, which assumes that all information-processing activities are essentially reactive, the Cognitive Systems Engineering (CSE) perspective is based on the premise that cognition is an active process that is shaped by the operator's goals and the prevailing situation or context. With this interpretation of cognition, it is more appropriate in describing the behaviour of the human operator to focus upon the global characteristics of human performance (both correct and incorrect responses according to specific situational characteristics) than to confine the analysis to malfunctions of presumed cognitive mechanisms. The implications of the CSE perspective have been used to guide the definition of contextual models of operator behaviour. An example of this type of model is the Contextual Control Model (COCOM) used in Cognitive Reliability and Error Analysis Method (CREAM) approach.

#### 3.6.4.3 Some Observations on Operator Models in HRA

Most of the first generation approaches have no operator model. The influence of PSFs is considered but there is no method to describe or explain how they exert this influence on operator performance.

- (a) The SOR model initially used in THERP was extended later with a description of cognitive functions assumed between perception and action, using a variation of Rasmussen's Step Ladder Model.
- (b) Expert elicitation methods like SLIM have no operator model.
- (c) Few HRA approaches use cognitive models.
- (d) The cognitive view implies that undesirable consequences are due to mismatch between context and cognition.

- (e) Representing Cognition: In cases where human interactions comprised cognitive functions, the event tree representation was not justifiable because what failed was a mental function that was inferred rather than observed. One solution (as explained in Section 2.2.2) was to breakdown an operator action into identification/diagnosis, decision-making, execution and recovery and represent the operator action as an event tree. The implication of this was that it was necessary to get Basic HEPs (BHEPs) for each of these - a requirement which arose from the 'structural' break down of an operator action.

### 3.6.5 Second Generation HRA - Concepts and Methods [8, 9]

#### 3.6.5.1 Basic Concepts of Second Generation HRA Methods

The basic concepts of second generation HRA methods are as follows.

- (a) The likelihood of incorrect action is determined by the performance conditions.
- (b) The conditions relevant to the context may force an error leading to human performance failure. Such conditions are termed Error Producing Conditions (i.e. conditions that can have a negative effect on human performance or conditions that increase the order of magnitude, frequency or probability of error). The context is then referred to as an Error Forcing Context (EFC). Analysis of accidents indicates that many erroneous events are the result of error prone situations and error prone activities rather than error prone humans.
- (c) As the context is an EFC, the focus shifts to performance as a whole. Whether the failure is on the part of an individual operator or of the crew/team becomes irrelevant.
- (d) Based on the observations b and c, the question can be posed whether error/failure probability can be determined by characterisation of the context.
- (e) The focus of HRA can now shift from identifying potential human failures to developing ways to describe how the joint Human-Machine System (HMS), a socio-technical system, depends on the prevailing conditions and predict how it can lose control - not whether the human can cause a failure.
- (f) A human failure is a single event that requires other conditions, referred to as Common Performance Conditions (CPCs), to result in an accident. CPCs were proposed as a way of taking into account the essential aspects of the situation and the conditions of work, which through long experience are known to have consequences for how work is carried out and in particular for how erroneous actions occur. The term CPC was not chosen because the individual CPCs are different from PSFs, but because there is a difference between how the PSFs and the CPCs are used in analysis. The influence of the PSFs is expressed as a numerical factor that is used to modify the HEP and the effects (of the context) are considered to be additive. In other words, the various performance conditions are considered not to influence one another. The assessment of CPCs in a second generation HRA method can lead to an overall prediction of how likely the operator (and hence the joint HMS) is likely to lose control. The prediction can be made without considering failure probabilities for specific operator actions.
- (g) The unit of analysis now is the joint HMS not the individual operator/operating crew.
- (h) Data - There is no need now to carry out extensive data collection on the level of individual human performance and generate HEP data.
- (i) Models - Models are to be developed of how working conditions influence the way humans adjust their actions to meet the set goals. Earlier the focus was on the analysis of human performance to arrive at the possible internal failure mechanisms.
- (j) The influence of organisational factors on performance gains new meaning. Organisation itself is a constituent of the context.

### 3.6.5.2 Second Generation HRA Approaches

Three second-generation HRA approaches exemplifying the concepts delineated above are described in the following sections. The approaches are:

- (i) A technique for human error analysis (ATHEANA)
- (ii) Cognitive reliability and error analysis Method (CREAM)
- (iii) Methode d'évaluation de la réalisation des missions operateur la surete (MERMOS) - [Method for assessing performance of human factor missions for safety]

### 3.6.6 Classification of HRA Methods

Considering the range of approaches to HRA (both first and second generation), a classification drawn from Pyy [19] is given in Appendix-1. Pyy classifies HRA methods according to:

- (i) Modelling level of detail
- (ii) Treatment of diagnosis/decision-making and cognitive mechanisms
- (iii) Treatment of time dependence
- (iv) Treatment of contextual factors
- (v) Data used.

The figure in Appendix-1 shows how some of the most generally used HRA methods relate to these classes.

## 3.7 A Technique for Human Error Analysis (ATHEANA) [8]

### 3.7.1 Purpose

The purpose of ATHEANA is to develop an HRA approach that could improve the ability of PSAs to identify important Human-System Interactions, represent the most important severe accident sequence and provide recommendations for improving human performance based on an analysis of possible causes. Although ATHEANA has been developed so that it can be used within the established HRA framework, it does not accept the HRA event tree as the only basis of analysis, but provides a possibility of enhancing the PSA model.

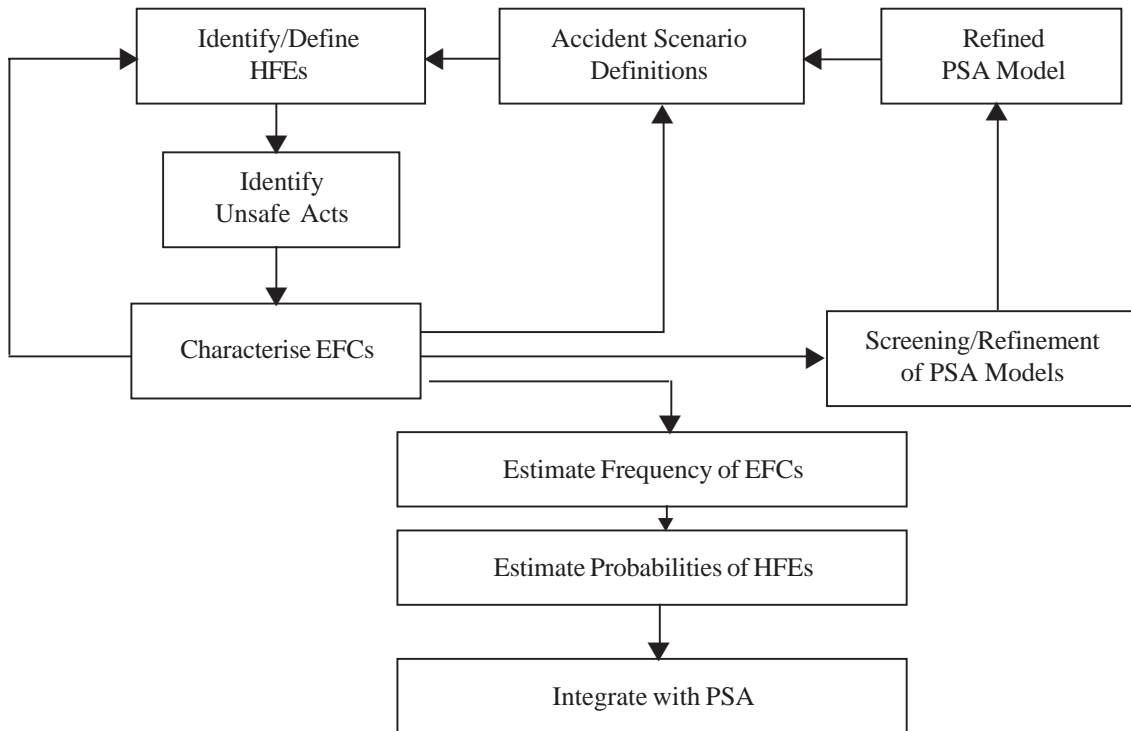
### 3.7.2 Method

The method used by ATHEANA is clearly described and is shown in Figure 3.1. The method begins by identifying possible Human Failure Events (HFEs) that are described by the PSA event tree. These are further characterised in terms of unsafe acts (slips, lapses, mistakes and circumventions) referring to the set defined by Reason [29]. The next step is to consider the Error Forcing Contexts (EFCs), which are defined as combinations of PSFs and plant conditions that make human erroneous actions likely. This is one important extension of the traditional concept of PSFs and acknowledges that human actions to a significant degree are determined by the context. EFCs are provided as verbal descriptions rather than as a set of predefined categories.

The ATHEANA method incorporates two important loops. The first is from characterisation of EFCs to the identification of HFEs. This recognises that improved descriptions of context may enable a better identification of HFEs and that this may amend the description of context. The second is from characterisation of EFCs to the PSA model. This suggests that the outcome from the qualitative part of HRA may be used to modify the underlying PSA model, for instance by pointing to conditions of the human interactions that have been missed in the first place.

The final quantification step is the same as in earlier approaches and is expressed by:

$$p(E/S) = \sum_{\text{unsafe act}_i} \sum_{\text{EFC}_j} p_{ij}(S)$$



**FIGURE 3.1 : THE ATHEANA METHOD**

where  $p(E/S)$  = Probability of HFE in scenario S and  $p_{ij}(S)$  = Probability of unsafe action  $i$  resulting from  $EFC_j$  in scenario S.

Loops incorporated:

Loop 1: Formed by the path from characterisation of EFCs to Identification of HFEs, through identification of unsafe acts back to characterisation of EFCs.

Loop 2 : Formed by the path from characterisation of EFCs, through PSA modelling to identification of HFEs, identification of unsafe acts and back to characterisation of EFCs.

### 3.7.3 Classification Scheme

ATHEANA uses a classification scheme in two different ways. Firstly, it conforms with PSA tradition in distinguishing between omissions and commissions as basic HFEs. Secondly, it uses Reason's characterisation of unsafe acts as a further refinement of basic HFEs. ATHEANA acknowledges several of the recent developments in cognitive psychology and cognitive engineering, but does not propose any classification system. The need to interface with practical PSA may have been the obstacle.

### 3.7.4 Model

Even though ATHEANA perhaps deliberately continues with the established classifications of error types, it argues that a better operator model is needed. In accounting for links between EFCs and HFEs, reference is made to an Information Processing model with four stages, which are Detection, Situation Assessment, Response Planning and Response Implementation. This is a generic model similar to Simple Model of Cognition (SMoC), which is presented later in the chapter. The model could have been used as the basis for a more elaborate classification scheme but this has not been done at the present stage of development.

### 3.7.5 Concluding Remarks

ATHEANA is an HRA approach that has been developed in the mid-nineties and described in publications in 1998. It was developed to increase the degree to which an HRA can represent the kinds of behaviour seen in serious accidents and near-miss events in NPPs and other situations with similar kinds of human-system interactions. Though it is by nature a first generation approach, it does propose an iterative qualitative analysis, which has the possibility of providing a significantly improved basis for quantification. Work is underway to develop an ATHEANA Application Tool and to strengthen the steps of the method.

### 3.7.6 Summary

Approach	Method	Classification Scheme	Operator Model	PSF Effects
ATHEANA	Well described	Minor extension of basic schemes	Basic Information Processing Model of 4 stages	Integrated with classification as EFCs

## 3.8 Cognitive Reliability and Error Analysis Method (CREAM) [8]

### 3.8.1 Introduction

CREAM is the result of E. Hollnagel's efforts to overcome the inadequacies in existing approaches to HRA and develop a new second-generation approach. The primary purpose of CREAM is to realise a practical approach to the analysis and prediction of human performance. The connotation of each of the terms in CREAM is as follows.

**Cognitive:** The approach considers the role of human cognition in human performance. Cognition is the act or process of knowing, including both awareness and judgement (Webster's New Collegiate Dictionary, 1975).

**Reliability:** For HRA contexts, human performance is determined by human cognition in conjunction with technology and organisation. The reliability of human cognition or cognitive reliability is important to HRA. It is necessary to evaluate the probability of cognitive reliability, or at least to estimate the upper and lower bounds of variability of human performance.

**Error/Erroneous action:** Error analysis is directed towards finding the causes of errors in retrospective analysis. While psychologists focus on developing systems to explain error, HRA practitioners focus on finding ways of calculating the probabilities of action failures.

**Analysis and assessment:** Analysis implies breakdown of a whole into smaller elements for study and better understanding. In analysis, qualitative aspects are emphasised. Assessment implies assigning a numerical value (probability of an event in HRA) and quantitative aspects are emphasised. As HRA is mostly carried out in the context of PSA, the emphasis on Quantification (Assessment) is strong. However, it is Analysis that really needs to be emphasised, because: 1. there cannot be an assessment without a preceding analysis, and 2. the value and use of HRA is in the improved understanding that comes from analysis. In contexts other than PSA/HRA, such as Human-Computer Interaction, it is analysis, which plays a prime role.

**Method:** The need for human reliability analysis and quantitative assessment makes an adequate method essential for HRA practitioners. It may be noted that the term 'Method' refers to a specific tool, while the term 'Methodology' refers to principles behind the tool.

### 3.8.2 Principles of Method and Model of CREAM

#### 3.8.2.1 Principles of CREAM

The main principles of the method are as follows.

- (i) The method is fully bi-directional (i.e. the same principles can be applied for retrospective analysis in the search for causes and also for performance prediction). This enables the analyst to use the results from event analyses to improve performance prediction.
- (ii) The method is recursive (i.e. it can repeat itself indefinitely until a specified condition is met) as opposed to sequential. This is a consequence of the classification scheme.
- (iii) The method contains a clear stop rule, i.e. there are well-defined conditions when analysis/prediction comes to an end. This is important so as to ensure consistency in use of the method and also necessary because, as the method is recursive, the analysis/prediction can otherwise go on forever.

### 3.8.2.2 Fundamentals of the CREAM Model

Any description of human actions must recognise that they occur in a context and any model that is used as a basis for describing human performance and actions should be capable of accounting for how the context influences actions. In this respect neither human factors models nor information processing models are able to account adequately for how context and actions are coupled and mutually dependent.

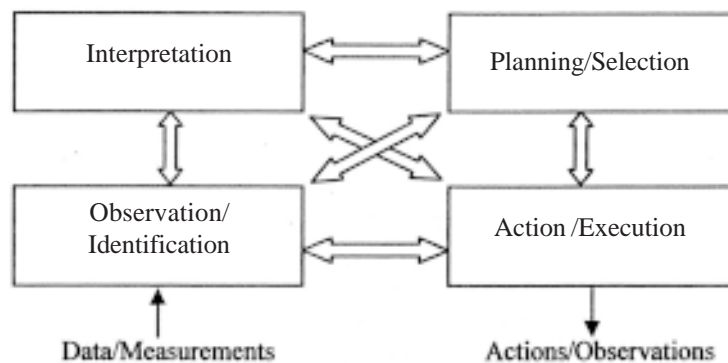
Hollnagel, in an earlier work, presented an approach to the modelling of cognition, which overcame the limitations of information processing models and described how performance depends on context. The basic principle in the approach was a description of competence and control as separate aspects of performance. Competence is what a person is capable of doing and control is how competence is realised, i.e. a person's level of control over the situation. The level of control depends on the situation (context). A better control of actions implies that actions are less likely to fail or performance is more reliable.

### 3.8.2.3 Models of Cognition

Two models of cognition, simple model of cognition (SMoC) and contextual control model (COCOM) are described below.

- (i) Simple Model of Cognition (SMoC)

SMoC has a small set of cognitive functions that reflects the general consensus on the characteristics of human cognition as it has developed and the basic functions found in new HRA approaches like ATHEANA (A technique for human error analysis). The cognitive functions in SMoC are observation/identification, interpretation, planning/selection and action/execution, as shown in Figure 3.2.



**FIGURE 3.2 : SIMPLE MODEL OF COGNITION (SMoC)**

The two fundamental features of this model are:

- (a) Observation/identification is distinct from inference. Human behaviour involving human actions can be observed. This corresponds to the functions of action/execution and

action/observation. Observation is the manifestation of perception, the actual cognitive process. The other cognitive functions (interpretation and planning/selection) can only be inferred from the observations.

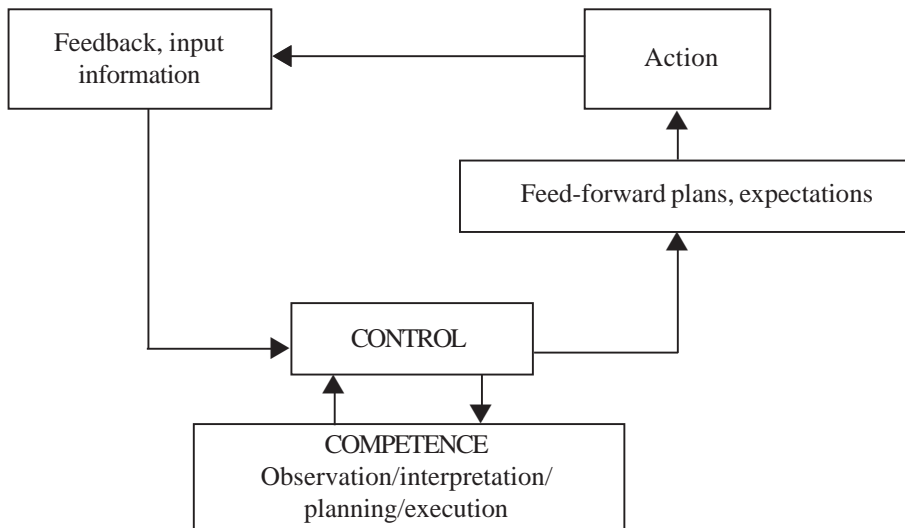
- (b) Human cognition has a cyclic nature. The cognitive processes occur in the context of past actions and anticipated future events. Action execution can be preceded/caused by planning, interpretation or observation/identification, all of which in turn can follow as a result of action or event occurrence.

A cyclic model like SMOc can generate any sequential model, including the well-known step-ladder model of Rasmussen, if the appropriate number and types of functions are included.

(ii) Contextual control model (COCOM)

The model used in CREAM is a development of SMOc called the Contextual Control Model (COCOM), based on a fundamental distinction between Competence and Control that offers a way of describing how performance depends on context, as shown in Figure 3.3.

Instead of describing the human mind as an information processor, the focus is on how actions are chosen. The degree of control that a person has over his/her actions may vary, and this to a large extent determines the reliability of performance. Control is described in terms of distinct modes on a continuum going from no control (erratic performance) to perfect control (highly reliable performance).



**FIGURE 3.3 : THE CONTEXTUAL CONTROL MODEL OF COGNITION**

COCOM does not define specific ‘routes’ of human information processing. It describes how a sequence of actions can develop as the result of interaction between competence and context. In addition to processing input and producing a response, cognition also involves the continuous revision and review of goals and intentions, i.e. a loop on the level of interpretation and planning. Cognition should therefore not be described as a sequence of steps, but as a controlled use of available competence (skills, procedures, knowledge) and resources.

3.8.3 Classification Scheme

The classification scheme in CREAM consists of a number of groups that describe phenotypes (error modes, manifestations) and genotypes (causes) of erroneous actions. Both phenotypes and genotypes are further divided into detailed classification groups, which are described in terms of general consequents (or effects) and specific consequents (or effects).

- (a) The phenotypes are the description of error modes, which are divided into four classification groups. Each phenotype group has general effects and each general effect is delineated into a set of specific effects. The four groups are as tabulated in Table 3.11.

**TABLE 3.11 : TABLE OF PHENOTYPES**

Group	Description	General Effects	Specific Effect
Group 1	Action at wrong time	Timing	Too early, too late, omission
		Duration	Too long, too short
Group 2	Action of wrong type	Force	Too much, too little
		Distance	Too far, too short
		Speed	Too fast, too slow
		Direction	Wrong direction
Group 3	Action on wrong object	Wrong object	Neighbouring, similar or unrelated object
Group 4	Action in the wrong place or sequence	Sequence	Reversal, repetition, commission, intrusion

- (b) The genotypes describe the categories in the classification scheme that serve as antecedents - hence ultimately as attributed causes. These are divided into different classification groups, which in turn are assigned to three main categories, person related, technology related and organisation related. The main categories are as delineated in Table 3.12.

Groups describing causes (Genotypes)

Each subcategory has general consequents and each general consequent is divided into a set of specific sub-consequents. The consequents describe observable or inferred consequences. For example, the general consequents for 'observation' are observation missed, false observation and wrong identification. The specific consequents for 'observation missed' are overlook cue/signal and overlook measurement; for 'false observation' they are false reaction and false recognition and for 'wrong identification' they are mistaken cue, partial identification and incorrect identification.

**TABLE 3.12 : TABLE OF GENOTYPES**

Genotype Category	Person Related	Technology Related	Organisation Related
Genotype subcategories	Observation	Components	Communication
	Planning	Procedures	Organisation
	Interpretation	Temporary interface	Training
	Temporary person	Permanent interface	Ambient conditions
	Permanent person		Working conditions

#### 3.8.4 Context Dependence of Classification Groups

The degree of context dependence of the classification groups and constituent factors is important for both analysis and prediction. In a retrospective analysis the context of the event is known in advance and this may be used to select a subset of the classification groups and/or antecedents that is particularly



relevant. This prior selection is not possible in the case of prediction, because the nature of the situation is unknown. All genotypes are context dependent, although the degree of context dependence can vary.

### 3.8.5 Relations Between Classification Groups

- (a) In accordance with the principles behind CREAM, there are no permanent or hierarchical relations between the various classification groups. A definition is given of the links between consequents (effects) and antecedents (causes) for each classification group.
- (b) In contrast to the scheme in a sequential model of cognition, which corresponds to a hierarchical ordering of concepts and causes and hence also a well-defined path or a set of paths through the classification groups, these links describe a number of potential pathways through the classification groups.
- (c) The realisation of a specific pathway depends on the conditions under which the actions take place, and therefore take the influence of the context into account. In other words, the non-sequential model of cognition selects a path through the classification scheme, guided by possible causal links between the various cognitive functions.
- (d) The above is the case for both backward propagation (accident analysis) and forward propagation (performance prediction). In both cases the links reflect the prevailing Common Performance Conditions (CPCs), as they are known/assumed by the analysis/prediction respectively. The depth of the analysis is determined by pre-defined stop rules.

### 3.8.6 A Recapitulation of the Main Points of CREAM

- (a) The basic assumption is that human performance is an outcome of the controlled use of competence, adapted to the requirements of the situation rather than the result of pre-determined sequences of responses to events. The method in CREAM reflects the assumption made.
- (b) The non-sequential nature of cognition could be accounted for by weakening/removing links between cognitive functions in SMoC. This would lead to an unorganised type of model with no obvious links between cognitive functions. COCOM differs from SMoC in that the links between cognitive functions have been relinquished, implying there are no cause-effect relations among them.
- (c) Competence can be described in terms of a relatively small number of the essential functions of human cognition. In addition, competence also includes a person's skills and knowledge that may have been compiled into familiar procedures and response patterns (action templates).
- (d) Control can be described by referring to a continuum going from a situation where a person has little/no control over events, to conditions where events are under complete control.
- (e) Earlier, it was assumed that the causes could be traced backwards from Observation to Interpretation to Planning. This assumption imposed a constraint on the classification scheme. Analysis showed that this constraint is unnecessary and its removal would improve the range of possible cause-effect links.
- (f) In the present stage of development of CREAM, analysis is guided by the way groups of antecedents (causes) are associated with each other, and with the consequents (effects). In CREAM, the concept of control and control modes provides a structure to the actions. Control is used to organise the actions within the person's time frame. The control modes enable the classification scheme (comprising groups of phenotypes-error modes and genotypes-error causes) and method (recursive, non-sequential) to be linked with COCOM, a model of cognition that is of dynamic nature. This is of particular interest in attempts to base HRA more explicitly on models of cognition. To use the classification scheme and the method, it is necessary to begin by establishing an understanding of what the likely context is. From this, it will be possible to infer the likely mode of cognitive control.

In COCOM, control and competence are separated, recognising the fact that cognitive functions (observation, interpretation, planning, execution) evolve in a context consisting of past, as well as anticipated, future events. This contrasts with a strictly sequential model of cognition where one action follows the next in a predefined pattern. COCOM principles can be used to describe how the execution of a particular action for instance can be preceded (or caused) by planning, by interpretation or by observation, depending on the context and the mode of control. In the event analysis to be carried out, the causal connections are to be arrived at, as there is no a priori causal chain that links the cognitive functions.

### 3.8.7 Method for Retrospective Analysis Using CREAM

Retrospective analysis is accident and event analysis. The purpose of a retrospective analysis is to find the likely causes for a given accident or event by developing a path of probable cause-effect relationships by working backwards from the observed effect. A retrospective analysis using CREAM consists of the following steps.

(a) Determine/Describe the context

This is done using the notion of common performance conditions (CPCs). To describe the context fully, it may be necessary to analyse in detail the aspects of the application, which may not be available in the event report.

(b) Describe the possible error modes.

This description is to be given for all possible actions, i.e. considering each specific action in turn. The description uses knowledge of the application and the context to delineate a limited set of error modes and also define the criteria for certain error modes (e.g. when is an action too late).

(c) Determine the possible causes.

From the knowledge of the context, it is normally possible to identify categories of causes that are more probable than others. In case the categories refer to cognitive functions, it is not possible to completely rule out any of them. For any given context, there will however be some that are more likely than others. Thus the work context may enforce compliance with rules, encourage deviations, support learning of skills and promote misunderstandings or execution errors because of a poor interface design.

(d) Perform a more detailed analysis of main task steps.

This stage will try to trace the possible consequent-antecedent links for selected error modes.

### 3.8.8 Concluding Remarks.

Some human errors, e.g. errors of commission and knowledge-based errors are not adequately modelled in PSAs. Even qualitative methods for analysis of these errors are not fully developed. CREAM was developed for prediction of cognitive error modes. It has not yet been comprehensively established how reliable, valid and generally useful it could be to researchers and practitioners of HRA.

## 3.9 **MERMOS- Methode d’Evaluation de la Realisation des Missions Operateur la Surete (Method for Assessing Performance of Human Factor Missions for Safety)**

### 3.9.1 Introduction

MERMOS, a HRA method developed by Electricite de France [16], takes into account the computerisation of control rooms and Emergency Operating Procedures (EOPs) in the newer plants. In MERMOS, the decisions and actions of operators are referred to as human factor missions. A human factor mission (HFM) is a set of macro actions (decisions and actions) the crew has to carry out in order to maintain/restore safety functions.

Operating crews in French NPPs comprise two operators (one in charge of the nuclear system and another in charge of the secondary system), a supervisor in charge of monitoring the actions taken by operators and a safety engineer who is there as a backup, if the need arises. Each member of the crew has his own specific procedure. In the N4 NPPs, EOPs are computerised for the operators and also for the supervisor. This ensures redundancies at various levels, apart from double checks. Any differences in points of view prompt collective exchanges on how to cope with an accident. As a result, coordination within the crew plays an indispensable role in emergency operation.

A Human Factor Mission (HFM) is considered to be a failure when the operations crew (excluding the safety engineer) fails in its tasks and the safety engineer (who is a backup to the operations crew) cannot recover from operator failure.

### 3.9.2 Development of 'MERMOS'

The need to develop the new HRA method, MERMOS, arose from the following factors.

- (a) There are four procedures, one for each member of the crew. To recover from an event, members individually apply their procedures. In addition, they also interact with each other frequently. To account for this collective functioning in emergency operation, a way to consider the crew jointly functioning as one, rather than as individual members, is to be found.
- (b) In the computerised control room, there are few elementary failures. Also, accidents due to elementary failures have seldom been observed in simulators, as most are recovered from by the operator, by another crewmember, or by a design feature. In addition, some of the elementary failures do not have any direct consequences in terms of safety. Therefore, since these elementary failures may not have any direct consequence on the success/failure of the human factor mission. HFM, a unit of analysis that is better and broader than elementary failure, was required to be defined for the purpose of HRA.
- (c) A good part of a crewmember's task is not written in the procedure. In performing a task, operators exchange information with each other, discuss decisions, or take initiatives that greatly affect operations. Moreover, some aspects are not covered in procedures. For example, there is no indication of time available for procedure execution, although time is one of the strongest influence factors impacting the outcome of a HFM. The management of time is entrusted mainly to the supervisor or safety engineer.

To incorporate the factors related to operations and failures in emergency conditions delineated above, together with the latest findings of human and behavioural science research, into the new HRA method, a multidisciplinary development team comprising both engineers and human factors experts was constituted and entrusted with the development.

### 3.9.3 Emergency Operation - A Different Point of View

A knowledge of accidents acquired from both real and simulated situations, led the MERMOS team to conclude the following.

- (i) Emergency operations, even those ending in failure, are to be viewed positively (as a learning experience).
- (ii) Operational activities are to be considered as a collective exercise.
- (iii) Both time and organisational factors are to be taken into account while explaining mission failures.

In modelling for 'MERMOS', the above aspects were considered in depth. The details are as given below.

- (a) Emergency operation, even if ending in failure, is to be viewed positively as a learning experience. Emergency operation at TMI ended in failure. Although operators at TMI had thought of the

possibility of such an accident many times, they disregarded such an eventuality for good reasons that the required actions would be carried out. However, if attention had been focused on good reasons why operators may not carry out the actions required to deal with the accident, then the eventuality of mission failure (arising out of possible deviations or erroneous behaviour) could have been envisaged. Thus, they would have been prepared for such an occurrence.

- (b) Operational activities are to be considered as a collective exercise.

In performing tasks, operators exchange information, discuss decisions made and generally work together as a team.

- (c) Both time and organisational factors are to be taken into account in explaining mission failures.

Emergency operations are to be evaluated against the 'required operations'. Required operations cover the requirements in respect of diagnosis, action, time-window (for diagnosis and action), etc. that are conditional upon the HFM and the state of the plant (at a given time and for a given amount of time).

Organisational problems can (and do) lead to accidents, but are often dealt with simply from the point of view of communications between the crewmembers. The organisation works out the distribution of tasks between humans and systems. On this static distribution of tasks is superimposed a dynamic one, with opportunities for crewmembers based on an informal organisation, generated by human activities in an emergency situation. It is important to assess the impact of organisational factors on the efficacy of emergency operations.

In conclusion, it can be stated that the operators (Man), the technical elements (Technology) and the organisational factors (Organisation) all act together in emergency operations. This aspect is taken into account by introducing the concept of modes of performance of human factor missions. Such an approach to operations can benefit from advances in the fields of cognitive psychology and organisational sciences.

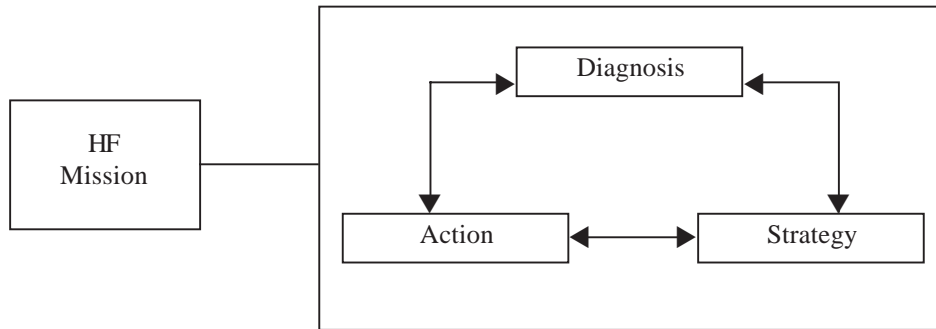
The work carried out by the development team led to the definition of the strategy - action - diagnosis (SAD) Model for MERMOS. The model incorporates the considerations detailed above in the explanatory scheme devised to explain failures of human factor missions.

### 3.9.4 Explanatory Scheme for Failures of Human Factor Missions

#### 3.9.4.1 The SAD Model

The SAD model has the following features.

- (i) The integration of organisational factors into the explanatory scheme leads to an alternative approach to the identification of failures, based on a search for difficulties in performing the required actions (including diagnosis) during an accident.
- (ii) The study of failures involves a search for conditions that could force the operator into faulty modes of functioning, i.e. conditions restricting the operators' response capabilities or conditions that are beyond his limited handling capabilities.
- (iii) Organisation adopted by a crew in a human-machine system depends not only on the limits of functioning of operators considered individually, but also the factors characterising the situation.
- (iv) The view of emergency operation considering the individual operator is replaced by the concept of the 'system in charge of the performing human factor missions'. An important development in MERMOS is the definition of this system, called emergency operation system (EOS), which includes crew, emergency operating procedures (EOPs) and human machine interface (HMI).
- (v) The strategy - action - diagnosis (SAD) model represents the functioning of the EOS. The three functions, strategy, action and diagnosis, all interact with each other, as shown in Figure 3.4.

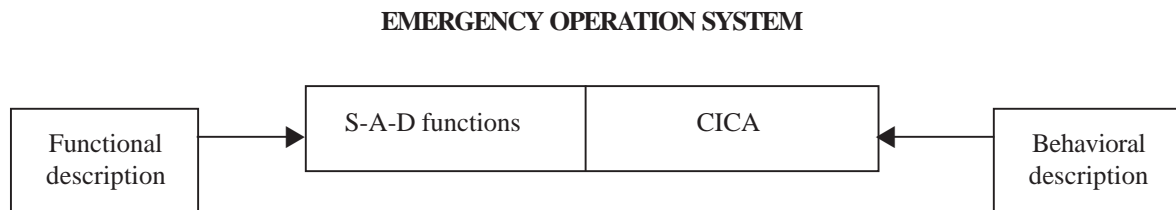


**FIGURE 3.4 : FUNCTIONAL DESCRIPTION OF EMERGENCY OPERATION SYSTEM (EOS)**

3.9.4.2 CICAs (Caracteristiques Importantes de la Conduite Accidentale) or Important Features for Emergency Operation.

The notion of CICAs is introduced to describe the functioning and (in particular) the evolving organisation of the EOS over time.

- (i) Organisation of EOS is considered in both static and dynamic configurations, as the arrangements and rearrangements occurring within the system during an accident are to be described.
- (ii) The EOS is organised in a way that enables collective or group functioning during operations. The phenomena of interest take place against the backdrop of the prescribed organisation, which can be described in terms of roles played and areas of responsibility.
- (iii) To express the dynamic behaviour of EOS, notions like ‘positioning’, ‘delegation’, ‘arrangements’ and the like are used.
- (iv) There are two descriptions of the functioning system, a functional description and a behavioral description as shown in Figure 3.5.



**FIGURE 3.5 : FUNCTIONAL AND BEHAVIOURAL DESCRIPTION OF EMERGENCY OPERATION SYSTEM**

3.9.5 Structured Qualitative Analysis Using the SAD Model

The SAD model structures the process for qualitative analysis of human factor missions. The outputs from qualitative analysis are used in quantification of failures in terms of probabilities. Qualitative analysis involves four steps.

- (i) Description of 'required operation' underlying the mission.
- (ii) Breakdown of 'required operation' in terms of S, A and D functions.
- (iii) Description of function failure in terms of non-compliance with the 'required operation'.
- (iv) Consideration of all conceivable scenarios connected with each failure mode and description of them in standard table format.

The last of the above four steps is the most difficult and requires a high level of expertise. Two complementary approaches are used to identify the knowledge necessary to carry out this step.

- (a) A deductive approach starting from the functional description.
- (b) An inductive approach starting from the knowledge of emergency situations and crew behaviour.

### 3.9.6 An illustrative example of qualitative analysis of a failure scenario using MERMOS from Le Bot et al [16].

#### Example

The example chosen is the PSA sequence initiated by a SGTR together with loss of SG feed water including auxiliary feed water system (AFS). The human factor mission that is to be studied is the completion of feed and bleed within the time window, after initiation of failures. The aim here is to describe the failure scenario given that the first three steps in the qualitative analysis have been completed.

#### Starting point

The failure scenario is developed from simulator tests, study of incidents that have occurred and assumed knowledge of the sequence. The classical description of this accident situation highlights the 'safety versus availability' conflict. In other words, operators know that the operation is irreversible and will damage the containment. Further, the AFS is a highly redundant system that is also readily accessible (outside the containment). The crew will attempt to repair the AFS knowing that its recovery avoids having to resort to feed and bleed. The concern here is how a failure can then occur.

#### Interpretation in functional requirement terms

Interpretation is effected in terms of strategy, action and diagnosis functions of the SAD Model.

Considering the first, the strategy is to give priority to the feed and bleed function. Failure occurs when this functional requirement is not met. The 'erroneous strategy' mode of failure is investigated.

The model indicates two possibilities for explaining an erroneous strategy.

- (a) Priority is given to an objective that is not a priority in terms of what is required or
- (b) Choice of resources is poorly made because of urgency.

#### Analysis for possibility 1

The competing objectives that go into the choice of feed and bleed as a strategy are as given below.

- (a) The starting point is the 'safety versus availability' conflict, which is generated by the crew's hope of recovering the situation by re-supplying the SGs after restoring at least one AFS pump.
- (b) From the operators' point of view, restoring AFS is felt to be an essential operational objective, for operators know that they can recover the situation. Therefore the objective of restoring AFS can rival the use of feed and bleed. This behaviour can be observed on a simulator (even if simulator conditions are not free from bias). The framework of the scenario then is as follows:

- Faulty Function - Strategy
- Failure Mode - Erroneous strategy
- Safety Requirement - Priority to feed and bleed
- Possible Bias - Priority to recovery of AFS

**TABLE 3.13 : QUALITATIVE ANALYSIS TABLE - REPRODUCED FROM [16]**

Function	Failure Mode	Safety Requirement	Possible Bias	Scenario	CICAs	Situation
Strategy	Wrong strategy	Priority is to be given to feed and bleed	Priority is given to the recovery of AFS	Scenario 1. The crew hopes for AFS recovery in time and puts off the completion of feed and bleed too long	Suspension of feed and bleed  Carrying on with the AFS recovery actions	Information from the crew leads the crew to believe _ _  The supervisor is deeply involved in recovery actions
			Priority is given to operating the radioactive SG	Scenario 2	---	---
	No Strategy	---	---	Scenario 3	---	---
Action	---	---	---	---	---	---
---	---	---	---	---	---	---

**Scenario**

To begin with, the location of failure is precisely defined. The crew gives priority to AFS recovery and the crew’s attention is devoted to this. But the crew is aware that feed and bleed will be needed in the end. Since failure of strategy is envisaged, it is not necessary to introduce an additional system failure, say by way of diagnosis failure. The crew attempts the risky exercise of transition to feed and bleed ‘at the last moment’ when time has run out. The failure therefore will be of available time (i.e. time for carrying out the mission will be exceeded). The scenario can therefore be described as: Hoping to be able to recover the AFS in time, the crew puts off transition to feed and bleed too long.

**CICAs**

The failure is determined to be that of time allowed for performing the mission being exceeded. It has therefore to be explained how a proper organisation of operation can lead to the failure. Strategically, the crew delays transition to feed and bleed ‘intentionally’ without questioning its necessity. In other words, the crew ‘suspends’ this operation. This is the first CICA.

The crew’s thinking is that there is always hope of recovering AFS and that is what is actively pursued, ‘come what may’. The second CICA is this orientation of operations, denoted as ‘Carrying on with AFS recovery operations’.

**Situation**

In the final step, it is to be explained what factors of the situation, resulting from a combination of context and features of the mission lead the crew onto this path.

As already delineated, crew must be convinced that recovery is possible to the point of risking delaying going to feed and bleed. The recovery must be seen as possible in the short term. In addition, no operation, which is initiated must result in negative feedback in the control room, if the operators have followed the chosen path thus far.

In addition, the specific attitudes of the two members of the crew (i.e. supervisor and safety engineer) who have to check what the others do, have to be examined. The conditions, which led them to agree to and follow (if not lead) this operational approach, are to be determined.

- (i) For the supervisor, tests show that his organisational role as the person in charge of recovery, will involve him deeply in the operations, which in this particular case concerns the auxiliary feedwater system, a highly redundant system outside the containment, which is readily accessible, and with which the operators are familiar.
- (ii) The safety engineer, it is seen, has to comply with the crew's strategy. This is something that has been observed on simulators, even if it did not progress to a failure.

The scenario is now clearly delineated. Each constituent element will be assigned a probability derived from simulator data, handbook data or expert judgement data. The product of all the probabilities will be the probability of occurrence of the event scenario. The probability of mission failure will be the product of the probabilities of the described scenarios. A residual probability corresponding to 'inconceivable scenarios' is used as the lowest value. If qualitative analysis has not been completed, the analyst has to use a conservative probability value.

### 3.9.7 Summary and Observations on MERMOS

- (a) Four major steps are involved in MERMOS. These are as follows.
  - (i) Identifying the safety functions that are affected, the possible functional responses and the associated objectives. Determining whether specific means are to be used to maintain/restore safety.
  - (ii) Breakdown of the safety requirements and the corresponding HFM into strategy, action and diagnosis functions.
  - (iii) Bridging the gap between theoretical concepts and real data by creating as many failure scenarios as possible.
  - (iv) Checking for consistency of results and incorporating them into PSA event trees.
- (b) Contributions of the method
  - (i) Unlike models in previous methods, MERMOS avoids considering operators as a source of errors and safety engineers as a recovery factor.
  - (ii) A realistic characterisation of the failure of missions is employed. MERMOS analyses take into account a broad range of failure causes. The elucidation of failure scenarios qualitatively enriches the human reliability analysis, as implied or not so obvious elements of knowledge of emergency operation can be taken into account.
  - (iii) With the notion of 'required operation' the norm of failure is defined with respect to what is required functionally and not with respect to what is prescribed by the procedures. Instead of focusing on the errors made in the application of procedures, the analysis concentrates on the effective result of any operations consistent with procedures.
  - (iv) The systemic approach in MERMOS considers operation as a whole. This makes it possible to restrict the consideration of individual operation errors to elements of a situation which cannot account on their own for the failure, considering the recoveries by crew, the procedures or the interface.



- (v) In using MERMOS, a deeper knowledge of operation is achieved. MERMOS requires an in-depth functional analysis (i.e. functional objective of mission, criteria for success, time period within which the mission is required to be carried out and the situations wherein the mission is considered as necessary by the procedures). This knowledge of operation can be very useful, e.g. for improvement of procedures.
- (c) Limitations and constraints of the method
- The method demands detailed qualitative analysis using a formalised structure. Applying the method logically requires good knowledge about emergency operation and HRA. A certain level of expertise in prescribed and actual (or simulated) emergency or normal operation ensures the validity of the analysis. However, demanding too much expertise may limit the extent to which the method is used for HRA studies. At the same time an HRA study carried out by an inexperienced analyst would compromise the validity of the results. Faults can occur due to a lack of homogeneity in reliability quantification of human factor missions.
- (d) Areas of development
- (i) Although a good deal of work has been done following the development of the method in 1998, the method needs to be made user friendly to HRA analysts by extending the database of analyses of standard human factor missions.
  - (ii) Accessible sources of experience feedback data on MERMOS would foster the use of the method.
  - (iii) The feasibility of taking into account the organisational elements, through their impact on situational factors and their probability, is to be explored. Also, the impact of an organisational change on safety of post-emergency operation is to be studied.

### **3.10 Guidance on Selection and Use of Human Reliability Assessment Methods**

Human reliability is considered to be quite important from a risk assessment and risk management perspective. Hence, there are high expectations in respect of the potential benefits of integrating HRA into PSA studies. However, in spite of the large number of applications of HRA in the last two decades, there is neither a HRA methodology, nor a human reliability database that has been generally agreed upon. HRA methods are still being refined and developed. Despite attempts to structure and standardise the human reliability analysis, there continues to be marked variability in the assessments of human reliability contribution to plant safety.

As HRA is characterised by a number of different technical approaches with limited support data, it becomes necessary to apply expert judgement in the selection of the most appropriate technical approach and furthermore, to apply expert judgement in deriving the necessary data. Only then can useful results be obtained from the qualitative and quantitative analyses. On completing an application, it is also normal to gather insights from the results. This is again done, by applying expert judgement and knowledge of human factors and systems engineering to the case being studied.

In the absence of a fully verified, validated and agreed upon approach to HRA, it is required to apply a 'compromise' approach on the basis of techniques available. However, while doing so it is necessary to be aware of the limitations of the HRA method. Problems can arise if there are misconceptions about the validity of the HRA quantification method, resources needed for applying structured expert judgement and documenting the HRA, the degree of qualitative and quantitative analysis provided and level of integration necessary with respect to PSA tasks.

These misconceptions can affect an assessment in different ways, e.g. through misapplications of known HRA techniques, through inadequate attention to the analysis of potentially significant human errors or through under-estimation of the level of effort needed to complete an analysis. In the extreme case, a quantification technique could be applied to a situation, which is completely outside its range of validity.

Whatever be the choice of quantification technique, the analyst is required to apply a certain degree of judgement, and this implies that the final analysis will invariably include subjective considerations.

### 3.10.1 Frequently Used HRA Techniques - Salient Observations

The most frequently used HRA methods for PSAs are THERP/ASEP, HCR and expert elicitation (SLIM-MAUD).

#### (a) THERP and ASEP HRA procedure

THERP is the most widely used technique and contains basic human performance models and underlying procedures for task analysis and developing HRA event trees. THERP allows the assessment of both pre-accident and post-accident operator actions. The THERP Handbook offers a large database of HEPs and details models for considering the effects of PSFs like stress and personnel redundancy. In this method each operator is considered to have the same failure probability in executing a specified task, and only dependencies between two tasks are considered. Handbook data is sufficient for treating execution errors in 'skill' and 'rule' based behaviour. The method does not model psychological causes of errors and has drawbacks in treating the dependencies among PSFs appropriately. The diagnostic models presented in the Handbook are based on expert judgement. The method gives realistic estimates of HEPs and response time and other human performance characteristics. THERP has been widely accepted and the methodology has been used in a very large number of PSAs published.

The ASEP method is a short version of the THERP Handbook. ASEP offers a step-by-step procedure to assess operator tasks. There is a detailed screening procedure provided for pre and post-accident screening. ASEP provides additional specific guidance on assessment of stress in accident sequences. In comparison to THERP, the ASEP HRA procedure produces more conservative estimates of HEPs and response time and other human performance characteristics.

#### (b) Human cognitive reliability (HCR) model

The HCR model, which is an empirical model based on data collected from simulators, has been developed for the estimation of non-response probability of an operating crew. The approach is well suited for the assessment of diagnosis and decision making tasks in time-constrained emergency situations. By inputting crew behaviour and performance characteristics to a mathematical correlation, a quantitative result in the form of a non-response probability is obtained.

A major assumption in using the HCR is that the cognitive behaviour of the crew can be exactly classified into one of three types. However, benchmark studies show that crew responses do not always fall into any one of three behaviour types. Another assumption is that PSFs affect only the non-response time and are independent of each other. This too may not be true. Under a high level of stress, the operator, not being able to recall the previously stored rules from memory, may go from rule based behaviour to knowledge based behaviour.

There is some possibility of misapplying the HCR model for reasons of ease of use and small amount of expert judgement required. The HCR, like all TRCs, has its area of implied and unproven validity. The analyst has to determine what the range of validity is and to ensure that the application and results are consistent and justifiable.

The numerical accuracy and consistency of the time correlations used in the HCR model for skill, rule and knowledge based behaviour are not adequately determined. In particular, probabilities lower than 0.01 are difficult to validate. However, HCR is one of the few HRA methods, which is based on (simulator) data and not on expert judgement alone.

(c) Expert judgement methods.

Direct numerical estimation (DNE) has the advantages of ease of use, the wide range of situations (for pre-accident and post-accident tasks and skill, rule and knowledge based behaviour), which can be considered and applicability in circumstances where misdiagnosis has worsened a situation. However, using DNE as an HRA model is time intensive and requires experts who are familiar with both HRA and the area of interest. DNE has moderate applicability.

Paired comparison (PC) Technique can be used to assess all types of operator actions. The validity depends on the knowledge of the experts who compare pairs of tasks and decide which of the two in a pair has a higher likelihood of error. Two or more tasks with well known error probabilities are used to calibrate the scaling. But, as it is sometimes difficult to find suitable calibration data, the PC method is relatively subjective. The PC technique is easy to use, and normally experts do not require extensive training. The method is quite well established and has been applied in some PSA studies.

Success likelihood index method (SLIM) is based on the premise that HEPs depend on the combined effects of the PSFs. Hence; several influence factors (typically excellence of design, meaningfulness of procedures, stress, time pressure, complexity of task, quality of teamwork and seriousness of consequences) can be taken into account. Most methods make the assumption that PSFs are independent of each other. This may not be strictly true. For example, the effects of a lack of supervision and a lack of training are likely to be greater when they occur in combination, than when they occur independent of each other. SLIM allows for taking this effect into account in an analysis.

SLIM does not require extensive decomposition of a task to an elemental level. Since it involves only the subjective evaluation of expert opinion, it is flexible and can be applied to a broad range of analyses.

SLIM also provides sensitivity analyses to identify weak points in plant design, ergonomics and procedures. Uncertainty bounds cannot be obtained with SLIM and have to be derived using other methods.

Application of SLIM requires reference tasks with known probabilities for calibration. In some cases, these are difficult to obtain, and analysts then have to resort to estimations. When elicitation of expert judgement is to be carried out using the SLIM-MAUD programme, analysts will need training before they can use it in an effective manner.

Issues in SLIM are the variability of experts and inappropriate treatment of the time available for a task. Further the sensitivity involved in withdrawing or including a task from the group of selected tasks is not inconsiderable. The time available for a task is not appropriately treated in SLIM.

SLIM has a high degree of acceptability. It has been used in several PSAs and also in the course of the ISPRA Human Factors Benchmark Exercise.

### 3.10.2 Selecting a HRA Method

#### 3.10.2.1 Formal Process

A formal process of selection of an HRA method should necessarily involve a number of factors. These include the following.

- (a) Usefulness/Completeness
  - (i) Types of operator behaviour that can be assessed
  - (ii) Types of operator tasks that can be assessed
  - (iii) Whether both qualitative and quantitative results are provided.

- (iv) Whether the method can provide insights for recommendations to be made.
- (b) Ease of application
  - (i) Requirement of special training of analyst
  - (ii) Equipment and time necessary
  - (iii) Requirement of data.
- (c) Recognition and acceptability
  - (i) Frequency of use.
- (d) Accuracy and validity
  - (i) Accuracy
  - (ii) Validity.
- (e) Reliability/Ease of sensitivity analysis

The capability to quantify human reliability varies considerably among the many methods, correlations or concepts available to analysts. Some of the currently used methods were specifically developed to address a particular aspect of human reliability and so are limited in their capability to address other aspects. For example, HCR was developed for the evaluation of non-response probability in a time constrained environment.

To make the best use of the analytical capabilities of the human reliability discipline, it is therefore a good practice to selectively employ a set of different models for quantification after having fully understood their capabilities and limitations.

### 3.10.2.2 Observations on THERP, ASEP, HCR and SLIM

Some observations on THERP, ASEP, HCR and SLIM, with respect the factors delineated above are presented below.

- (a) With regard to the 'usefulness/completeness' factor

THERP is useful to a high degree. Skill-based and rule-based errors are treated. It contains basic human performance models and procedures for task analysis and development of HRA event tree models. Guidance for modifying handbook data for different situations is provided. It treats several important PSFs and also dependencies and RFs. One drawback is that it is not appropriate for errors involving complex diagnosis/high level decision tasks. ASEP, a shortened version of THERP, has a detailed screening procedure for pre and post accident tasks. It is widely used as a method for HRA in PSAs, with detailed THERP analysis being carried out when necessary only for dominant sequences with operator errors. HCR is well suited for integral assessment of tasks (involving diagnosis and decision making) and is therefore quite useful. SLIM is very useful for situations where little or no data is available as it can be used to estimate human reliability on the basis of expert judgement. SLIM can be used for carrying out sensitivity analysis to identify the weak points in a situation.

- (b) With regard to the 'ease of application' factor

With THERP, the integration of HRA and equipment reliability analysis is straight-forward and so easily understood by system analysts. ASEP like THERP is well documented and therefore easy to apply. THERP HRA requires a considerable amount of time, but an ASEP HRA takes much less. THERP is associated with a large set of data, which can also be used with ASEP. Application of HCR is straightforward, and so there is some possibility of mis-application. It is a method, which is based on simulator data. SLIM can be applied without decomposing a task to an elemental level. The domain experts may have to be given training in HRA. With SLIM, there is also a need for HEP calibration data.

- (c) With regard to the 'recognition and acceptability' factor

THERP and ASEP are used in a majority of HRAs and have a high degree of recognition and acceptability. While HCR is frequently used, its applicability to all kinds of situations is not verified. SLIM is accepted widely as an expert judgement method and has been applied in many HRAs for PSAs.

- (d) With regard to the 'accuracy and validity' factor

THERP gives realistic estimates of HEPs, response and other human performance characteristics. ASEP estimates are more conservative. In THERP, as detailed analysis is carried out, the accuracy is greater. THERP models are based on expert judgement, as are models in ASEP, which is a version of THERP. So their validity is based largely on experience and judgement. The HCR curves are produced from simulator experiments and so their validity can be verified to a degree, which depends on the extent the simulator environment is actually representative of the real plant. SLIM, particularly when a group of experts exercise their judgement, produces quite accurate estimates.

- (e) With regard to the 'reliability/ease of sensitivity analysis' factor

All four HRA methods, THERP, ASEP, HCR and SLIM, are reliable when used as specified, taking into consideration their capabilities and limitations.

The principal limitations of HRA generally considered are those of HEP data and validation. There is a good amount of data from various kinds of human factors situations, but their applicability is open to question. They provide guidance on the relative importance of PSFs but need to be supplemented by information from other sources. The quantity and quality of field data are relatively low. Those data that do exist are predominantly for slips rather than mistakes or violations. Other sources of data are expert judgement and simulators.

Studies on the validation of HRA methods are few in number. Four kinds of validity were considered by study group on human factors of Advisory Committee on Safety of Nuclear Installations (ACSNI); constituted by Nuclear Energy Agency of Organisation for Economic Cooperation and Development (OECD). They were predictive validity, convergent validity, content validity and construct validity. Essentially for prediction of a given analysis, predictive validity is concerned with agreement with the real situation, convergent validity is concerned with agreement with the predictions of other analyses, content validity is concerned with agreement between model elements and critical real life features and construct validity is concerned with agreement between structure of the model and that of the real life situation.

### 3.10.2.3 Types of Human Interactions and Selection of HRA Models

It is observed from the above, that HRA methods have their own strengths and weaknesses. These have to be considered together with data availability and types of human interactions involved in the HRA study. In general, the model/method selected for human reliability quantification strongly depends on data availability and types of human interactions for which HRA is to be carried out.

- (i) For Type 1 (maintenance and test) interactions involving errors that degrade system availability, THERP and ASEP pre-accident HRA procedure are most suited. If the HRA study has to be completed in a short time, ASEP pre-accident HRA procedure may be used, although the estimates would be less accurate.
- (ii) Type 2 (accident initiating) interactions are quantified using operating experience data or expert judgement data.
- (iii) For Type 3 (procedure following including decision making) interactions, THERP, ASEP post-accident HRA procedure, HCR or SLIM is applied on the basis of the specific requirements of the HRA study. The essential considerations involved in selection of the HRA method are as follows.

- (a) The operating crew has to first recognise (detect) that an incident/event has occurred, identify (diagnose) the event, the causes and types of equipment failures, decide on the series of actions and then perform the actions within the time necessary to prevent core damage. Human failures at any stage would lead to overall system failure.
  - (b) For each of the postulated initiating events, there is an emergency operating procedure to be followed and its associated HEP is required by the PSA.
  - (c) There are three possibilities for operator response, viz., correct response, no response and wrong response. If the possibilities of wrong response are very low because of compelling and diverse cues or if their consequences are not more severe than those for no action, then the basic detection, diagnosis and decision tree may be merged into a single 'cognitive' node. Cognition is followed by action. Cognition and action stages have to be completed within a given period of time after event initiation.
  - (d) Depending on the definition of the cognitive node, non-response probability can represent all three failure possibilities, viz., wrong diagnosis, wrong action, and non-response. For quantification of non-response, inclusive of wrong response, the HCR model may be used. This integral time model can treat overall non-response probability. The operator's task is not broken down into steps. Cognitive processes are recognised but the analyst must be experienced enough to identify the task as skill based, rule based or knowledge based. Three performance shaping factors are considered but it needs to be confirmed that the PSFs only influence non-response time. The method provides only an approximate image of the reality prevalent in the system as no task analysis is done. Aspects like complexity of the situation and number of work functions to be performed are not considered adequately.
  - (e) If non-response does not include wrong diagnosis and wrong action, their probabilities can be evaluated using THERP, ASEP or SLIM.
  - (f) Identifying cases where detection, diagnosis, and decision cannot be coalesced is the key to identification of potential problem areas in the HIs, e.g. a case where there is potential for alternate strategies for coping with the event by the crew. In these cases the plant information system and functional procedures become very important PSFs helping crew to monitor and control plant to a safe state.
  - (g) Even if the cognitive mode can be coalesced, there are conditions for which the HCR model is not applicable, particularly in the extended time frame when additional personnel will augment the crew and shift changes take place. An expert judgement method may be used in this case.
- (iv) Type 4 (Accident Aggravation): Responses are made in the belief they mitigate the consequences of the accident, but actually exacerbate the situation. For example, operators may concentrate on diagnosis or recovery of failed equipment to the exclusion of developing an alternative strategy to control core conditions, and carry this to a level where the alternative becomes unavailable. Some guidelines for handling Type 4 interactions in HRA are given below.
- (a) Type 4 can be viewed as a subset of errors in Type 3 and Type 5 HIs, which cause operators to take wrong actions as a result of misdiagnosis of the situation. The failure to diagnose branch includes this. Misdiagnosis occurs in cases where operators' mental image of the plant differs from actual and so operators perform actions appropriate to wrong plant state or fail to take correct actions. Hardly any data is available for predicting this type of HIs, but retrospective analysis of actions during actual events can identify such HIs.
  - (b) In many cases that have occurred there have been recoveries from these initial

misdiagnoses. In PSA, an interaction is Type 4 only if it is non-recoverable prior to core damage. If it is recoverable, the event tree can show follow on recovery.

- (c) Quantification of Type 4 HIs is performed by use of THERP, HCR or SLIM or a combination of these models.
- (v) Type 5 (Recovery Improvisation): Recovery actions are included in the accident sequences. Actions involve recovery of failed equipment, use of alternative equipment to fulfill the needed functions or use of non-standard procedures to ameliorate the accident conditions. Some guidelines for handling Type 5 interactions in HRA are given below.
  - (a) Probability of failure to perform recovery action is included as a non-recovery probability for each group of failures represented by a minimal cutset in a specific accident sequence, for which the recovery action is applicable.
  - (b) For quantification, one may employ direct estimation based on expert judgement or a time correlation between performance and requirement. HCR is useful in some cases (e.g. for recovery following failure of an auto start system, which may be considered as a Type 3 action instead of a Type 5 action).
  - (c) Recovery actions in the control room are significantly influenced by availability of operator support systems like safety parameter display system (SPDS) and also the availability of safety function oriented procedures.

### 3.11 Further Needs in HRA [21]

Improvements to HRA are being made in a number of areas. In addition to the development of second-generation HRA methods, these include the development of models for human errors that occur in accident management, low power and shutdown operations and external events.

In our context, PSA applications have until now generally dealt with normal aspects, e.g. full power operation state, conservative assumptions in respect of success/failure criteria and a quasi-static treatment of plant response and human behaviour. Currently, PSAs are carried out for:

- (i) Non-full power conditions (including low power and shutdown)
- (ii) Level - 2 PSA
- (iii) Accident management (AM) situations
- (iv) External events (fires, floods, earthquakes)

The nature of human operations under these conditions differs from that in full power operations. There are aspects of importance in the analyses that are often not modelled explicitly in full-power PSAs currently being conducted. These include actions outside the control room, coordination and communication within and between teams, actions without procedures and decision burden.

Factors significant to further development of HRA are given below.

Ex - control room actions

- (1) Delivery of instructions to field operators
- (2) Movement to access controls
- (3) Availability of local feedback indications
- (4) Need for data on plant layout, quality of labelling and tagging, communication practices, and feedback indications.

Communication and coordination (within and between teams)

- (1) In shutdown/accident management situations more number of persons are involved, who make decisions at various levels. Important factors are coordination and control, possibility of conflicts and unforeseen consequences of actions, a possible lack of written procedures, and possibility of obstacles to availability/flow of information from/to the person(s) in the plant to the person(s) in the remote location. HRA has to consider and model group-coordinated behaviour.
- (2) Communication procedures, protocols and equipment are to be considered in HRA.
- (3) Data related to failure of crew coordination and communication, failure of delivery of command and/or information between control room and field.

#### Actions without procedures

- (1) The number of configurations that are possible in shutdown/accident management (AM) situations are too many and uncertainty about plant configuration can lead to error.
- (2) When written procedures are not available, operators have to depend on their knowledge and training. Mistakes are possible in considering the potential consequences of planned response.
- (3) The lack of procedures may bring out unconstrained possibilities of plant state as a result of performing actions in situations not recognised or situations misinterpreted from the instrument readings.
- (4) There could be a change or changes of persons executing a job.
- (5) To improvise recovery actions, unambiguous data that indicate the actual plant state are required.

#### Decision burden

Arises in situations when operators have to consider the consequences of actions required in a 'real' situation. When there are uncertainties about the plant state (appearance of unexpected alarms/parameter indications), or when actions (foreseen and/or addressed in operating procedures) are not in accordance with plant safety vis-à-vis the real situation, probability-consequence tradeoffs between two or more actions are involved, and this results in decision burden. HEPs then would be related to chances of recovery.

The approach to human reliability analysis and quantification would in general follow the pattern of the HRA methods adopted for full power PSA. Usually, the risk in events associated with non-full power PSAs is somewhat higher. And, there is evidently a need, to explicitly consider in HRA, the important factors discussed above. The second-generation HRA approaches have features that are useful in incorporating the factors of concern into HRA, and so may be explored for application in HRA for PSAs that are currently being planned.



## 4. DATA FOR HUMAN RELIABILITY ANALYSIS

### 4.1 Types, Uses and Sources of Data

#### 4.1.1 Types of Data

Two major types of data can be collected for HRA, qualitative and quantitative. Qualitative data is useful for error reduction based on human factors and operating experience data. Quantitative HRA data can be in relative form (e.g. probability of error X is 2 times the probability of error Y) or in absolute form (e.g. the probability of error X is 0.001). Both types of data (qualitative and quantitative) are required in HRA, but there is a great need for quantitative data in the form of HEPs for use in PSAs. The HEP data can be used directly for human error quantification (if sufficient data exists) or in the validation of human error quantification techniques. Qualitative data can be collected simultaneously with quantitative data. Qualitative data on error mechanisms and PSFs characterise HEP and aid in the determination of the range of applicability of HEP data to various scenarios in PSA.

#### 4.1.2 Uses and Sources of Qualitative Data

The uses and sources of qualitative data are given in Table 4.1.

**TABLE 4.1 : USES AND SOURCES OF QUALITATIVE DATA**

Users of Data	Uses of Data	Sources of Data
Plants	<ul style="list-style-type: none"> <li>- Understanding plant events, developing plant specific error reduction measures.</li> <li>- Improvement of work organisation and operating crew performance.</li> <li>- Providing supporting evidence for the validation of HRA methods.</li> <li>- Development and/or improvement of the safety management system and quality assurance</li> </ul>	<ul style="list-style-type: none"> <li>- Event reports</li> <li>- Near miss or precursor event reports</li> <li>- Records of violations</li> <li>- Maintenance reports</li> <li>- Log books</li> <li>- Simulators</li> <li>- Plant specific information</li> </ul>
HRA research	<ul style="list-style-type: none"> <li>- Examining and understanding the root causes and human error mechanisms for purposes of modelling and evaluation of human performance (this can lead to detailed error reduction strategies).</li> </ul>	<ul style="list-style-type: none"> <li>- Generic data for HRA modelling</li> <li>- Simulations</li> </ul>
Regulatory bodies and government agencies	<ul style="list-style-type: none"> <li>- Monitoring safety in operations</li> </ul>	<ul style="list-style-type: none"> <li>- Data from plant event reports</li> <li>- Other reports</li> </ul>

#### 4.1.3 Sources of Quantitative Data

There are three possible sources from which data suitable for the generation of HEPs can be collected. These are: (1) Data from relevant operating experience, (2) Data from experimental research and (3) Data from simulator studies. The ideal case would be where all required data is available from relevant operating experience or realistic experiments. However, in practice, not enough data have been collected from such sources and therefore, sources such as expert judgement have to be used to generate data.

### 4.2 Generic and Specific Data

Generic data are data derived using expert judgement. They are data that are applicable to a whole range

or class of tasks and therefore provide acceptable guidelines for quantitative analysis. The data are usually given for generic task descriptions such as ‘very simple task performed quickly’, ‘simple task requiring little attention’, ‘complex task requiring a high level of concentration and skill’ and so on. A table of typical generic guideline data drawn from Kirwan [13] is given in Table 4.2.

**TABLE 4.2 : GENERIC GUIDELINE DATA [13]**

	<b>Description</b>	<b>HEP</b>
1	General error rate in very high stress level situations	0.3
2	Complex non-routine task in stress situations	0.3
3	Supervisor does not recognise operator’s error	0.1
4	Non-routine operation simultaneous with other duties	0.1
5	Operator fails to act correctly in the first 30 minutes of a stressful emergency situation	0.1
6	Errors made in carrying out simple arithmetic with self-checking	0.03
7	General error rate for oral communication	0.03
8	General error of omission	0.01
9	Error in routine operation requiring care	0.01
10	Operator fails to act correctly after the first few hours in a high stress scenario	0.01
11	Operator fails to return a manually operated valve to the correct position after maintenance	0.01
12	Omission of an action step in a procedure	0.003
13	General error rate for an action performed incorrectly	0.003
14	Error in simple routine action	0.001
15	Selection of wrong switch (dissimilar in shape)	0.001
16	Selection of a key-operated switch, rather than a non-key operated switch (error of commission)	0.0001
17	Limit of human performance for a single operator	0.0001
18	Limit of human performance for team of operators performing a well-designed task, with very good PSFs	0.00001

Specific data is data that is applicable to a particular task, which is often restricted to a specific industry/plant. Data for specific task descriptions in a plant (e.g. ‘error of selection in changing or restoring the state of locally operated valve, when the valve that is to be manipulated is clearly and unambiguously labelled’) is considered to be plant specific data. It is possible to develop both industry specific and plant specific databases.

#### **4.3 Data from Plant Operating Experience**

Analysis of plant operating experience, yields a good amount of valuable qualitative data, but collecting quantitative data on human reliability in the form of HEPs is difficult. Operating experience data collection systems in general have a number of limitations. Taylor-Adams [27] gives a good account of these limitations.

- (i) Human errors that do not lead to any violation of technical specifications are unlikely to be reported, although set limits of acceptability with respect to the human errors may be transgressed. This can result in a database that is incomplete.
- (ii) Human errors that are recovered from immediately, especially errors recovered by the committer himself, do not get included in the database.

- (iii) Information on low probability errors, or errors which occur in low probability event scenarios is generally not sufficient. Not many events would be found in a data search to yield statistically significant data. Hence, one has to take recourse to simulators or expert judgement.
- (iv) Error reduction can rarely be based on information on root causes of errors (e.g. inadequate procedure, poor work environment, ambiguous information feedback) because usually only the consequences/observable manifestations of error, called external eError mechanisms (EEMs), are reported, e.g. valve left open after test. Different causes can give rise to the same observable consequence. For prediction of possible error in an event sequence, it is important to understand the origins of an error. It is necessary to understand the error in terms of operator functions, as well as the actual PSFs involved. Otherwise, errors, which are only externally similar may be aggregated and the error reduction measures that are taken may be insufficient or even ineffective.

The above technical difficulties imply that the HEPs derived may involve a degree of uncertainty in their accuracy, which is in addition to uncertainty attributed to the data generation process, involving among others, factors like the number of observed events.

#### **4.4 Data Collection Systems**

Operating plants have in general a system of mandatory reporting of events with actual or potentially serious consequences, to regulatory bodies. Human performance problems delineated in such reports become a source of data. While the level of reporting is variable, it is still possible to derive useful information from event reports.

Data collection systems using Licensee Event Reports (LERs) or plant event reports were first developed in USA and tried to overcome some of the difficulties in deriving HEPs. The LER database however, generally gives almost no information on the PSFs in an event. So the usefulness of the database is limited. Some innovative schemes to collect information on a voluntary basis have been developed. One such scheme is Human Performance Evaluation System (HPES), a structured data collection system introduced by Institute of Nuclear Power Operations (INPO) of USA. In the INPO scheme, the consistency in data collected is achieved by the use of standard forms. Voluntary reporting schemes have the potential to significantly improve qualitative data on human error and recovery. Another example of such a scheme is IAEA's Incident Reporting Scheme (IRS).

#### **4.5 Human Error Probability Data**

The general definition of Human Error Probability (HEP) is the ratio of the number of observed errors to the total number of chances for error to occur. In other words, it is equal to the ratio of number of errors that occurred to the number of opportunities for the error.

This has been the major, if not sole form of human error data in PSAs. For generation of a HEP database, human performance reliability is to be evaluated for different kinds of human errors (e.g. operator turns a valve in the wrong direction or operator omits a step in a procedure). Both the number of times the error is made and the number of opportunities for the error are required to be obtained to evaluate HEP. Human error probability data derived in this manner have a number of limitations [27]. These are as follows.

- (i) Specificity of data - Data from a particular plant is to a significant degree specific to that plant. There can be large variations between plants in respect of operation, procedures, training practices, design ergonomics and safety management culture. But, in PSAs, HEP data from a specific plant are likely to be applied to a different type of plant in an unselective manner. The differences in HEP values however, being relatively small in PSA terms, may not result in a significantly erroneous prediction for either plant, given the uncertainty already inherent to the PSA process.
- (ii) Usefulness of data for error reduction - In PSA, it may be found that that the plant does not

meet the risk criteria due to human error impact. But data in the form of HEP does not give information on how to improve human reliability. In fact the best way would be to make use of the factors that influence human performance (e.g. quality of the human-machine interface, extent of training) instead of resorting to other means like interlocks or additional safety systems. HEPs per se are not useful in indicating means of error reduction.

- (iii) Purely quantitative form of data - The data unless qualified gives only the observable manifestation of error, i.e. External Error Mode (EEM). An operator could have turned a valve in the wrong direction due to a slip or because of his previous experience in other plants where the valves are to be turned in the other direction, in which case the error is a population stereotype error. The associated HEP could thus be significantly different. In other words, the EEM is the same, but the root cause or Psychological Error Mechanism (PEM) is different in the two cases. There are two implications of this.
  - (a) If data is generated in the form of EEMs alone, then the application of such data in PSA may lead to inaccurate results, because of the existence in the plant scenario of PEMs, not accounted in the data used. Therefore data from a database may be inaccurately applied.
  - (b) Though PSFs may be used to reduce the impact of human error, this may not be as effective a strategy as eliminating the root cause. The changes suggested for improving PSFs, may in certain situations, even go against the most appropriate measure suggested for elimination of root cause, e.g. more training in procedures might be provided in a case where the root cause of the problem is taking shortcuts (skipping steps) due to 'overlearning'. Therefore the data available may not be useful for effective error reduction.

#### **4.6 Data Collection in Indian Nuclear Power Plants**

The systematic collection, classification, recording and analysis of human error and human reliability data are crucial activities for PSA. A readily accessible source of human reliability (human error probability) data that is applicable in the context of Indian Nuclear Power Plants is needed. Data from published literature serves as a generic database for HRA. An example of such a database is the data in the Handbook of Swain and Guttman [25]. In addition to generic databases, there is a need to have plant specific data, which is based on operating experience in Indian NPPs. Such data will be relevant to HRA/PSAs of Indian NPPs.

##### **4.6.1 Using Event Reports as a Source of Human Error/Human Reliability Data**

In Indian Nuclear Power Plants, all plant events are reported in the form of incident reports. An event reporting form is also completed for each event with the event categorised into the appropriate level in the International Nuclear Event Scale (INES).

While event reports are useful for a general identification of the source of the problem, they may be limited by the fact that the details of the actual internal process by which a human error occurred may not be recorded. In studying event reports pertaining to human error events, one may not come to know all the observations that were made by the operating crew, or the alternative courses of action that were considered, prior to the erroneous action.

To study a human error in depth, a substantial amount of information on the processes that lead to the error is needed. The information should preferably include time tagged records of displayed and/or monitored variables and human actions. The root cause analysis reports, prepared for all significant events, are a good source of such information.

To aid the interpretation of this objective data, additional subjective data (e.g. the skill and training of the operator, number of times the same task has been carried out earlier) will also be required. Discussions and interviews with plant personnel can aid the acquisition of this kind of information. In general, a

plant event report may not contain such information.

The practical problems with plant event reports as a source of data can be summarised as follows.

- (i) Reports contain varying amounts of data. While in some reports data is clear and detailed, in others it is not.
- (ii) Reports are usually not prepared for near-miss events or adverse trends (accident precursors). Reports are made only for events, which occurred. Errors made, but immediately recovered from, do not get reported.
- (iii) Reports may at times only describe the events, but not give information on the causal aspects, i.e. the how and why of the events may not be given.
- (iv) Reports in general may refrain from mentioning any inadequacy in human performance and may tend to withhold such information for fear of reprisal.
- (v) Reports may at times not contain a true account of the error as it actually occurred, because of a possible attempt to rationalise the error and/or assign responsibility.
- (vi) There is in general no data available in respect of very infrequent events like design basis events/accidents (DBEs/DBAs).

#### 4.6.2 HRA Data Collection Problems

To generate quantitative data for HRA, it is necessary to estimate the number of opportunities for error, in addition to gathering information on the number of times a given human error has occurred. From plant data, the opportunity for error can be estimated for regular or periodic tasks. For other tasks, it may be difficult, and one has to resort to a simulator for collecting data.

The possibility of collecting and analysing data on operator response to infrequent events such as DBEs, is rather small, if one depends on plant data. Simulators are good tools to make use of in such situations, but there is a need to contend with problems of limited simulator runs and of correlating performance on a simulator to performance in the plant control room.

Hardly any concerted efforts have been made to assess the effects of PSFs on operations. Simulators are valuable tools for such assessments too.

The primary problem for HRA is the dearth of error frequencies for process tasks. Even when quality data (in the form of error relative frequencies) is available, these data need to be extrapolated (i.e. generalised) to situations other than those in which the data were obtained. Errors in generalising data from one situation to another increase significantly with increasing differences in PSFs. Even for identical tasks there can be substantial differences in the PSFs. An understanding of the PSFs is very important, because of their criticality in affecting behaviour of plant personnel with respect to safety. The development of appropriate human error taxonomy is very useful in the context of data collection for HRA.

#### 4.6.3 Guidelines for Development of a Successful Data Collection Scheme

There are five major areas influencing the success of a data collection scheme. Success is decided by the frequency and level of detail of event reports that get included into the database and whether plant personnel are sufficiently motivated to actively participate and report errors, near-miss events or potential problems. The five areas are discussed below.

- (i) Nature of information collected - The consideration here is whether the scheme collects mainly descriptive reports (covering who, what, where and when of the event) or if it additionally covers the causal nature of an error (why it occurred). Other factors are whether near-misses are collected as well as actual incidents, and whether the reports are written descriptions of the event or text supplemented by answers to specific questions. A written description is useful in understanding the sequence of events, which occurred. But answers to specific pre-framed questions can provide details necessary to establish root causes.

- (ii) Level of help given with collecting data - Most of the information collected on human performance problems in significant events in NPPs is gathered by interviewing plant personnel. Plant personnel are generally not trained in human factors and psychology, and it is therefore difficult for them to focus on aspects necessary to establish why the error occurred. Schemes may or may not provide help in answering the relevant questions. Also, the forms for collection of information may themselves be complex and difficult to use. Another factor is whether the analyst himself is given help in determining the root cause from the information provided. Such help can increase the reliability of the analyst, without any increase in his/her training time. Further, it is essential to collect the information soon after the occurrence of the event, when the relevant details are still fresh in the minds of plant personnel.
- (iii) Use of database information - It is important to the success of the data collection scheme to provide regular and appropriate feedback to plant personnel. For doing so, it must be possible to easily generate summary statistics and pertinent examples from the information in the database. Also important is whether specific error reduction strategies are derived from the data collected and implemented by the management. Regular feedback, which shows such effective use of the data collection scheme, will make the scheme increasingly acceptable to plant personnel.
- (iv) Organisation of reporting scheme - This covers factors related to whether the scheme is plant-based or centrally organised, and whether incident reporting is mandatory or voluntary. Another factor is whether the scheme is paper-based or computerised. A plant-based computerised scheme is to be preferred for event reporting.
- (v) Acceptability to plant personnel - For the data collection scheme to be successful there should be a feeling of 'ownership' shared by plant personnel and management in a spirit of cooperation. It is also important to have a plant-based coordinator (known to the personnel) in charge of data collection and analysis. Other important factors include comprehensive initial training to personnel on the nature of human factors and the purpose of data collection, provision of some guarantees of anonymity wherever possible and immunity from punishment other than in case of exceptional rule violations.

Functioning human performance data collection schemes are regarded to be successful in some of the areas discussed above, but not in others. INPO's Human Performance Evaluation Scheme (HPES) for example, is considered to be generally good in the last three areas but weak in the first two.

#### 4.6.4 Designing a Human Performance Data Collection System - Summary of Considerations

The considerations involved are as given below.

- (i) Nature of information collected
  - (a) Include causal information in descriptions
  - (b) Cover significant events and near-misses
  - (c) Include specific questions in reporting forms
- (ii) Level of help given with collecting data
  - (a) Provide help to plant personnel with data gathering
  - (b) Provide help to analyst in Root Cause Analysis
  - (c) Design easy-to-use forms and systems
- (iii) Use of database information
  - (a) Provide good regular feedback
  - (b) Include provisions for easy analysis
  - (c) Generate error reduction strategies

- (iv) Organisation of reporting scheme
  - (a) Implement computerised plant based scheme
  - (b) Foster voluntary reporting
  - (c) Keep the costs of the scheme low
- (v) Acceptability to plant personnel
  - (a) Foster “shared ownership”
  - (b) Have a plant coordinator for data gathering and analysis
  - (c) Impart introductory training to plant personnel

#### 4.6.5 Data Collection Methodology

##### Introduction

The material presented in this section is drawn from [21]. The steps in the data collection methodology followed are as follows.

- (i) Development of human error taxonomy
- (ii) Human error reporting form (HERF) - design and verification
- (iii) Analysis of plant events and filling of forms
- (iv) Review and tabulation of data
- (v) Analysis of data collected
- (vi) Presentation of analysis results

The steps are detailed below.

- (i) Development of human error taxonomy

A human error taxonomy was developed for use in data collection from Indian NPPs. The taxonomy is outlined in Appendix-2.1. The taxonomy covers Human Error Categories (i.e. mistakes and slips), External Error Modes or Mechanisms (i.e. observable manifestations of human error or error in action response, e.g. omission, commission or extraneous act), Internal Error Modes (i.e. error in cognitive response, e.g. error in detection, interpretation, diagnosis or decision making), Internal (Psychological) Error Mechanisms (e.g. attention failure, memory failure, judgement failure, stereotype takeover, spatial mis-orientation, indecision, uncertainty, invoking a shortcut or pressure of time) and Error Causes (i.e. reasons for occurrence of error as decided by the PSFs extant in the actual plant context). Errors can be caused by factors related to task complexity, ergonomics of HMI, procedures (content, format, violation), inadequate supervision, communication problems, improper or unauthorised operation, poor skill or inexperience, inadequate training, stress and physiological factors.

- (ii) Human error reporting form (HERF) - design and verification

A human error reporting form (HERF) for nuclear power plant was designed to document the data pertaining to each human error caused/related event from the details given in the incident report. The form is given in Appendix-2.2. This HERF was used by the AERB HRA working group for collecting data from Indian NPPs. A set of guidelines was prepared for streamlining the use of the form. The form was also used in the work carried out under the IAEA Coordinated Research Programme, 1995 - 1998 [21].

##### Structure of HERF

The HERF incorporates a human error taxonomy of the kind detailed earlier, so that all details relevant to human reliability can be systematically documented. The form aids the analyst in

maintaining quality and consistency of data across human error caused/related events in the plant. One of the main aims of data collection and analysis using the HERF is to arrive at measures for preventing the recurrence of the human error, or at the least reducing its probability of occurrence.

The HERF employs a combination of free text descriptions and coded format entries to record the requisite data in a simple readily understandable manner. The HERF, when filled and completed for an event, would contain both factual (objective) and subjective information. The information gathered from interpretations of plant personnel is subjective. It is influenced by factors such as those given below.

- (a) Inability to recall important facts over a period of time.
- (b) Inadequate understanding of causal factors and human behaviour.
- (c) Unwillingness to accept responsibility.
- (d) Holding back key information for fear of being disciplined.

The form consists of three main sections.

- (a) Problem description
- (b) Human error data
- (c) Human error analysis.

Problem description - The problem description part contains the following items of information.

- (a) Free text description of the problem, including plant unit, pre-event and post-event plant status, date and time of occurrence and event sequence details.
- (b) Personnel involved in the event and their contributions.
- (c) Number of hours the personnel (operators, maintainers) involved in the incident, had already been on the job at the time of occurrence of the human error event.
- (d) Number of times the same error event has occurred earlier.

Human error data - This part of the HERF is used to document information on the human error, which includes error categories, error modes/mechanisms, error causes, error recovery information (i.e. feedbacks used) and performance shaping factors.

Human error analysis - This section considers, wherever possible, the estimation of an HEP for the error under study. The HEP is calculated as:

$$\text{HEP} = \text{basic HEP (BHEP)} \times \text{PSF multiplier} \times \text{RF multiplier},$$

where BHEP, i.e. probability of human error for the task considered as an isolated activity or entity, is modified by the extant Performance Shaping Factors (PSFs) and Recovery Factors (RFs). The PSF multiplier depends on the values assigned to the PSFs present in the task environment. The RF multiplier takes into account any recovery from error effected by the operator on detection of error. The PSF and RF multipliers appropriately adjust the BHEP to give an estimate of the HEP for the error under investigation.

Verification of HERF

The initial version of the HERF was applied to data collection case studies in two Indian PHWRs, so as to check whether the form was adequate for the purpose of collecting human error and human reliability data from incident reports. Discussions with plant personnel helped to clarify important human performance issues. Suitable changes were made to the form, and its effectiveness in data collection was confirmed. Appendix-2.3 presents a sample form completed for a typical human error related event in RAPS 1.



(iii) Analysis of plant events and filling of forms

Incident reports pertaining to Indian NPPs were studied and those cases were sorted out where a human error was clearly the cause of the incident, or one or more human performance issues contributed in some way to the incident. Some events involving unavailability of a system/component, attributed in the incident report to system/component failure, were found to have been actually caused by human error or less than adequate human performance in a prior maintenance/test activity.

Reports pertaining to human error/human performance related events were reviewed and analysed in detail. The events were discussed with plant personnel and engineers, in order to gather supplementary information (e.g. limitations due to poor ergonomic design of the work place, workload and environmental factors) or clarify how the event actually took place. The analysis, which began with the incident report, thus moved backwards until explanations were found and details of circumstances under which the event occurred, could be established. However, in cases, which pertained to events, which had occurred a number of years earlier, adequate details could not be gathered.

HERFs were filled for the human error and human performance related events identified and analysed. The details entered into the forms were based on analysis of the recorded data, using the information gathered during discussions with plant personnel. The data collection team included an engineer who had worked as an operator.

(iv) Review of information and tabulation of data

The information contained in the HERFs was reviewed. All useful information pertaining to human error/human performance related events was organised in a tabular format (Appendix-3.1). The data fields used in tabulation were drawn from those used in a standard format developed during the IAEA CRP. The data fields in the standard format are as follows.

- (a) Plant identification (e.g. station, unit)
- (b) Human interaction type (category A, B, or C)
- (c) Time, plant state (pre-event), event and task descriptions, plant state (post-event).
- (d) Error description
- (e) Equipment/controls operated
- (f) Location, major activity (operation, maintenance, testing)
- (g) External error mode/mechanism (omission, commission, extraneous act) and internal error mode (detection, diagnosis, interpretation, decision making)
- (h) Internal (psychological) error mechanism
- (i) Error causes/performance shaping factors
- (j) Data origin (e.g. plant experience)
- (k) HEP(point estimate), uncertainty bounds (UCBs) - 5<sup>th</sup> and 95<sup>th</sup> percentiles
- (l) Model (if data is manipulated or derived using an HRA model)
- (m) Reference source (e.g. incident report-IR), data pedigree (quality, validation status, why generated and how used, e.g. in PSA).

(v) Analysis of data collected

The error data collected were classified and analysed with respect to the following.

- (a) Major activity group (operation/maintenance/testing).

- (b) External error mode (omission, commission, extraneous act).
- (c) Internal (psychological) error mechanism. Determination of the internal failure mode for an error was only possible in a few cases. There is a good deal of uncertainty associated with it, due to the fact that the analysis is often carried out a considerable time after the occurrence of the event.
- (d) Error causes/performance shaping factors (PSFs) influencing error.
- (e) Error relation to plant state (errors in operation leading to shutdown/trip, errors in operation for which plant survives and continues to operate, errors in shutdown).
- (f) System-wise categorisation (system-wise grouping of errors - primary heat transport, moderator, secondary, reactor regulating, reactor protection, fuelling machine, shutdown cooling, turbine generator and electrical, and containment and ventilation).
- (g) Location-wise error distribution (control room, turbine building, reactor building, reactor building shutdown accessible area, service building, motor control centre, switchgear area, battery room and switchyard).
- (h) Error relation to shift (morning, afternoon, night) and time interval of occurrence in shift (first two hours, mid four hours, last two hours of shift).

Sample human error/human performance related event data, arranged in tabular format, is presented in Table AP 3.1 in Appendix-3.1.

(vi) Presentation of analysis results

Prior to and during the IAEA CRP, a total of over fifty human error/human performance related events were identified for investigation and analysis in two twin unit stations, RAPS and MAPS. The number of error events for the two stations, were found to be nearly equal, and were spread out over a period of eight to ten years. The errors were analysed with respect to the dimensions outlined in the previous step. A summary of the results of analysis of plant event data is given in Appendix-3.2.

4.6.6 Plant Specific Human Error Probability (HEP) Data

4.6.6.1 Calculation of Human Error Probabilities From Indian Pressurised Heavy Water Reactor (IPHWR) Event Data.

Estimating HEPs, from human error event data gathered from the operating plants, is beset with problems. Events are generally few and far between, so that the number of times a human error of given type has occurred in a plant, may be quite small. Many kinds of human errors may have never occurred at all. Also, errors that occur, but do not cause events of consequence, simply go unreported. So is the case with errors, from which recovery is made in time to prevent any reportable consequence. As a result, the values of the numerator (number of errors) and denominator (number of opportunities), used in the calculation of HEP, do not reflect the actual error situation. Therefore, there is a certain degree of uncertainty associated with the estimated HEP.

Of the over fifty human error/human performance related events in RAPS and MAPS, in only nine cases had the same type of human error occurred more than once. These nine cases were studied and it was found that for five of the nine cases, it was possible to estimate the number of opportunities for the concerned error. Based on the relevant plant data and supported by confirmatory discussions with plant operations and maintenance personnel, the number of opportunities for each error was estimated. Event details, together with HEP estimates are given in Appendix-4.

4.6.6.2 Observations on the Quantification

The calculated HEPs are indicative estimates and accurate in terms of the order concerned. At the time the data collection was carried out, the number of operating IPHWR units were few and only four units were considered. The figures for both numerator (number of errors) and denominator (number of

opportunities), used in the calculation of HEP therefore turned out to be rather small numbers. Further, the number of repeat error cases were also very few, to provide any reasonable number of HEPs.

In the last decade and a half, there has been a significant addition to the number of IPHWR units in the country. This means that the number of plant units currently in operation, and therefore available for collection of IPHWR specific human error probability data, are enough to provide a sufficient number of human error/human performance related incident records for a fairly large HEP database for HRA.

#### **4.7 Currently Used Databases**

Human reliability databases are collections of properly collected, classified and analysed human reliability data. Databases may contain both generic and specific human performance data.

##### **4.7.1 THERP Database**

THERP was the first moderately comprehensive human reliability quantification technique. It incorporated both a procedure for formulation and analysis of event tree logic for human error and a database of typical human error rates and related PSFs. THERP was developed initially for NPP applications, but the data used in THERP did not come from NPP tasks. The data is derived from data pertaining to other industries, and the data in respect of task error rates covered only operator procedural errors. Subsequent developments however, led to the method becoming more all inclusive, and the database now provides human error rates and recovery factors for diagnosis of abnormal events using display cues, manually operated controls, locally operated controls, oral instructions and written procedures. Later developments of the database allow the consideration of the influence of cognitive errors, dependencies (within person and person to person), management and administrative control, stress, staffing, experience levels and other PSFs [25]. The THERP database consists of twentyseven tables of human reliability data and data for errors relevant to the common error events experienced in engineering systems. The tables are reproduced in Appendix-5.

Despite being quite exhaustive, and after nearly three decades of work, the database still does not cover all tasks of interest to NPP safety analysts. This is understandable, given that the tasks are unique and that the original database, as well as subsequent refinements, may not actually represent all the PSFs affecting human performance. While noting the subjectivity of estimated HEPs in the handbook, experts realised they had no substitutes. This reflected the major problem of HRA, the lack of adequate experiential data from which HEPs could be determined.

##### **4.7.2 Time Reliability Correlation (TRC) Data**

THERP provides a time-dependent model of the diagnosis process, called the Nominal Diagnosis Model. This Time Reliability Correlation (TRC) is supposedly applicable to the estimation of the probability of failure in choosing the proper procedure, because the diagnosis of the abnormal situation is incorrect.

The TRC is a consensus of the judgement of several risk and human reliability analysts, and not based on data. ASEP, a modified version of THERP, provides both a screening diagnosis model and a nominal diagnosis model.

Another TRC database is the Human Cognitive Reliability (HCR) Model, which has been developed for the evaluation of non-response probability under time constrained emergency situations. The HCR has been validated with data from plant simulators. However, the model does not consider the quantification of dependency between tasks and is not designed for procedural events in which no time constraints are imposed. In addition to the THERP TRC and HCR, other TRCs have been developed and are covered in the literature. The THERP TRCs and HCR are reproduced in Appendix-6.

##### **4.7.3 Simulator Data Collection and TRC Development**

Simulator data is the basis of TRCs used for quantifying time dependent human failures. Postulated accident sequences are run on simulators for training operators in the emergency procedures. Such a

sequence commences with the introduction of a plant upset (initiating event) with one or more system faults and simulation continues for a specified time into core damage, until fidelity of simulation becomes too uncertain to carry on.

Data in the form of 'time-lines' of key events, with event time and event details is recorded. The information is arranged into a TRC format by focusing on a particular action and determining from the timelines, the time from a leading cue (indicating the need for carrying out the action), to the time the action is performed, or the sequence was terminated. Statistics for the action is compiled using an aggregation formula and plotting the result on log-probability paper.

$$p_i = \frac{N_i}{N + 1}$$

where 'i' indicates the i<sup>th</sup> failure of a specified type,  $N_i$  is the cumulative number of failures upto and including the i<sup>th</sup> failure,  $p_i$  is the empirical cumulative probability for the time of the i<sup>th</sup> failure.

Note : Relation is not  $N_i/N$ , as  $N=0$  will mean  $N_i=0$  and  $0/0$  has no meaning. So the relation is taken to be  $\frac{N_i}{N+1}$ . Then for  $N=0$  and  $N_i=0$ ,  $p_i=0$

The data so derived can be fitted to any typical probability distribution or plotted on log-probability paper. TRCs have been derived using log-normal, Weibull and other distributions.

HRA researchers in a number of countries have used NPP simulator data to develop TRCs. As an example, the development of TRCs by EDF in France is discussed. An approach termed the Probabilistic Human Reliability Analysis (PHRA) Procedure was developed by EDF [18] to study human interactions in PWRs. PHRA combined a systematic analysis approach with a large database generated from simulator tests. The main features of the PHRA Procedure are as follows.

- (i) A distinction was made between routine operations and post-initiating event operations.
- (ii) Different categories of routine operations were distinguished such as alarm response, administrative check and periodic test, and error probabilities were evaluated using established human reliability quantification methods.
- (iii) For post-initiating event human interactions, 200 simulator runs were carried out and TRCs for predetermined situations of varying complexity were produced. Error probabilities for the human interactions were evaluated from the TRCs.

The time reliability curves produced from the simulator experiments conducted by EDF are given in Appendix 6. In Figure AP 6.4, P1 and P1' represent TRCs for tasks involving simple diagnosis, P3 is a TRC for tasks involving difficult diagnosis with contradictory information displayed and P2 is for tasks involving a mix of both.

There are drawbacks associated with the EDF TRCs. The underlying data for the simulator experiments and method of data collection are not generally accessible. Furthermore, it is difficult to use the data for situations other than those that constitute the basis of the curves and the applicability of the data, must be judged by the analyst. Whether the diagnosis curves can be transposed to other NPPs is not known.

#### 4.7.4 Other Human Reliability Databases

##### 4.7.4.1 Nuclear Computerised Library for Assessing Reactor Reliability (NUCLARR)

NUCLARR [5] is a PC based risk analysis software package, data manual and users' guide, developed by the US NRC to support safety analysis of NPP operations. The database contains some 2500 data points. Half of these are human failure rates and half are electrical and mechanical component failure rates. In addition to raw data values, information on references/sources is also included, so that users can query the database to determine the applicability of the referred data to a specific situation. Type of plant, brief description of error, applicable PSF information and list of source documents also form part

of the data. For human failure rates, the sources are plant specific PRAs, databases of individual plants, technical reports and engineering and simulator studies. Some data from NUCLARR is presented in two tables in Annexure-1

Human failure rates for plant systems are included in the database. As an extension, HEP values for decision-based errors are identified using SLIM or other methodologies. Further, a selected set of data records can be combined to give a single aggregated value (i.e. a single data point estimate and distribution limits, UCB and LCB). Aggregated data are useful in risk assessment when no original data are available that fit the application.

The NUCLARR data repository is used by HRA practitioners, but its use is limited to what data exists. Data from many sources are represented in NUCLARR, e.g. THERP, SLIM, HCR data and simulator data. However, the availability of NUCLARR is restricted.

#### 4.7.4.2 CANDU Nuclear Power Plant HRA Data

CANDU HRA and HRA data is discussed in the following four sections.

##### (i) Early CANDU HRA and HRA data

Human reliability has been estimated and incorporated in PSA of CANDU nuclear power plants since the mid seventies. All the elements of each PSA, including HRA were specifically designed to provide feedback to design and operations groups. The primary objective of early CANDU HRA was to focus on difficulties faced by the control room crews in diagnosing events. From reviews of expected alarms during event occurrences and estimations of available time to respond, HEPs for 'failure to correctly diagnose the events' were assigned a value of 1, 0.1 or 0.001. Compared to the HEPs in the handbook, over almost the complete time frame, CANDU HRA assigned a higher probability of human error for critical diagnosis activity, using a three step TRC [17].

The ground rules applicable in the computation of probabilities for failure to diagnose were:

- (a) Probabilities apply to control room crew and not for one individual.
- (b) Probabilities are applicable to accidents with a frequency of  $< 1$  / year.
- (c) The TRC is the median joint HEPs nominal model for a single event

The HEPs from the TRC are increased/decreased by appropriate factors depending on the situation. In CANDU HRA, error probabilities are increased by a factor of 10 when: 1. A situation does not result in directly useful alarms and 2. Analysis postulates prior operator error in the same accident sequence.

In any PSA, an event tree is built for each postulated accident, with branching on success/failure of various mitigating functions. In CANDU HRA, each operator action was emphasised as a separate 'mitigating function' in each event tree. Each event tree featured a time axis and alternative operator actions were incorporated at appropriate points in the accident sequence. The usual practice in PSA/HRA then was to include the post-accident operator actions within each alternative branch of the event tree.

Later, HRA included the following inputs.

- (a) Pre-accident human unreliability involved in test, maintenance and calibration activities is explicitly incorporated in all pertinent systems. Basic HEP (BHEP) of 0.001 was used in each case with applicable PSFs and RFs modifying it.
- (b) Post-accident human involvement is separated into diagnosis plus execution steps. HEPs for failure to diagnose the event are as before. Failure to execute the appropriate corrective action (as detected by diagnosis) was assigned an  $HEP = 0.001 \times N$ , where N is the number of individual corrective action steps.

Documentation figured as an important aspect. Standard forms were employed to systematically record the details of each identified human action. The details recorded included the following.

- (a) Plant status when operator was called upon to act.
- (b) Detailed description of the human action.
- (c) Annunciations expected and their timings.
- (d) HEP calculations.

The standard forms provided guidance to the analyst and served to promote consistence in the application of the HRA method.

(ii) Subsequent developments in CANDU HRA [6]

A subsequent development in CANDU HRA was the introduction of a Human Interaction (HI) Taxonomy, which is divided into three sections. Section 1 comprises Simple Interactions and Sections 2 and 3 comprise Complex Interactions. Sections 1 and 2 are further divided into two groups. Group I contains interactions, which are called Disability HIs. Group II contains Failure Detection interactions. Section 3-Complex Interactions consider disability and failure detection components together. The human interaction taxonomy is delineated below.

Section 1: Simple human interactions

These are divided into two groups; Group I (Disability) and Group II (Failure Detection) interactions.

Group I: Disability

- (a) Component is left in incorrect state after maintenance and not detected.
- (b) Component is left in incorrect state after testing and not detected.
- (c) Component is left in incorrect state during normal plant operation and not detected.

The disability interaction includes both the fact that the component is left in the wrong state and the fact that that this error is not detected by operating personnel.

Group II: Failure detection

Component failure is not detected by direct indication during routine maintenance, testing or normal operations.

The failure detection interactions cover those human errors wherein the operator has not detected a failed component or system. The detection includes the possibility that the operator fails to notice the display or notices the display but takes no action. In either case, the operator fails to respond.

Section 2: Complex interactions

These are divided into two groups; Group I (Disability) and Group II (Failure Detection ) interactions.

Group I: Disability

- (a) System/subsystem left in incorrect state and not detected following maintenance or testing or during normal operation.
- (b) Non-simple component left in incorrect state and not detected following maintenance or testing or during normal operation.

- (c) Multiple redundant components left in incorrect state and not detected following maintenance, testing or calibration or during normal operation.

Group II: Failure detection

No response to failed component or system by interpreting display devices during routine maintenance or testing or normal plant operations.

Section 3: Complex post-initiating event interactions

Disability and failure detection are considered together.

- (a) Required action not taken and not detected.
- (b) Required action is taken incorrectly (too soon/too late/out of sequence/too much or too little an extent) and not detected.
- (c) Action taken when not required and not detected (component/system caused to function due to error or component/system prevented from functioning due to error).

(iii) HRA quantification

Ready reference tables of HEPs, for both Simple and Complex interactions, were developed and used in CANDU HRA. The HEP database used in CANDU HRA is detailed below.

(a) Simple interactions

Simple interactions occur during routine plant operations in which task conditions and procedures to be used are known. Generic methods can be developed for the quantification of simple human interactions.

A basic (unmodified) HEP is estimated from plant experience for each simple human interaction. The basic HEP is to be modified to take into account:

- the location of the human interaction.
- whether control room display devices are available to allow the operator to detect the error(s) and recover from it.
- whether error might be detected by plant walk-around or main control room panel checks.

HEP modification

Location: As the environment becomes more difficult to work in, there is increased chance of error. The location where a human action is to be performed becomes important. The probability of error increases progressively from Main Control Room (MCR) to field to radiation area by a multiplying factor.

Indicating devices: The probability of error is to be adjusted for the kind of indicating devices available. The error or failure is detected by an indicating device in the MCR. These devices can include window alarms, CRT display alarms, CRT information displays, Digital Panel Meters (DPMs), recorders and indicating lamps. The absence of an indicator (of any kind) would call for no modification at all of the HEP. The HEP can be adjusted for the presence of more than one device.

Inspection: The inspection factor takes into account the probability that the period of unavailability of equipment/system between error occurrence and discovery by inspection could be significant. By estimating the average time between manipulations (opportunities for failure), the corrective inspection multiplier can be calculated from

empirically derived equations for error detection through window/CRT display alarm in MCR, without an alarm of any kind in MCR, walk-around and also for the case with none of these available.

A table of data used for the preliminary quantification of simple human interactions in Pickering Nuclear Generating Station, is given in Annexure-2.

(b) Complex interactions (Post-initiating event)

In post-initiating event human interactions, the possible human errors include actions required not taken (i.e. errors of omission) and not detected, and actions required performed incorrectly (errors of commission) and not detected. The need to perform a task arises on detection of a component or system failure and/or diagnosis of an event requiring corrective/mitigating actions.

Quantification for HRA considers three dimensions to be the prime determinants of error probability. These are task characteristics, quality of indications and available time. The three determinants are detailed below.

Task characteristics

The more complex the task, the more likely it is that errors will be made. Tasks are classified into three levels of complexity as given in Table 4.3.

**TABLE 4.3 : TABLE OF TASK TYPES**

Task Type-1	Uncomplicated routine operations performed on regular basis. Procedure with check off provisions. Timing of steps in an operation is unimportant. Strong feedback is available on successful completion.
Task Type-2	More complex multiple actions performed infrequently, but well documented or part of simulator training. Timing of steps in an operation may be important. Feedback of successful completion may be unclear.
Task Type-3	Actions rarely performed /never performed. Operator may not have been trained. Operator knowledge required for diagnosis of abnormal condition and performing mitigating actions. Feedback may be confusing or absent.

Quality of indications

The quality of indications affects detection/diagnosis of the event. Indications can be grouped into four classes as given in Table 4.4.



**TABLE 4.4 : CLASSES OF INDICATIONS**

Class 1 (I1)	Unambiguous indications in the Main Control Room allowing diagnosis without analysis.
Class 2 (I2)	Indications for which the cause can be one of many and for which interpretation is required to isolate the cause.
Class 3 (I3)	Unclear indications, which inform the operator of deviance but the nature of the problem is not easily determined from the available information (which may be misleading).
Class 4 (I4)	No indication available in the Control Room. The operator does not detect the deviant condition.

Time available for action

There are four classes of this determinant and these are as given in Table 4.5.

**TABLE 4.5 : TIME AVAILABLE**

Class 1(T1)	Unrestricted time available.
Class 2 (T2)	Time available more than required.
Class 3 (T3)	Time available is nearly equal to that required.
Class 4 (T4)	Time available is less than required.

Using the above levels/classes for the three determinants, a matrix of human error probability values has been developed for preliminary post-initiating event quantification in CANDU nuclear power plants. The matrix shown in Annexure-3 is from Bruce A Risk Analysis Fault Tree Guide, December 1989 included in C.W. Gordon's A Course on System Reliability using the Fault Tree Method [6].

(iv) Current HRA methodology in AECL

The HRA methodology used is based on previous work performed within AECL in the area of HRA and on industry accepted methods and guidelines. For pre-accident and post-accident diagnosis, and, in part, for recovery actions, HRA methodology is based on the experience accumulated during PSA for CANDU NPPs. The modeling of post-accident execution errors is in accordance with international practice. It is based on the ASEP HRA Procedure detailed in the U.S. NRC Report, NUREG/CR - 4772 [26].

## **5. APPLICATION OF HRA DATA AND METHODOLOGY TO CASE STUDIES**

### **5.1 Application of HRA Data**

In carrying out human reliability analysis studies, human reliability is quantified using data from available sources of HEP data. The data, which include generic data, are judgement-based data applicable to a whole range or class of tasks. Generic data often provide acceptable guidelines for HRAs. One commonly used source of generic HEP data is the Handbook of Swain and Guttman (1983). The twenty-seven tables of data from the Handbook are given in Appendix-5. Also used in HRA studies are Time-Reliability Curves (TRCs) and Human Cognitive Reliability (HCR) Correlation. These are given in Appendix-6. HEP data from plant operating experience (plant specific data) may also be used, where such data are available, with due consideration to the situation/context to which they refer. Data from ergonomics and simulator studies also find use in HRA.

### **5.2 Case Studies in HRA**

This section describes eight case studies in human reliability analysis. Four case studies pertain to Indian PHWRs. The other case studies are sourced from the literature and have been appropriately referenced. The purpose of including these case studies is to illustrate the application of various HRA methods and models, discussed in this technical document, to different situations.

The case studies described are as follows :

- (i) Human reliability analysis of manual switchover to auxiliary feedwater system.
- (ii) Human reliability analysis study using success likelihood index methodology (SLIM).
- (iii) Human reliability analysis of emergency operating procedure (EOP) for high pressure process water system failure in MAPS.
- (iv) Human reliability analysis of EOP for inadvertent stuck open failure of instrumented relief valve (IRV) in kaiga nuclear power station.
- (v) Human reliability analysis of EOP for station blackout event in kaiga nuclear power station.
- (vi) Human reliability analysis study of total power failure due to fire incident in Narora Atomic Power Station - Unit I.
- (vii) Human reliability analysis case study of accident management task in PWR - quantitative analysis using SLIM.
- (viii) Human reliability analysis case study of accident management task in PWR - qualitative analysis using cognitive reliability and error analysis method (CREAM).

The specific aspect focused on in each of the above case studies is summarised in Table 5.2.

#### **5.2.1 Human Reliability Analysis of Manual Switch Over to Auxiliary Feedwater System**

##### **5.2.1.1 The Case Study**

This case study is excerpted from section 8.2.3: Brief Example of Human Factors Safety Analysis - Manual Switchover to Auxiliary Feedwater System in 'System Safety Engineering and Risk Assessment: A Practical Approach', by Nicholas J. Bahr [1]. This example has also a reference in the handbook of Swain and Guttman [25]. Their results were derived from a plant visit, review of procedures, interviews with operators and observations of tasks performed.

Plans were underway to change from a manual main feedwater system, in a pressurised water reactor at a nuclear power plant, to an automatic switchover. The concern was whether the manual switchover was a safe procedure to follow during the transition to the automatic system. In different plants this

**TABLE 5.2 : SUMMARY OF SPECIFIC ASPECTS OF CASE STUDIES  
IN HUMAN RELIABILITY ANALYSIS**

	Case Study	System or Plant	Emphasis	Method or Model	Reference Number
1.	Nuclear Power Plant Scenario - Main to auxiliary feedwater switchover	NPP - PWR	Safety of manual switchover	THERP	[1]
2.	Error in a human interaction	Chlorine tanker	Applying expert judgement method SLIM	SLIM	[13]
3.	HRA of EOP	MAPS	Analysis of dominant human interactions	ASEP and HCR	[23]
4.	HRA of EOP	KAIGA nuclear power station	Analysis of dominant human interactions	ASEP	[23]
5.	HRA of EOP	KAIGA nuclear power station	Analysis of dominant human interactions	ASEP	[24]
6.	NPP incident scenario	NAPS-I	HRA-real event	HCR and ASEP	[23]
7.	NPP accident management task	NPP - PWR	HRA-quantitative assessment	Quantitative assessment using SLIM	[12]
8.	NPP accident management task	NPP - PWR	HRA-human error analysis	Qualitative analysis using CREAM	[12]

switchover could take from 5 to 60 minutes to perform. If the action was not performed in time, then the steam generator might run dry and cause a safety hazard.

A second operator whose sole function was to maintain sufficient water inventory in the event of a transient was assigned to the control room. This was in addition to the primary operator, who monitored the rest of the control room activities. The second operator was relegated to a small (work) space to perform his task. The plant viewed the job as training for becoming a primary operator.

Further, the plant had adopted a procedure to eliminate the need for decision making to initiate the auxiliary feedwater system. Whenever the plant was operating at more than 15 percent power and a reactor trip initiated, the second operator would perform his task. Many switchovers were performed at the plant, in both real and simulated cases. The second operator knew the task steps very well, and it was felt that there was little chance of human error in the performance of the task. The larger concern was the failure to begin the switchover procedure. The table on the next page (Table 5.2.1) shows the analysis results.

The first step in the analysis was to consider the implications of only the primary operator performing the task along with his other duties. A HEP of 0.05 for the first five minutes was taken from handbook table for annunciated displays. If the need to switchover does occur, there could be 40 or more other annunciators sounding and the primary operator has to sort through all this information simultaneously.

If time constraints were relaxed from 5 to 15 minutes, it would result in a HEP of 0.01 (a reduction by a factor of 5). Relaxing the time constraints to 30 minutes further lowered the HEP to 0.005.

The shift supervisor was a natural backup to the primary operator performing the (manual switchover) task, but would not be available for the first 5 minutes because of other duties. Between 5 and 15 minutes into the emergency he would only be 'coming up to speed' and would not be fully cognizant of

what precisely was going on. The conditional probability of the shift supervisor's failure to compensate for primary operator's failure was 0.5 (equivalent to a high level of dependence). In 30 minutes, this figure changes to 0.25.

Swain and Guttman do not consider any estimates for 60 minutes because if the switchover had not taken place by 30 minutes, the operators in the control room would be very much occupied with other tasks. Switchover performance would not improve until other problems were under control.

**TABLE 5.2.1 : HUMAN ERROR PROBABILITIES**

<b>Situation without second operator</b>			
At the end of x minutes:	Primary operator	Shift supervisor	Joint HEP (JHEP)
5 minutes	0.05	0.05	
15 minutes	0.01	0.5	0.005
30 minutes	0.005	0.25	0.001
60 minutes	No change	No change	No change
<b>Situation with Second Operator</b>			
At the end of x minutes:	Second operator	Shift supervisor	Joint HEP (JHEP)
5 minutes	0.002	--	0.002
15 minutes	0.001	0.5	0.0005
30 minutes	0.0005	0.25	0.0001
60 minutes	No change	No change	No change

Looking at the second operator, emphasis was placed on the passing of information through oral instructions. A HEP of 0.001 was determined based on a 15 minutes response time. The estimate was doubled (to 0.002) for 5 minutes response time because it was felt the second operator would be somewhat unsure if this (i.e. the event requiring manual switchover to AFS) was really happening. He too would be inundated with the other alarms, all sounding. For 30 minutes, the HEP reduces further to 0.0005.

The success probability (or human reliability probability) is equal to (1- HEP). One can see that the success rate or reliability of the primary operator working alone is 95 percent-not very good. This means that the primary operator working alone will fail to perform the action (of manual switchover to AFS), 5 times out of 100. Just increasing the time available to 30 minutes gives a success probability = 1- 0.001 = 0.999 (or 99.9 percent). This is much better, but not as good as using the second operator.

The reason for this is that the second operator has a sufficiently low human error rate (0.002) even in 5 minutes response, which is probably safe enough as a temporary measure. Extending the time allowed to 15 minutes increases the chance of success significantly. The engineer of course would have to look at the cost implications of the two alternatives.

One other item to note: Notice that the supervisor does not add anything to help the situation, contrary to intuition. In fact, the shift supervisor will make a mistake 50 percent of the time in the first 15 minutes and a mistake 25 percent of the time in 30 minutes.

The data used in this example is taken from generic human error data tables and then modified to what seemed to make sense. It is important to remember that these numbers are highly questionable. This does not mean however that they are completely useless. If we don't apply the numbers in absolute terms-a HEP of 0.05 really meaning that the operator will fail 5 times out of one hundred-then we can use them for what they are valuable for. We should compare the results and determine which situation is best, the single operator or using dual operators. With the estimates, one gets a rough idea of magnitude, and that is very useful.

### 5.2.1.2 Author's Observations on the Human Reliability Analysis

- (a) The PWR plant considered in this example appears to be one of the earliest in its genre, and the situation considered, presumably cannot be extrapolated to a newer PWR nuclear power plant.
- (b) The data used in the above example on HRA has generally been taken from the generic HEP data given in Chapter 20 of Swain and Guttman's Handbook [25]. The tables are reproduced in Appendix-5 of this compendium and are referred to in these observations.
- (c) Table 20-23: Annunciator Response Model-Estimated HEPs for multiple annunciators alarming closely in time [25].
  - 'Closely in time' refers to cases in which two or more annunciators alarm within several seconds or within a time period such that the operator perceives them as a group of signals to which he must selectively respond. Elsewhere in Chapter 20 (Table 20-1 and Table 20-3) it is suggested that 'within 10 minutes' be used as a working definition of 'closely in time'
  - The table gives the probability of failure to initiate action for each annunciator (or completely dependent set of annunciators) successively addressed by the operator.
  - In the situation under consideration there could be 40 or more annunciators sounding, which the primary operator has to sort through simultaneously.
  - The probability of failure to initiate intended corrective action for 10 annunciators is given to be 0.05 (EF=10). This value is the arithmetic mean of 10 values in a row. The upper limit for > 40 annunciators is given to be 0.25.
  - On the basis of the above, the HEP for 5-minute response by the primary operator in the control room (for the situation under consideration) has been judged to be 0.05. For time constraints relaxed to 15 minutes, this is assumed to reduce by a factor of 5 to 0.01 and for 30 minutes still further to 0.005 (i.e. a factor of 10).
- (d) Backup from the shift supervisor is assumed to be unavailable for the first 5 minutes (low to moderate dependence with other operators). Further it has been assumed that shift supervisor would take another 10 minutes to understand the situation. So the shift supervisor would be constrained by his high level of dependence on the primary operator. These conclusions are drawn from Table 20-4: Number of operators and advisors available to cope with an abnormal event and their related levels of dependence-assumptions for PSA.
- (e) From Table 20-17 [25], for high level of dependence (HD), the conditional error probability (with HEP for primary operator = 0.05) =  $\frac{1}{2} (1+0.05) = 0.525$  (taken = 0.5). Further, at 30 minutes, moderate dependence is assumed. For moderate dependence, conditional error probability would be  $(1 + 6 \times .005) / 7 = 0.15$ , which has been increased to 0.25 in the example.
- (f) The second operator receives oral instruction from the primary operator. Table 20-8 gives estimated probabilities of errors in recalling oral instruction items not written down. In the example, a HEP of 0.001 is determined, based on a 15-minute response. This matches with the HEP of 0.001 given failure to initiate the task specified by the oral instruction. It is assumed that the HEP would double to 0.002, if the response time was constrained to 5 minutes and halve to 0.0005, if the time available for the action was relaxed to 30 minutes.
- (g) It is stated that the data used in the example have been taken from the generic data tables in the handbook, and then modified to make sense. The deviations from tabled data observed in 'c' and 'e' above could be attributed to these modifications.
- (h) In the example, HEPs are not estimated for 60-minute response. The reasoning given is that, in the event the switchover action had not been carried out by 30 minutes, the operators in the

control room would get involved with other tasks, and the switchover operation would get postponed until other problems were resolved. It is the author's view that it is unlikely that such an important operation would get superseded by other operations, given the extent of training given to operators and shift supervisors.

- (i) The example serves to illustrate the utility of a HRA study in which accurate human reliability quantification (i.e. obtaining absolute HEP estimates) is not very important to the purpose of a HRA study. In the study, it is the relative HEP estimates arrived at for the two cases, viz., situation without second operator and situation with second operator, that is important to understanding how improved performance reliability is achieved by adding a second operator in the control room. This HRA study exemplifies how human redundancy can be used to improve operational safety.

## 5.2.2 Human Reliability Analysis Study Using Success Likelihood Index Methodology (SLIM)

### 5.2.2.1 The Case Study

This case study is excerpted from section 5.5.3.1. Success Likelihood Index Method (SLIM) of 'A Guide to Practical Human Reliability Assessment' by Barry Kirwan [13]. It is included here to illustrate human reliability assessment using SLIM.

#### Methodology

The SLIM [4] can best be explained by means of an example of Human Reliability Assessment - in this case, an operator decoupling a hose from a chemical (chlorine) road tanker. In this situation the operator may forget to close a valve upstream of the filling hose, which could lead to undesirable consequences, particularly for the operator, i.e. the operator could get a rather nasty and possibly fatal dose of chlorine. The human error of interest here is the 'Failure to close Valve 0101 prior to decoupling the filling hose'. In this case the decoupling operation is simple and discrete, and hence the failure occurs catastrophically rather than in a staged fashion.

The 'expert panel' required to carry out the SLIM exercise would typically comprise, for example, two operators with a minimum of ten years' operational experience, one human factors analyst and a reliability analyst who is familiar with the system and who also has some operational experience.

The panel is initially asked to identify a set of Performance Shaping Factors (PSFs), defined as any factors relating to the individual(s), environment or task, which affect performances, positively or negatively. The expert panel could then be asked to nominate the most important or significant PSFs for the scenario under investigation. In this example, it is assumed that the panel identifies the following major PSFs as affecting human performance in this situation.

- Training
- Procedures
- Feedback
- Perceived level of risk
- Time pressures involved

#### PSF rating

The panel is then asked to consider the other possible human errors arising in this scenario (e.g. mis-setting or ignoring an alarm) and then to decide to what extent each PSF is optimal or sub-optimal for that task in the situation being assessed. The 'rating' for whether a PSF is optimal or sub-optimal for a particular task is made on a scale of 1 to 9, with '9' as optimal. For the three human errors under analysis, the ratings obtained are as follows.

Errors	Training	Procedures	Feedback	Perceived Level of Risk	Time
V0101 open	6	5	2	9	6
Alarm mis-set	5	3	2	7	7
Alarm ignored	4	5	7	7	2

#### PSF weighting

If each factor were equally important, one could simply add each row of ratings and conclude that the error with the lowest rating-sum (alarm mis-set) was the most likely error. However the expert panel in this example does not feel that the PSFs are all of equal importance. In this particular case, it feels that the perceived level of risk and feedback PSFs are the most important, and are in fact twice as important as training and procedures, which are in turn one and a half times as time pressure-in this case as it is a routine operation, time is not perceived by the panel to be particularly important. Weightings for these PSFs can be obtained directly from these considered opinions and normalised so as to add upto unity, as follows.

Perceived level of risk	0.30
Feedback	0.30
Training	0.15
Procedures	0.15
Time pressures	0.10
Sum=1.00	

Both the SLIM and the decision-analysis technique, on which it is based, propose that the degree of preference can be worked out as a function of the sum of the weightings multiplied by their ratings for each item (task error). The SLIM calls the resultant preference index success likelihood index (SLI). This is illustrated below with a table that shows the weightings (W) multiplied by the ratings (R), such that the SLI = (sum) WR.

Weighting	PSFs	V0101	Alarm mis-set	Alarm ignored
(0.30)	Feedback	0.60	0.60	2.10
(0.30)	Perceived risk	2.70	2.10	2.10
(0.15)	Training	0.90	0.75	0.60
(0.15)	Procedures	0.75	0.45	0.75
(0.10)	Time	0.60	0.40	0.20
	SLI (total)	5.55	4.30	5.75

In this case, the lowest SLI is 4.30, suggesting that alarm mis-set is still the most likely error. However, due to the weightings used, the likelihood ordering of the other two errors has now been reversed (a close inspection of the figures reveals that this is because there is ample feedback for 'alarm ignored' but not for 'V0101 open'). Clearly at this point a designer would realise that increased feedback to the operator about the position of V0101 might be desirable.

In order to transform the SLIs into human error probabilities (HEPs), it is necessary to 'calibrate' the SLI values. Kirwan [13] mentions studies that have suggested a logarithmic relationship of the form:

$$\text{Log } p(\text{success}) = a(\text{SLI}) + b$$

If two tasks for which HEPs are known are included in the set of errors being quantified, then the parameters of the equation can be derived via simultaneous equations and the other (unknown) HEPs can be quantified.

If in the above example, two more tasks, X and Y were assessed, which had known HEPs of 0.5 and  $10^{-4}$  respectively, and were assessed SLIs of 4.00 and 6.00, then the equation would be derived as follows:

$$\text{Log (HEP)} = a (\text{SLI}) + b. \text{ For Task X, } \text{Log} (0.5) = a.4 + b, \text{ For Task Y, } \text{Log} (10^{-4}) = a.6 + b.$$

$$\text{Therefore, } \text{Log (HEP)} = -1.85 (\text{SLI}) + 7.1$$

The HEPs would be :

$$\text{V0101} = 0.0007$$

$$\text{Alarm mis-set} = 0.1400$$

$$\text{Alarm ignored} = 0.0003$$

#### 5.2.2.2 Author's Observations on the Human Reliability Assessment Using SLIM.

- (a) The SLIM essentially makes use of expert judgement requiring a small group of (e.g. four) experts. It assumes that these experts are capable of estimating failure probabilities associated with task performance.
- (b) Experts assign ratings (on a scale of 1 to 9) to PSFs, on the basis of their relative goodness in the given situation. One end of the scale, e.g. 9, is used to represent the success-inducing level of the PSF. In the above example, a rating of 9 is considered to be optimal and a rating of 1-8 sub-optimal. For some PSFs, e.g. stress, the optimal rating may lie between the two end points of the scale. As an example, consider stress. Too little or too much stress can adversely affect performance. A mid-scale rating (e.g. 6) can be chosen to represent the optimal value of such a PSF.
- (c) The weightings assigned to PSFs are decided on the basis of their relative impact on task performance. In the above example, the impact of two PSFs, Procedures and Training, on task performance, is judged to be 1.5 times that of the Time Pressure PSF. The impact of perceived level of risk, as well as feedback, is judged to be 2 times that of the PSFs, procedures and training, or in other words 3 times that of the Time Pressure PSF.
- (d) Several forms of the calibration equation [ $\text{Log } p(\text{success}) = a (\text{SLI}) + b$ ] exist. Alternatively, it is possible to assess the complement of SLI, called the Failure Likelihood Index (FLI) and use it to calculate HEP.
$$\text{Log (HEP)} = a (\text{FLI}) + b$$
- (e) Determination of the values of the two constants 'a' and 'b' (or 'a' and 'b') requires knowledge of two calibration tasks for which the HEPs are known. In the example, the HEPs of the calibration tasks (X and Y) are 0.5 and  $10^{-4}$  respectively. With these values 'a' and 'b' are evaluated to be -1.85 and 7.1 respectively.
- (f) In the above example, uncertainty bounds are not generated. To do so, experts have to perform direct estimation of upper and lower bounds.
- (g) If SLIM-MAUD software were used, the HEP values for 'V0101 OPEN', 'ALARM MIS-SET' and 'ALARM IGNORED' would be slightly different from those arrived at in the hand calculation method illustrated in the above example. The computerisation facilitates ease of use of SLIM and prevents the biases found in the elicitation of expert opinion from influencing the results. The mathematics of multi attribute utility theory incorporated in the software allows refinement of the weightings and ratings.



## 5.2.3 Human Reliability Analysis of Emergency Operating Procedure for High Pressure Process Water System Failure in Maps

### 5.2.3.1 Introduction

The emergency operating procedure (EOP) for high pressure process water system (HPPWS) failure is analysed from a human reliability perspective. The analysis is used to identify the human actions in the procedure that have a significant impact on event progression and assess their potential to exacerbate the event into an accident in case of failure. The assessment employs the post-incident human reliability analysis method in the accident sequence evaluation programme (ASEP) HRA Procedure.

### 5.2.3.2 High Pressure Process Water System (HPPWS)

The high pressure process water system (HPPWS) in IPHWR is a support system designed to remove heat from process water cooled systems. The HPPWS loads are shutdown cooling system, bleed cooler, end shield cooling system, fuelling machine return cooler, sampling system, thermal shield cooling system and reactor building cooling system. There are five pumps (three running and two on auto standby) in the system. The heat loads on the system are distributed in various locations/buildings at the site. A process water surge tank and a process water emergency storage tank are provided in the system. In case of unavailability of HPPWS, firewater is injected into the HPPWS headers to provide the necessary cooling water supply.

### 5.2.3.3 EOP for HPPWS Failure

HPPW system is considered to have failed when:

- All three running HPPW pumps fail and the standby pumps fail to start on auto.
- HPPW pump discharge header pressure is low.

The main steps involved in the diagnosis of HPPW system failure event and execution of the EOP are outlined below.

Cues for diagnosis and diagnosis

- (i) HPPW system pressure low annunciation in control room. The operator confirms 'Low HPPW Pressure' by checking the indications pertaining to:
  - (a) Process water pumps motor current
  - (b) Class III bus voltage is normal
  - (c) HPPW pump discharge valve is 'open'
  - (d) 'Outlet valve' of the emergency storage tank is 'open'
  - (e) Standby pumps started on 'auto' and are running
  - (f) Discharge valves of the standby pumps are open

A persistent HPPW system failure ultimately causes the following alarms and indications.

- (a) End shield temperature high alarm
  - (b) HPPW system pump discharge header low pressure alarm
  - (c) Bleed cooler temperature high indication
  - (d) Purification inlet temperature high indication
  - (e) Biological shield temperature high indication
- (i) Process water emergency storage tank level low and very low annunciations in the control room. These annunciations occur only when HPPW system pressure cannot be restored even after the following immediate operator actions.

- Starting the standby HPPW pumps if these have failed to start on 'auto'.
- Opening the discharge valves of the standby pumps if these have failed to open on 'auto'.

After carrying out the above actions, if the low HPPW system pressure persists, the operator has to trip the reactor before process water emergency storage tank level low alarm comes. If he does not, the end shield temperature will rise and this may result in structural damage. Also, PHT system pump gland cooler return temperature will rise and this will after some time trip the running PHT System pumps, which will in turn result in a reactor trip.

Time for process water storage tank level low and very low annunciators to come will depend on the size of the leak. In the event of header break in HPPW system, the alarms will come about 3 minutes after HPPW system pressure low is announced. In the event of a leak of say, 15 percent break size, the time taken will be much longer. For the purpose of analysis, the alarms are assumed to come about 20 minutes after the occurrence of HPPW system failure. The break is assumed upstream of the header or in the downstream pipe which is to be isolated.

Other actions in the EOP then follow. Operator has to ensure that the firewater injection valve to HPPW headers is open (auto/manual operation). However, fire fighting water system will not be able to cope with water flowing out through the break. Header low pressure condition will not improve. The persistence of low HPPW system pressure in spite of the above actions is an indication of a continuing leakage from the system. Under such conditions, leak identification and isolation are necessary for selecting the strategy for ensuring removal of heat from the secondary.

Leak identification involves:

- (a) Checking the reactor building (RB) floor beetle alarm to check for leak in RB and isolation of the leak.
- (b) If leak is not in RB, checking for leak in turbine building (TB) and isolation of the leak.
- (c) If leak is not in RB and TB, checking for leak in pump house and isolation of the leak.
- (d) If the leak is not in any of the above, checking for and isolation of leak in the open areas. Leak in open areas is revealed by flooding and leaks through manhole covers.

Depending on the success in identifying the leak location and its isolation, the operator has to resort to either 'Valving In' the shutdown coolers with fire water supply to the secondary side of the shutdown cooling heat exchanger if HPPWS is not available, or Injection of fire water into the steam generators, in manual mode, in order to ensure decay heat removal.

The human interactions in a HPPW system failure incident constitute a dynamic task involving a high degree of person-equipment interaction such as decision making, keeping track of the situation and controlling several functions.

#### 5.2.3.4 Human Reliability Analysis

The human interactions involved in the execution of the EOP are assessed using the Operator Action Tree (OAT) shown in Figure 5.2.3-1. Out of the seventeen possible sequences, only seven sequences have potential to affect core cooling. These sequences are analysed using the ASEP HRA Procedure [26].

- (i) Screening HRA

ASEP HRA for screening diagnosis

Based on the alarms and indications the operator has to initiate reactor trip before the process water storage tank level low alarm appears. The time available before this alarm appears is 20 minutes. In case the operator fails to trip the reactor the end shield temperature may rise and this can lead to structural damage.

PHT system pump gland cooler temperature will rise and after some time, trip the running PHT system pumps, which would subsequently result in reactor trip. No credit for this is taken here.

Out of the total available time of 20 minutes, 5 minutes is assumed to be the time for action and 15 minutes the time available for diagnosis. From the ASEP screening diagnosis curve (Appendix-6), the HEP for failure to diagnose is found to be 0.03 (lower bound value). The lower bound value is chosen because the cues are compelling, the interface is good and the operator is well trained in the EOP.

ASEP screening HRA for operator actions

(a) Manual restoration of HPPW system pressure - actions to be performed are:

- Check whether standby pump is on
- If not on, start it manually
- Check whether discharge valve is open
- If not, open the discharge valve manually
- Check HPPW system header pressure
- Trip the reactor before process water storage tank level low alarm appears. This alarm appears if manual restoration of HPPW System pressure is not successful.

The actions in this set are judged to be completely dependent on each other. The stress is moderately high. The actions are considered to be critical procedural actions. Referring to Table 7.3 (Appendix-6) in the ASEP HRA Procedure, HEP is assessed = 0.05 (EF = 5).

(b) Fire water injection into HPPW system headers-the actions to be performed are:

- Check whether MOV for injection of fire fighting water into HPPW system headers is open
- If not, open the MOV
- Check HPPW system header pressure

These actions are similar to those in 'a' above. Hence, a HEP value of 0.05 is assigned to this set as well.

(c) Leak detection, identification and isolation of leak location- The actions to be carried out are:

- Check for beetle alarm in RB. If beetle has alarmed, isolate the leak. The time required is assessed to be ~10 minutes, allowing an additional time of 5 minutes for the isolation action, since the action is not the kind of regularly practiced written procedure committed to memory.
- If there are no beetle alarms, the TB operator is instructed to check for a leak in TB area and isolate it if it exists. The time for this action is 15 minutes (10 minutes for checking whether there is a leak and 5 minutes for its isolation).
- If there is no leak in RB or in TB, check for leak in the pump house area. If a leak is found, isolate the leak. The assessed time for this action is about 15 minutes (10 minutes for checking and 5 minutes for isolation).
- If there is no leak in any of the above areas, check for flooding in open areas (observed as leaks through manhole covers) and isolate the leak. Assessed time is ~15 minutes (10 minutes for checking and 5 minutes for isolation).

As per the above, leak detection and identification of its location and can take from about 10 to 40 minutes. On a conservative basis, for the purpose of screening, it is assumed to take 45 minutes. The total time available for the event is ~60 minutes. In addition, the actions are conservatively assumed to be knowledge based. The median time ( $T_{1/2}$ ) is taken to be 45

minutes. The normalised time ( $t/T_{1/2}$ ) is equal to  $60/45 = 1.33$  and the correlation coefficients for knowledge based response are  $A_i = 0.791$ ,  $B_i = 0.5$  and  $C_i = 0.8$ . Using the HCR Model, this HEP (non-response probability) is found to be 0.35.

Leak isolation is considered to be a critical procedural action under moderately high stress. From Table 7.3 (Appendix 6) in ASEP HRA Procedure, HEP is assessed to be 0.05.

(d) Valving in shutdown cooling

Shutdown cooling is to be valved in when fire water is available as backup to process water in shutdown heat exchangers. The actions involve in valving in of the shutdown cooling system are closing of two bleed condenser isolation valves, opening of two shutdown cooling line warm-up valves, closing of two shutdown cooling line warm-up valves, opening shutdown cooling line MVs and starting of one shutdown cooling pump. The HEP for valving in shutdown cooling was evaluated in probabilistic safety assessment for Kaiga Atomic Power Project (1996) to be 0.0003.

(e) Valving in fire water into steam generators

Fire water is injected into the steam generators when secondary steam relief (SSR) is available and shutdown cooling or fire water backup to shutdown heat exchangers is not available.

Fire water can be injected into the steam generators in case BFPs and ABFPs are not available. These pumps will not be available due to lack of cooling to the pump motors as a result of failure of HPPW system. The HEP for valving in fire water to SGs was also evaluated in PSA for Kaiga Atomic Power Project to be 0.05

Based on the above discussion, the HEPs of sequences ending in failure were assessed (Refer Figure 5.2.3-1). These are given below. The probability values used in the assessment are given in Table 5.2.3-1.

Sequence No.	Assessed value of HEP (per year)
3	1.4 E - 5
6	4.1 E - 7
9	2.0 E - 8
11	7.5 E - 5
13	8.1 E - 4
15	1.2 E - 4
17	1.5 E - 3

Considering a cutoff value of  $10^{-5}$ , only five sequences are found to dominate. These five sequences, 3,11,13,15 and 17 are analysed using the ASEP nominal HRA procedure. The analysis is outlined below.

**TABLE 5.2.3-1 : TABLE OF PROBABILITY VALUES**

HUMAN ACTION	SCREENING VALUES		NOMINAL VALUES	
	SUCCESS	FAILURE HEP	SUCCESS	FAILURE HEP
Diagnosis of HPPW system failure	0.97	0.03	0.9994	0.0006
Auto/Manual restoration of HPPWS pressure	0.95	0.05	0.98	0.02
Fire water injection into HPPWS header	0.95	0.05	0.98	0.02
Leak detection; identification	0.65	0.35	0.65	0.35
Leak isolation	0.95	0.05	0.95	0.05
Attempt at restoration of HPPWS pressure	0.95	0.05	0.98	0.02
Valving in shutdown cooling	0.9997	0.0003	0.9997	0.0003
Fire water injection into steam generators	0.95	0.05	0.95	0.05

(ii) Nominal HRA

Diagnosis

For diagnosis of low HPPW system header pressure, two main sets of cues are available. The first includes the low HPPW pressure alarm and the second, in case operator fails to restore HPPW system pressure, is the process water surge tank level low alarm. Using the Annunciator Response Model (Table 20-23, Appendix 5) giving estimated HEPs for multiple annunciators alarming closely in time, such that the operator perceives them as a group of signals to which he must selectively respond, the probability of failure to initiate action in response to the first set of completely dependent annunciators is taken to be 0.0001, and to the second set it is taken to be 0.001. So, the probability of failure to initiate any kind of corrective action = the mean of 0.0001 and 0.001  $\sim 6 \times 10^{-4}$ .

HEPs for operator actions

- (a) Manual restoration of HPPW pressure: The actions are assumed to be critical actions that are part of a step-by-step task performed under moderately high stress. A nominal value of 0.02 is assessed as per Table 8.5 (Appendix 6).
- (b) Fire Water Injection to HPPW system headers: The actions in this task are similar in nature to those in a. The stress level is moderately high. As in the above, a HEP of 0.02 is assessed as per Table 8.5 (Appendix 6).
- (c) Valving in shutdown cooling system: Shutdown cooling has to be valved-in in 30 minutes. The procedure of valving in shutdown cooling is understood, memorised and well practiced in training. Therefore, the actions, although rule based, can be considered to be skill based. HEP for this task is taken to be 0.0003, as in Screening HRA.
- (d) Fire water injection into steam generators: Fire water is to be injected into the SGs in 30 minutes. Though the actions are simple rule based actions and operators are well aware of the situation, they can be under considerable stress. HEP is assessed to be 0.05 as in Screening HRA. Since there is no other means of decay heat removal, the impact of failure is high.

Using the nominal values, the sequence probabilities are worked out as below (Refer Figure 5.2.3-1).

Sequence No.	Assessed probability (per year)
3	1.5 E – 5
11	5.5 E – 5
13	3.4 E – 4
15	2.0 E – 5
17	3.0 E – 5

(iii) Conclusions

Of the above five sequences, sequence 13 is most significant in the execution of the EOP. In order to minimise the probability contribution from the above sequences, it is necessary to reduce the HEP for valving in fire water into the SGs.

5.2.4 Human reliability analysis of the EOP for inadvertent ‘stuck open’ failure of instrumented relief valve (IRV) of primary heat transport system in Kaiga Nuclear Power Station.

5.2.4.1 Introduction

Human reliability analysis of the EOP for inadvertent “stuck open” failure of an IRV of PHT system of Kaiga Nuclear Power Station is carried out. The analysis helps in identifying the actions having significant impact on the IE and potential to exacerbate the event into an accident situation. This analysis employs -the post-incident HRA method outlined in the ASEP HRA Procedure [26].

5.2.4.2 Description of the EOP

In Indian PHWRs, three IRVs are connected to one of the outlet headers of primary heat transport system (PHTS). The IRVs are kept closed by air actuators. The valves open to relieve the PHTS pressure when the set point is exceeded. The relief is to the bleed condenser. If an IRV is stuck open, the bleed condenser becomes a part of the primary heat transport system. To prevent the possible opening of the safety relief valve of the bleed condenser and subsequent LOCA, besides certain auto actions, some human actions are to be carried out by the operator. The EOP identifies the signal indications that help recognition of the event and comprises the actions to be carried out, in order to achieve a safe termination of the event.

5.2.4.3 Diagnosis of the Event

The cues for diagnosis of the event are:

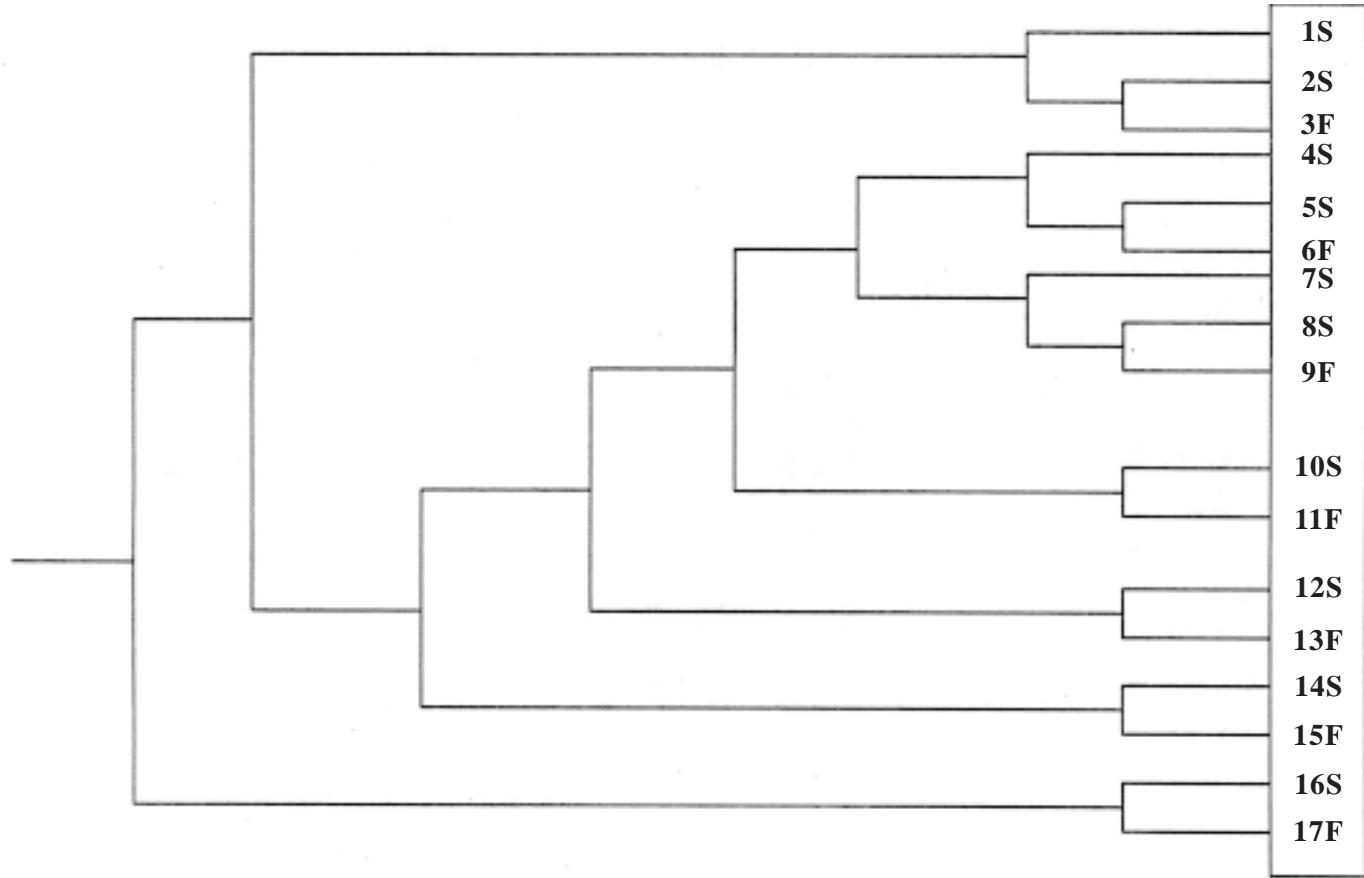
- IRV fully closed light goes off indicating IRV ‘OPEN’
- IRV ‘OPEN’ window annunciation from its limit switch.
- High level in bleed condenser - window annunciation
- High pressure in bleed condenser - control room computer (CRC) alarm
- Bleed cooler inlet temperature high - CRC alarm.

Other (indirect) cues, although available, are not considered here. The compelling signals are IRV ‘OPEN’ light and IRV ‘OPEN’ alarm.

IRV opening leads to the following.

- Sharp fall in PHTS pressure and reactor trip on low pressure (window annunciation)

<b>HPPW system failure</b>	<b>Diagnosis of HPPWS pressure low</b>	<b>Auto or manual restoration of HPPWS pressure</b>	<b>Fire water injection into HPPWS header</b>	<b>Leak detection</b>	<b>Leak isolation</b>	<b>Attempt at restoration of HPPWS pressure</b>	<b>SDC valve in</b>	<b>Fire water injection into steam generators</b>
----------------------------	--	---	---	-----------------------	-----------------------	---	---------------------	---



**FIGURE 5.2.3-1: OPERATOR ACTION TREE FOR HIGH PRESSURE PROCESS WATER SYSTEM FAILURE**

- Low level in PHT system storage tank (window annunciation).
- Rising bleed condenser (BCD) level and pressure.
- Standby primary pressurising pump (PPP) starts on auto (Alarm).
- Reduction in bleed flow.
- BCD temperature, pressure goes high.
- Large BCD level control valves (CVs) close. Small level CV remains open.

#### 5.2.4.4 EOP Actions

- (a) Observe PHTS pressure and BCD pressure, level, temperature. BCD fills up and PHTS recovers due to running of primary pressurising pumps (PPPs). PHTS and BCD pressure rises to 83 kg/cm<sup>2</sup> (g). BCD spray and reflux valves close on auto. Both PPPs trip on auto. F/M pump starts on auto. Small LCV will close on auto leading to total 'boxup' of PHTS.
- (b) Trip PPPs if these have not tripped on auto. Note that PPPs are not to be tripped manually unless pressure has recovered to 83 kg/cm<sup>2</sup> (g).
- (c) If the F/M pump has not started, start it manually by selecting its hand switch to 'ON' position.
- (d) Take pressure controller on manual and control PHTS pressure to maintain it between 70 - 80 kg/cm<sup>2</sup> (g) by the F/M pump. In case it is not, close BCD drain valve and adjust F/M discharge pressure to do so.
- (e) Monitor BCD overflow tank level.

After these actions are completed, the crew should ensure closure of IRV using the hand wheel, by sending a person to the field. Normal decay heat removal procedure will be initiated after the closure of IRV, in order to bring the reactor to a safe shut down state.

#### 5.2.4.5 Human Reliability Analysis

The dominant human interactions involved in executing the EOP are assessed using the Operator Action Tree (OAT) and HRA Event Trees as shown in Figures 5.2.4-1, -2 and -3. The number of event sequences that are possible is limited. Therefore, only ASEP Nominal HRA, as outlined in Swain [26], is carried out. Screening HRA method is not employed. ASEP TRCs and tables are given in Appendix 6.

- (a) HEP for diagnosis

As there are compelling signals for the detection and diagnosis of IRV stuck open condition, the time taken for diagnosis will not be more than 5 - 10 minutes. For a diagnosis time of 10 minutes, nominal diagnosis model gives median joint HEP = 0.1 with an error factor of 10. Lower bound of the nominal HEP (0.01) is considered appropriate, as the diagnosis would generally be quickly accomplished.

The actions here are taken to be rule based. It is assumed that the operators are well trained. The situation of stuck open IRV condition is assumed to be one of potential emergency as it can lead to a small LOCA. The quality of the operator-plant interface is considered to be good.

- (b) HEPs for actions (first set)

The first set of actions, i.e. crew's first operation (Figure 5.2.4-1), is represented by the HRA Event Tree shown in Figure 5.2.4-2. The actions are expected to be completed within 2 - 5 minutes after the event has been diagnosed. The HEP for post-accident post-diagnosis actions is assessed to be ~ 0.02. In arriving at this figure, the values employed for each sub task are as shown in Table 5.2.4-1.



**TABLE 5.2.4-1: HEPs FOR ACTIONS (FIRST SET)**

No.	Action	Probability Value	Remarks
1.	Failure of PP pumps to trip on auto	0.001	Assumed
2.	HEP for manual trip of PP pumps	0.004	Lower bound value for critical action that is part of a step-by-step task, carried out under moderately high stress.
3.	Failure of FM pumps to start	0.001	Assumed
4.	HEP for manual start of FM pumps	0.004	Same as for 2 above
5.	Monitoring PHTS pressure so that it is maintained in the range 70 to 80 kg/ cm <sup>2</sup> g by closing BCD drain valve, adjusting F/M discharge pressure.	0.01	Considered to be a dynamic critical action performed under moderately high stress. The action is considered to be critical as failure to perform the action leads to a small LOCA.

Notes

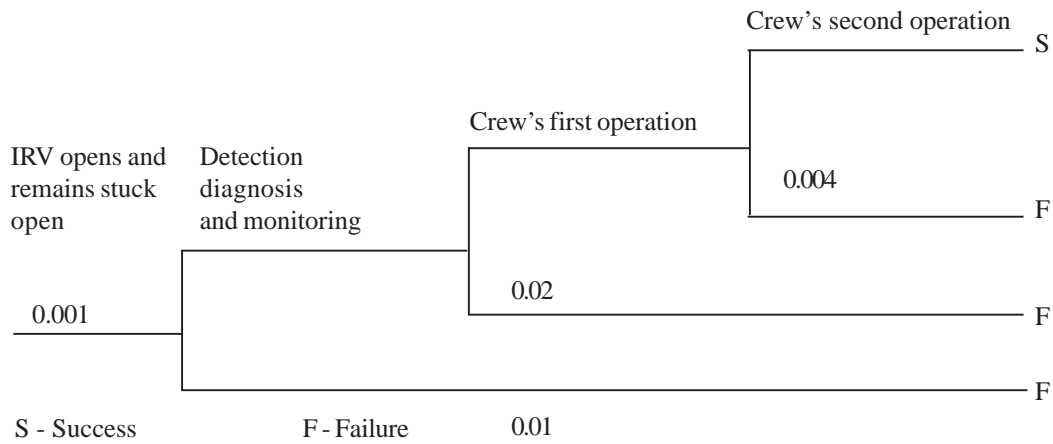
Manual trip of PPPs is part of a step by step (i.e. routine procedural) task. In ASEP, a task is critical if it has potential to put a component or system at risk. Failure to trip PPPs can lead to small break LOCA. Manual trip of PPPs is therefore judged to be a critical task. For a critical step by step task performed under moderately high stress, ASEP nominal HRA gives HEP = 0.02 (EF=5). Lower bound HEP = 0.004.

Monitoring PHTS pressure and maintaining it within a range of 70 - 80 kg/cm<sup>2</sup> (g). is a dynamic task as it involves a high degree of operator-system interaction. The operator has to monitor PHTS pressure and keep it in the range of 70-80 kg/cm<sup>2</sup> (g). This task is considered critical as failure can lead to a small break LOCA. ASEP nominal HRA for post-diagnosis actions gives HEP = 0.05 (EF=5). Lower bound HEP=0.01.

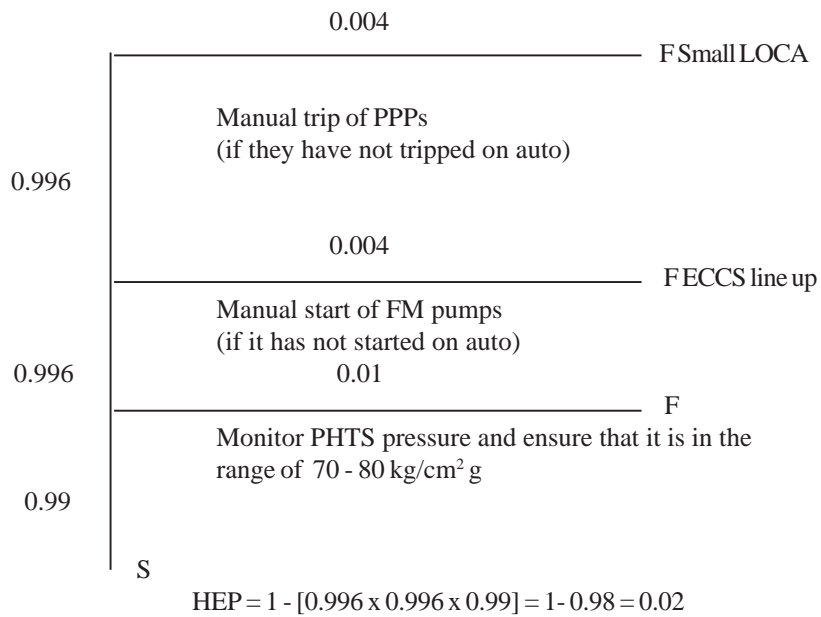
Lower bound HEPs are used here as operators are assumed to have had extensive training including training on simulator.

(c) HEPs for actions (second set)

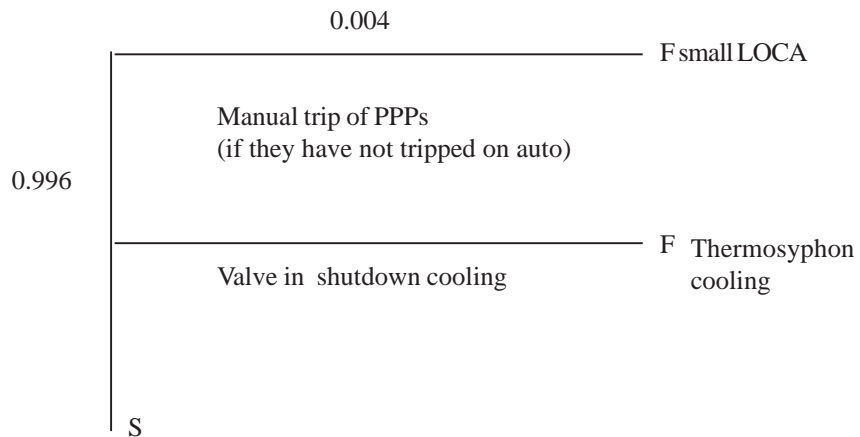
The second set of actions or crew's second operation (Figure 5.2.4-1), is represented by the HRA Event Tree shown in Figure 5.2.4-3. Closing the stuck open IRV by its hand wheel, is an important action to be carried out within 30 minutes. Hence, the HEP associated with this action is expected to be ~0.004. The second action, valving in shutdown cooling is considered to be non-critical, because sufficient time is available and thermosyphon mode of heat transfer is effective, even if the valving in of shutdown cooling system is delayed. Failure probabilities associated with the crew operations are given in the operator action tree (OAT) shown in Figure 5.2.4-1.



**FIG. 5.2.4-1 : OPERATOR ACTION TREE**



**FIG. 5.2.4-2 : HRA EVENT TREE FOR CREW'S FIRST OPERATION**



**FIG. 5.2.4-3 : HRA EVENT TREE FOR CREW'S SECOND OPERATION**

(d) Overall HEP for EOP

Using the operator action tree (Figure 5.2.4-1), the HEP for the EOP is evaluated to be:  
 $(0.99 \times 0.98 \times 0.004) + (0.99 \times 0.02) + (0.01) = 0.0039 + 0.0198 + 0.01 = 0.0337$ ,  
 i.e.  $\sim 3.4 \text{E} - 2$

5.2.4.5 Conclusion

The closure of 'stuck open' IRV manually by handwheel is a very important operation, which is infrequently done. Non-closure of 'stuck open' IRV could lead to opening of safety relief valve of bleed condenser and subsequent small LOCA. HEP for failure of the EOP for inadvertent 'stuck open' failure of IRV of PHTS is evaluated to be  $\sim 0.03$ , i.e. a failure likelihood of 3 in 100.

5.2.5 Human Reliability Analysis Study of the EOP for Station Blackout (SBO) Event in Kaiga Nuclear Power Station

5.2.5.1 Introduction

The occurrence of a simultaneous unavailability of both onsite and offsite AC power is commonly referred to as a station blackout (SBO) event. When events like SBO occur in a NPP, operators realising the event have to carry out the corresponding EOP. Human interactions involved in the execution of an EOP play an important role in determining the course of an event. If errors occur and operators fail to recover from them, the situation can get aggravated and even result in the event turning into an accident. A human reliability analysis study of the EOP can identify the human interactions that are dominant contributors to risk. This would enable designers to implement necessary modifications in procedures and/or develop operator aids to support reliable human performance. In this case study, HRA carried out for the EOP for station blackout (SBO) event in Kaiga NPS is presented.

From the results of PSA Level 1 studies carried out for IPHWRs, it has been observed that accident sequences initiated by Class IV power supply failure and active process water system failure are

significant contributors to core damage frequency. Human interventions in these sequences play an important role as the operator can terminate the accident situation by the appropriate actions as mentioned in the emergency operating procedures.

Simultaneous unavailability of both onsite and offsite AC power supplies will cause all running equipment connected to class IV and class III buses to stop and remain in tripped condition until power is restored. An extended SBO has to be properly handled in order to prevent unacceptably excessive heatup of various reactor and end shield components. The purpose of the EOP for the SBO event is to maintain the reactor in safe shut down state and ensure long term sub-criticality, core decay heat removal and integrity of the containment. SBO is a low frequency event. However, SBO can also occur due to external events like earthquake, storm, flooding or fire.

#### 5.2.5.2 HRA of Emergency Operating Procedure (EOP) for Station Blackout

##### (i) Station blackout event scenario and operator actions

The event scenario and operator action versus time logic for SBO event is shown in Figure 5.2.5-1. The dominant human interactions are as follows.

- (a) Detection and diagnosis of the occurrence of an SBO event
- (b) Manual crash cooldown of primary heat transport system (PHTS)
- (c) Purging of hydrogen in generator casing with CO<sub>2</sub>.
- (d) Taking actions to conserve fire fighting water (FFW).
- (e) Observing continuous fall in steam generator (SG) pressure and opening fire water injection valves to SGs.
- (f) Isolating air supply to main air lock (MAL) and emergency airlock (EAL) and connecting air cylinders to keep seals inflated.
- (g) Injecting fire water into endshields.
- (h) Closing induced draught cooling tower (IDCT) blowdown valves to preserve fire water.
- (i) Reopening fire water injection valves to SGs after air supply failure.

All of these human interactions are important from reactor safety point of view and human reliability quantification is therefore carried out for all the human interactions.

##### (ii) Human reliability quantification

###### Detection and diagnosis of SBO

The occurrence of SBO is accompanied by a large number of unambiguous alarms/annunciations. Annunciation of Emergency Transfer (EMTR) Incomplete prompts the operator that the event is a SBO event. It is therefore a compelling signal. Diagnosis is a holistic process and a single value may be assigned for failure to diagnose a SBO. Diagnosis should, in the worst case, not take more than a minute. In the present case, HEP for diagnosis will be very low and for convenience can be taken to be zero (0).

###### Operator actions

The dominant interactions are quantified using ASEP HRA Procedure. The first action (Manual Crash Cooldown of PHTS) is to be initiated only 6 minutes after the occurrence of SBO, although diagnosis would have been made in less than 1 minute. This is followed by other operator actions as detailed in Figure 5.2.5-1.

###### Screening HRA

Using ASEP Screening HRA, the post-diagnosis actions can be evaluated. Screening Analysis is conservative in estimates of HEPs. Screening HRA makes use of Table 7.3 in Swain [26]. The

table is reproduced in Appendix-6 of this report. The total failure probability is calculated by adding the diagnosis HEP to HEPs for actions. The screening value is estimated to be 0.115. The assessment is given in Table 5.2.5-1. Screening HEPs are indicated in the HRA event tree (Figure 5.2.5-2).

#### Nominal HRA

Since the estimated HEPs in screening HRA are conservative and contribute significantly to core damage frequency, nominal HRA using ASEP is carried out to avoid undue conservatism. Nominal HRA makes use of Table 8.5 in Swain [26]. The table is reproduced in Appendix-6 of this report. The total probability is calculated by adding diagnosis HEP to the HEPs for actions. The nominal HEP value is estimated to be 0.027. The assessment is detailed in Table 5.2.5-1. In the HRA event tree (Figure 5.2.5-2), nominal HEPs are given in parenthesis.

#### 5.2.5.3 Conclusions

HRA studies can contribute to improvement of operational safety as HRA quantitatively assesses the risk involved in the set of important actions that have a significant impact on the event sequence. If the risk involved is high, suitable modifications to procedure and or system may be carried out for actions that are significant contributors to the risk involved. The HEP estimated for the SBO EOP is 0.03. This implies that the likelihood of a failure during the execution of this EOP is 3 times out of 100.

**TABLE 5.2.5-1 : ASSESSMENT OF HEPs FOR SCREENING AND NOMINAL HRA**

<b>Operator Actions</b>	<b>HEP-(S)</b>	<b>Remarks for Screening HRA</b>	<b>HEP-(N)</b>	<b>Additional Remarks for Nominal HRA</b>
1 Detection and diagnosis of SBO event	~ 0	Compelling cue/signal is present. Sufficient time is available for the initiation of the first action.	~ 0	
2 Manual crash cooldown of PHTS	0.01	Post-diagnosis immediate emergency action. The crucial critical task of de-pressurising the steam generators is judged to be committed to memory and a skill based task with a backup written procedure.	0.001	Here, it is also assumed that there is no immediate Recovery Factor (RF) from a second person. This implies that the HEP estimate is conservative.
3 Purging the hydrogen in generator casing by CO <sub>2</sub>	0.05	This is a critical procedural action to be correctly done under moderately high stress. As seal oil pumps are not available there is potential for hydrogen leak and fire. No credit is given for recovery factors.	0.02	Critical procedural action to be correctly done under moderately high stress. The HEP must be adjusted for the effects of other operators and RFs.
4 Taking actions to conserve fire water	0.01	Critical action in the EOP. Judged to be committed to memory, a skill based task that is supported by a backup written procedure	0.001	Here, it is also assumed that there is no immediate RF from a second person. This means that the HEP estimate is conservative.
5 Injecting fire water into SGs	0.01	As above	0.001	As above
6 Connecting air cylinders to keep air lock seals inflated	0.01	As above	0.001	As above
7 Injecting fire water into the end- shields.	0.01	As above	0.001	As above
8 Closing IDCT blowdown valves	0.01	As above	0.001	As above
9 Re-opening the fire water injection valves to SGs after air supply failure (the valves close on air failure)	0.01	As above	0.001	As above

Note : HEP-(S) is screening HRA value and HEP-(N) is nominal HRA value

0 minutes	Detection	<ol style="list-style-type: none"> <li>1. Class IV, III buses under voltage alarm.</li> <li>2. Emergency transfer initiated annunciation.</li> <li>3. Reactor trip on No PCP, turbine generator (TG) trip</li> <li>4. All 3 diesel generators fail to start</li> </ol>
1 minute	Diagnosis	Annunciation - EMTR incomplete (confirms the occurrence of blackout event).
6 <sup>th</sup> minute	Action	<ol style="list-style-type: none"> <li>1. Initiate crash cooldown (hand switch operation).</li> <li>2. Break condenser vacuum and close steam supply to turbine glands and ejectors, to conserve battery power by switching off seal oil and emergency oil pumps.</li> <li>3. Declare SBO. Inform station management and declare plant emergency.</li> <li>4. Initiate H<sub>2</sub> purging in TG by CO<sub>2</sub> and continue to purge.</li> </ol>
7-9 minutes	Action	<p>Crash cooling continues.</p> <ol style="list-style-type: none"> <li>1. Actuate secondary shutdown system (SSS) manually. Liquid poison injection system (LPIS) also comes in if not done earlier.</li> <li>2. Conserve firewater by closing boiler blow down valves and stopping firewater diversion to moderator pumps and ensuring that firewater backup valves to different coolers and heat exchangers are closed.</li> <li>3. Check and confirm that ECCS/D<sub>2</sub>O Injection valves are open, else open them manually from control room</li> <li>4. Switch off supplementary control room (SCR) batteries to conserve battery power.</li> </ol>
10-15 minutes	Action	<ol style="list-style-type: none"> <li>1. Observe SG pressure. Open fire water injection valves when SG pressure = 3 kg./cm<sup>2</sup>.</li> <li>2. Ensure fire water injection to SGs by noting SG level and opening valves.</li> <li>3. Stop seal oil and emergency oil pumps after ensuring TG has come to rest and H<sub>2</sub> is purged out.</li> <li>4. Valve in air cylinder to main air lock (MAL) and emergency air lock (EAL) seals.</li> <li>5. Inject fire water into endshields by connecting fire hose to line in reactor auxiliary building (RAB).</li> </ol>

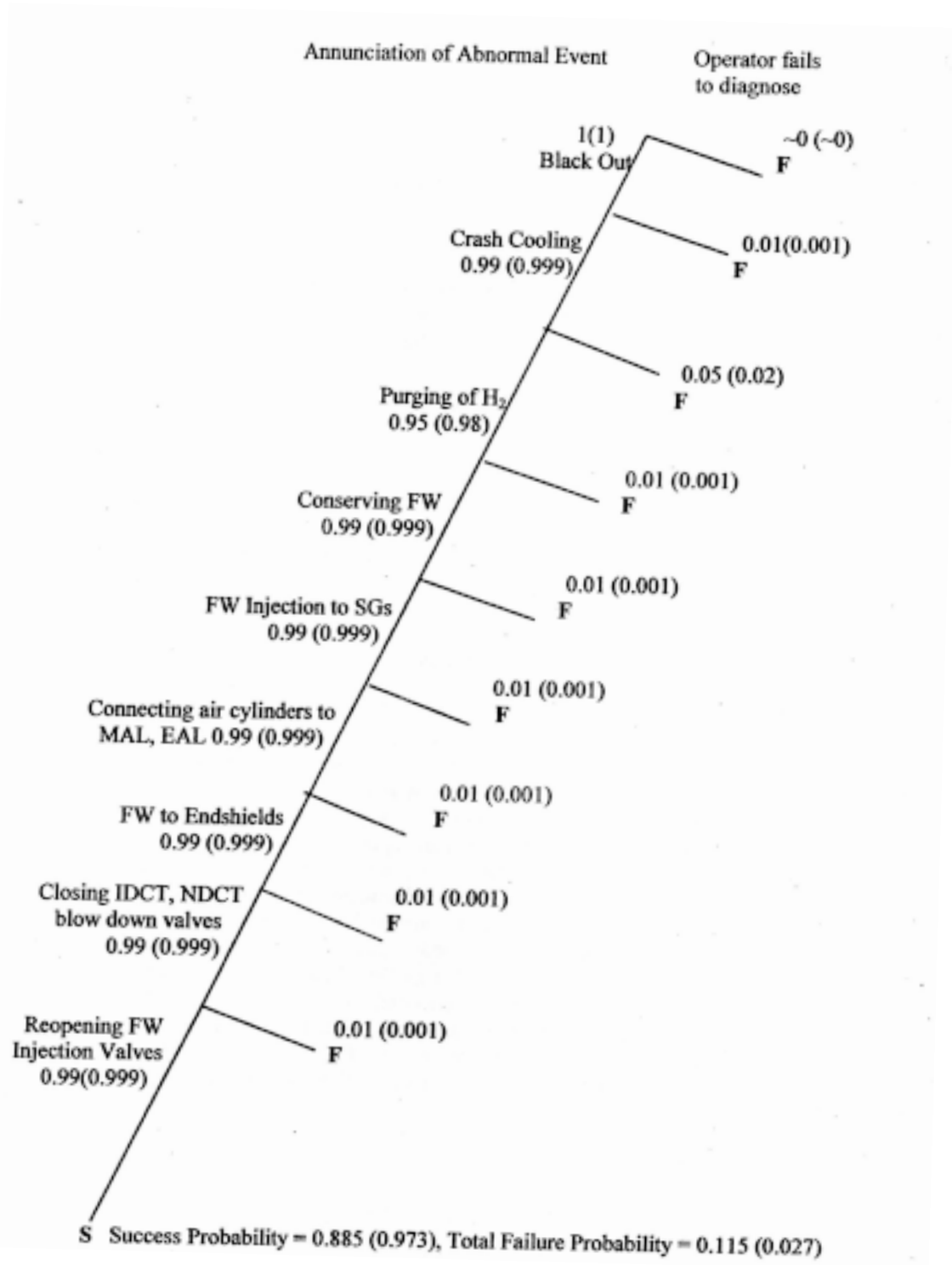
**FIGURE 5.2.5-1 : OPERATOR ACTION VERSUS TIME DIAGRAM FOR SBO EVENT (Figure continues on next page)**

16-30 minutes	Action	<ol style="list-style-type: none"> <li>1. Ensure fire water injection into SGs continues.</li> <li>2. Control SG Level by throttling fire water valves to SGs.</li> <li>3. Get RB radiation level on radiation data acquisition system (RADAS).</li> <li>4. Isolate air supply to MAL and EAL. Connect air cylinders to keep seals inflated, if not done earlier.</li> <li>5. Close IDCT, NDCT blow down valves, if not done earlier.</li> <li>6. Arrange for torches and multimeters with power packs</li> <li>7. When D<sub>2</sub>O accumulator low level is reached close injection valves to avoid N<sub>2</sub> ingress in core.</li> </ol>
30 minutes-1 hour	Action	<ol style="list-style-type: none"> <li>1. Ensure fire water to SGs continues.</li> <li>2. Enter RB after checking radiation level and note down endshield tubesheet temperatures from junction boxes.</li> <li>3. Fire water injection valves to SG will close on air failure. Open them from field.</li> <li>4. Monitor important parameters from secondary control room (SCR) after switching on batteries.</li> </ol>
1 hour-2 hours	Action	<ol style="list-style-type: none"> <li>1. Get report on endshield metal temperature. If it crosses 80° C, ensure fire water flow to endshields at 100 lpm.</li> <li>2. Purge moderator system Helium cover gas.</li> <li>3. Check RB radiation level from radiation data acquisition system/hand monitors.</li> <li>4. Check digital recording system parameters for variation since SBO commenced.</li> </ol>
2 hours- till the restoration of class III, IV power	Action	<ol style="list-style-type: none"> <li>1. Ensure fire water injection to SGs continues.</li> <li>2. Ensure fire water is flowing out of endshield expansion tank.</li> <li>3. Keep watch on diesel oil in day tank of operating firewater pumps and replenish if required.</li> <li>4. Keep monitoring important reactor parameters.</li> <li>5. Carry out radiological survey.</li> </ol>

Class III and Class IV power restored

**FIG. 5.2.5-1 : OPERATOR ACTION VERSUS TIME DIAGRAM FOR SBO EVENT**





Note: All failure probability values for Screening and Nominal HRA are as per Table 5.2.5-1. Nominal values are in parenthesis.

**FIGURE 5.2.5-2 : POST INCIDENT SCREENING AND NOMINAL HRA EVENT TREES**

## 5.2.6 Human Reliability Analysis Case Study of the Total Power Failure Due to Fire Incident in Narora Atomic Power Station-1

### 5.2.6.1 Event Description

A total power failure due to fire occurred at Narora Atomic Power Station (NAPS) Unit-1 on March 31, 1993. The fire was caused by ignition and burning of hydrogen and lube oil from ruptured lines after a catastrophic turbine blade failure. Cables in the area caught fire and a total blackout resulted. The chronological record of alarm registration and main events and actions in NAPS-1, after turbine trip at 03 hours 31 minutes 40.004 seconds, is given in Figure 5.2.6-1. Time T=00 refers to the time of turbine trip registration. All events are sequenced with respect to this time as reference. An HRA study carried out for this real event is detailed herein.

#### (i) Event outline

NAPS Unit-1 was operating at 185 MWe. Unit-2 was in shutdown state with the PHT System in cold and pressurised condition. At time 3:31:40:004 (T=00) on 31.3.93, turbine of Unit-1 tripped. Several alarms registered at the same time on control room panels for turbine and auxiliaries and the parameters, which initiated the turbine trip, could not be separately identified. An explosive sound, ground vibrations and visible fire cued control room operators to the seriousness of the event.

#### (ii) Immediate actions - automatic and manual

Turbine trip initiated the opening of unit transformer breaker, main generator breaker and field breaker and closure of the start-up transformer breaker. A reactor setback on 'auto' was initiated as per the logic. On seeing the magnitude of the fire, the reactor was tripped manually at T=38 seconds. Within a few minutes, several trips and alarms registered in control room, due to burning of cables and tripping of control motor generator sets. PHT System cooldown was initiated by manual opening of small atmospheric steam discharge valves (ASDVs), but on observing the gravity of the situation, a crash cooldown was started at T = 5 minutes 48 seconds, by manually opening the large ASDVs. The secondary shutdown system (SSS) got actuated on the initiation of crash cooldown, as per logic. There was a complete loss of power supply in Unit-1 (T=7 minutes 40 seconds), including loss of Class I and Class II supplies. Senior plant management personnel were informed. A plant emergency was declared from the Unit-2 side of control room (T=8 minutes) on the public address system. Prior to the total loss of power, control room staff noted that primary heat transport system (PHTS) pressure was 50 kg/cm<sup>2</sup>(g) and fuelling machine supply pump was in operation. All PHTS pumps tripped at T=6 minutes 47seconds.

#### (iii) Incident mitigating operations

Fire fighting could be started in the area below the generator within about 20 minutes, using water from the fire hydrant and a fire tanker. There was no difficulty in using water even for cable fire, as the power supply failure was total. Two diesel engine driven firewater pumps had already been started at T=10 min. by the operating crew. The third firewater pump was under maintenance. Major fire was put out in about 1 hour 30 minutes and the fire was completely extinguished in about 9 hours. Fire tenders from nearby places were also summoned for additional support. Members of the Advisory Committee for Accident Management reached the site in about 30 minutes after the initiation of the incident and took charge of the situation. The guard house at the entrance of turbine building was designated as control centre for guiding further operations.

#### (iv) Other critical operations

A group of staff members were sent to the boiler room (T = 1 hour) for checking the status of valves in the firewater backup circuit connected to the steam generators. These valves were

opened manually upto 50%. With this, the availability of heat sink for removal of core decay heat was established. Till this time, the inventory of water present in the steam generators continued to provide the heat sink for decay heat removal by thermosyphon in the PHT system. Borated heavy water was added to the moderator through gravity addition of boron system (GRABS), as per the emergency operating procedure for (EOP), to ensure adequate long-term sub-criticality. The GRAB System in IPHWR has been specially engineered to cater to the station blackout (SBO) condition. Up to the time of tripping of the PHT System pumps (T = 6 minutes 47 seconds), core heat removal was through forced circulation in the system. Subsequently, core decay removal was due to the flow coast down followed by natural circulation. The efficacy of thermosyphon cooling, experimentally demonstrated during plant commissioning was further reconfirmed during the fire incident.

(v) Radiation survey and end shield cooling

A quick survey outside the reactor building, using portable radiation survey instruments (T=30 min.) had shown normal radiation levels and no release of activity. Radiation surveys carried out inside the secondary containment (T=2 hours) and inside the primary containment (T=4 hours) showed normal values. Operating personnel were therefore allowed to enter primary containment. Firewater was connected to the suction side of end shield cooling system pumps to cool the end shields (T=5 hours 30 minutes). One of the end shield cooling pumps could be started only after 32 hrs.

(vi) Auxiliary power system recovery and establishment of shutdown core cooling

During the incident, station diesel generators (DGs) on Unit-1 side had started automatically, but tripped due to loss of control power supply. One DG (No. 3) common to both units was started (T=6 hours) and one of the Class III buses could be charged. Thereafter, essential equipment was started one after another in a planned manner. One of the shutdown cooling pumps was started at around T=17 hours. The station blackout condition can thus be considered to have lasted for a period of about 17 hours. Plant emergency was lifted at 22.45 hours (T=19 hours).

The incident resulted in a complete station black out, including loss of Class I and Class II power supply, which lasted for about 17 hours. The cable fire and ineffective fire barriers/fire retarding provisions, together with the inadequate physical separation in redundant safety related cables, was the main cause of the extended station black out and consequent degradation of several safety systems.

(vii) Damage caused

There was extensive damage to the TG and its accessories, bus ducts and excitation cabins. The fire damaged many cables, the Emergency Transfer Relay (EMTR) panels and the Line, Transformer and Generator (LTG) panels. Smoke entering the control room through the control equipment room (CER) and air supply diffusers, forced the control room staff to vacate the control room within 8-10 minutes of the turbine trip. An attempt was made to take charge of the situation from the emergency control room, but it was observed that no indications were available on Unit-1 panel, due to the loss of control power supply. Indications for Unit-2 were however available. The main control room could be reoccupied only after about 13 Hours.

#### 5.2.6.2 Event Rating and Consequences of the Incident

On the international severity scale, the event was classified as a serious incident and rated at level 3 on the International Nuclear Event Scale. Several systems important to plant safety were degraded, including automatic liquid poison addition system (ALPAS), emergency heavy water injection, PHTS circulation including shutdown cooling and auxiliary feed to boilers. During the incident, control room had to be vacated due to ingress of smoke. In the emergency control room, no indications were available on Unit-1 panel due to loss of control power supply. Some of the important parameters had to be directly

measured from field. An emergency operating procedure (EOP) for a total power failure event was prepared after the occurrence of this incident.

### 5.2.6.3 Human Reliability Analysis of the Incident

(i) HRA event tree

The HRA event tree for the total power failure due to fire incident in NAPS -1 is shown in Figure 5.2.6-1.

(ii) Quantification of human reliability

quantification of human reliability has been carried out in two ways. a. Using the human cognitive reliability (HCR) model and b. Using handbook data. The main human interactions involved during the course of the incident are as detailed below.

- Detection and diagnosis

The occurrence of fire in turbine building and the explosive sound were the cues to the operator regarding the seriousness of the situation. These cues led him to (i) trip the reactor and (ii) initiate crash cool down. Subsequent occurrence of total power failure at around 8 minutes into the incident was an additional cue.

- Actions in station blackout

The actions to be taken in a station blackout situation are:

- Starting the diesel engine driven fire-fighting pumps.
- Opening two fire water injection valves to steam generators
- Ensuring PHT system integrity for assuring continued core cooling.
- Ensuring 'sub-critical' state of the reactor core.

The time available (t) for injecting FW into SGs is about 60 minutes and this is based on the inventory in the SGs. Hence, all the above actions need to be taken within an hour.

(iii) Quantification using human cognitive reliability (HCR) model

The nominal time for detecting the occurrence of the serious fire event, taking immediate emergency action to trip the reactor and initiate crash cooldown, and then carrying out the actions required in a SBO event, viz., starting the two diesel engine driven fire fighting pumps and opening the two fire water injection valves to SGs, is taken to be 20 minutes. At NAPS, the operators carried out all these actions well within this nominal time.

Performance shaping factors (PSFs)

In Indian PHWRs, the operator is well trained. Hence the PSF for operator experience,  $K_1 = 0.22$ . Considering the situation to be one of grave emergency, the PSF for stress level,  $K_2 = 0.44$ . The factor for MMI is considered to be inapplicable, as the situation involved total power supply failure, which rendered the MMI unusable. So the PSF for quality of operator-plant interface,  $K_3 = 0$

The median time of 20 minutes adjusted for the PSFs,

$$T_{1/2} = 20 \times (1-0.22) (1+0.44) (1+0) = 22.46 \text{ minutes.}$$

$$\text{The normalised time } t/T_{1/2} = 60/22.46 = 2.67$$

The actions are rule based. Hence the HCR correlation coefficients are  $A_i = 0.601$ ,  $B_i = 0.6$ ,  $C_i = 0.9$ .

P(t) the crew non-response probability in time t is given by:

$$P(t) = \exp - [(t/T_{1/2} - B_1)/A_1]^{C_1}$$

For the given situation P(t) is calculated to be = 0.048

Thus, crew non-response probability (HEP) =  $4.8 E - 2 \sim 5 E - 2$ .

(iv) HRA quantification using handbook data.

As above, the total time taken to diagnose the event and carry out the required actions is taken to be 20 minutes. The diagnosis time (Td) is taken to be 6 minutes (crash cooldown to be initiated by 6 minutes) and the action time (Ta) is 14 minutes.

HEP for diagnosis

For a diagnosis time Td of 6 minutes, the nominal diagnosis curve gives HEP (Lower Bound) as equal to 0.03. The lower bound value has been chosen because of the unambiguous and compelling signals pointing to a serious total power loss (due to fire) event.

HEPs for actions

The actions involved are (a) Starting of diesel driven pumps and (b) Opening of the fire water injection valves to SGs.

(a) Starting of diesel driven pumps.

The sub-tasks involved with associated HEPs and the handbook tables from which the data has been sourced are given in Table 5.2.6-1.

**TABLE 5.2.6-1 : HEPs OF SUB-TASKS**

	<b>Sub-task</b>	<b>HEP</b>	<b>Table: Item</b>	<b>Remark</b>
1.	Starting the diesel engine	0.001	20 – 12: 3	For error of commission in operating manual controls arranged in well delineated functional groups.
2.	Observing whether rated speed has been attained	0.001	20 – 11: 2	For error of commission in check-reading analog meter with easily seen limit marks.
3.	Opening the pump discharge valve	0.001	20 – 12: 3	For error of commission in operating manual controls arranged in well delineated functional groups.
4.	Checking the downstream pressure gauge	0.001	20 – 11: 2	For error of commission in check-reading analog meter with easily seen limit marks.

As the fire fighting pumps are tested weekly, the operator is experienced in carrying out this task. The stress level is considered to be only moderately high as the immediate emergency actions of manual trip and crash cooldown have been successfully carried out. Hence, a stress factor of 2 is considered (From Table 20 – 16: 4 – Modification of estimated HEPs for effect of stress for step by step task). Also, following ASEP, as the action is supervised, the recovery factor is taken to be 0.1.

From the above, HEP (Pump) =  $0.004 \times 2 \times 0.1 = 8 E - 4$ . HEP contribution for starting of two pumps would be  $2 \times 8 E - 4 = 1.6 E - 3$ .

Thus  $HEP(\text{Pumps}) = 1.6 \text{ E} - 3$ .

- (b) Opening of fire water injection valves to steam generators.

Probability of failure to open one valve is 0.001 (Table 20 - 12: 3 - For error of commission in operating manual controls arranged in well delineated functional groups). Since the action is not frequently carried out, this HEP is conservatively increased to 0.005. As in the case for pumps, a stress factor of 2 is considered. So  $HEP(\text{Valve}) = 1 \text{ E} - 2$ . For two valves, the HEP contribution for valve operation,  $HEP(\text{Valves}) = 2 \text{ E} - 2$ . Operators have enough time available to check that PHT system is intact and that core is being cooled by thermosyphoning. So the HEPs for these checks are considered to be negligibly small.

$$HEP(\text{Actions}) = HEP(\text{Pumps}) + HEP(\text{Valves}) = (1.6 \text{ E} - 3) + (2 \text{ E} - 2) = 2.16 \text{ E} - 2 \sim 2.2 \text{ E} - 2 = 0.022.$$

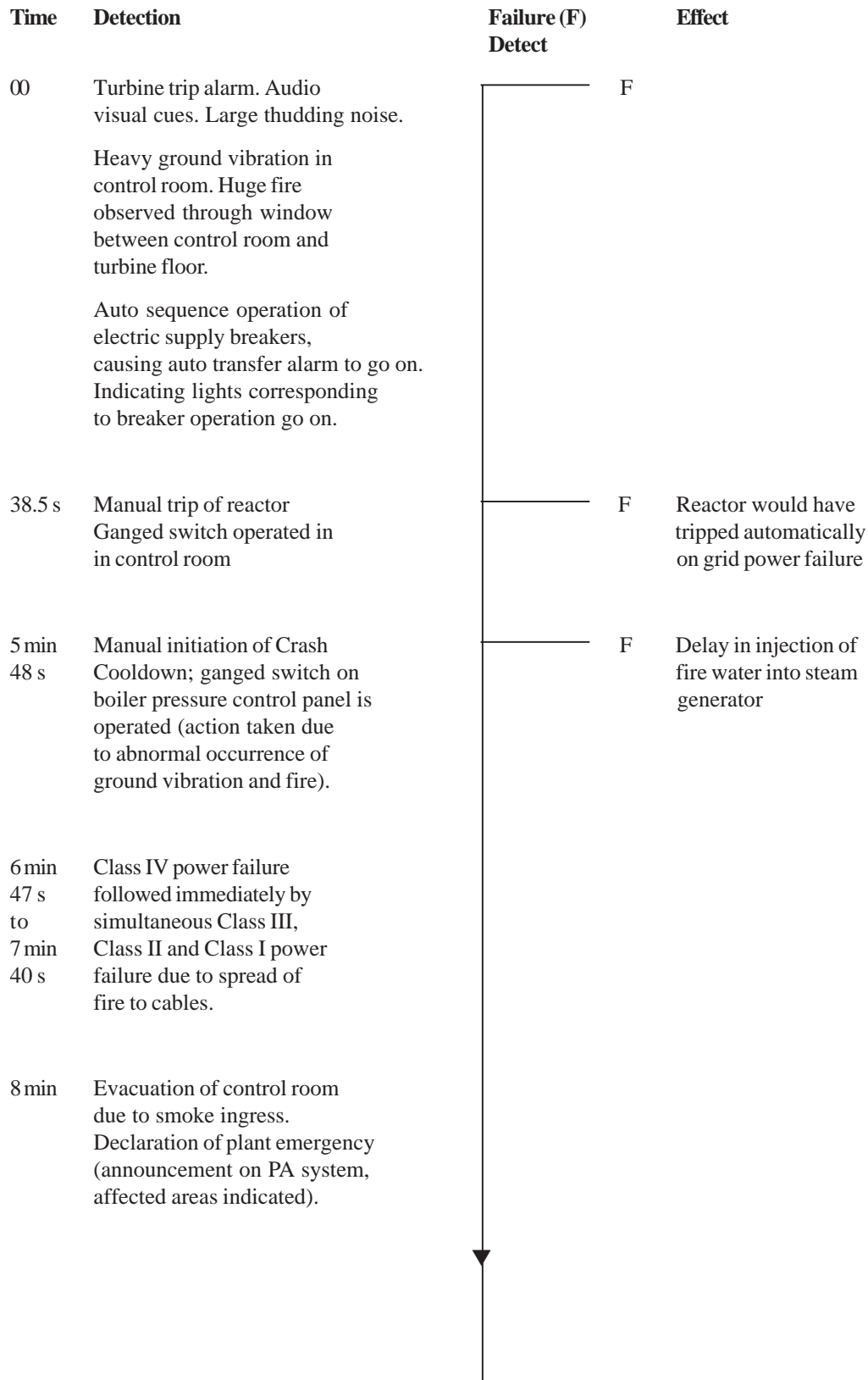
Therefore the total HEP is

$$HEP(\text{Diagnosis}) + HEP(\text{Actions}) = 0.03 + 0.022, \text{ i.e. } 5.2 \text{ E} - 2 \sim 5 \text{ E} - 2.$$

#### 5.2.6.4 Concluding Remarks

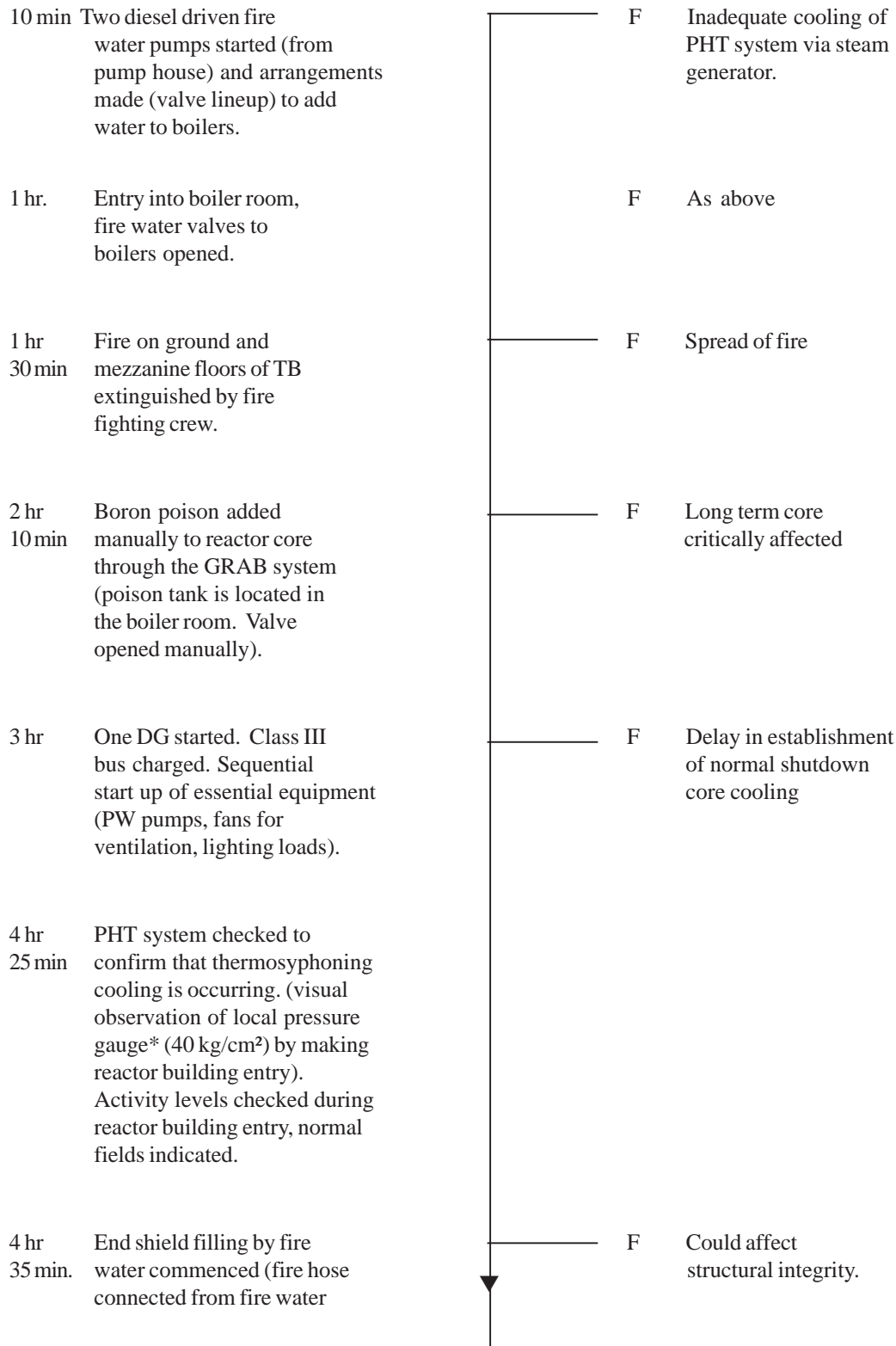
The power failure due to fire incident at NAPS unit I was serious in nature. However, the timely action in promptly shutting down the reactor, cooling down immediately and subsequently taking steps to ensure prolonged reactor sub-criticality and continued core cooling, resulted in maintaining the unit in a safe state, despite seventeen hours of total station blackout. The incident confirms the importance of the extensive training that is imparted to operators.

Human reliability analysis has been carried out using two different methods, the HCR method and the Handbook method. The human reliability quantification gives an HEP in handling the SBO event of the order of  $5 \text{ E} - 2$  in both cases. In other words, the likelihood of a human failure in event diagnosis and performance of post-incident actions is 5 in 100.



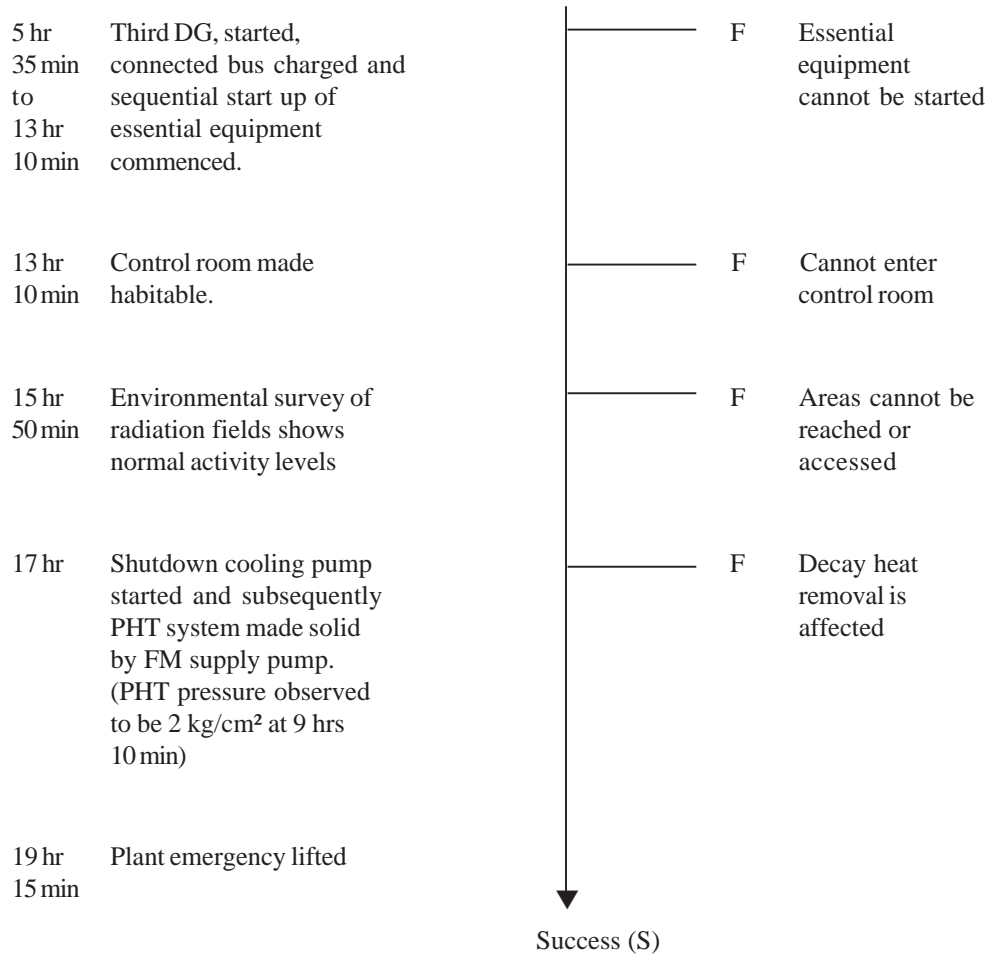
**FIGURE 5.2.6-1: HRA EVENT TREE**

**FIGURE 5.2.6-1: HRA EVENT TREE (CONTD.)**





**FIGURE 5.2.6-1: HRA EVENT TREE (CONTD.)**



\* Precision Pressure Gauges are provided on 107300 floor level in reactor building, mounted on 6070 panels for south and north side header pressure measurement.

## 5.2.7 Quantitative Human Reliability Analysis of an Accident Management Task in PWR Using Success Likelihood Index Methodology (SLIM)

### 5.2.7.1 Preamble

The aim here is to examine the quantitative human reliability analysis of an accident management task in a nuclear power plant. For this purpose, a paper on the subject, entitled 'Cognitive Reliability Analysis of Accident Management Tasks using HRMS and SLIM Methods' by Jaewhan Kim et al, published in 1998, in the Final Report of IAEA CRP on Collection and Classification of Human Reliability Data for Use in PSA [12], was studied. Since the focus here is on the various aspects of application of a HRA method that has been described in this technical document, only the portion on application of SLIM to human reliability analysis, is extracted and reproduced below. The other method human reliability management system (HRMS), which is discussed in the paper, is not considered here. The excerpts on application of SLIM reproduced here are followed by observations on the HRA study, by the author of this technical document.

### 5.2.7.2 Excerpts from 'Cognitive Reliability Analysis of Accident Management Tasks using HRMS and SLIM Methods', Jaewhan Kim et al, Final Report of IAEA CRP on collection and classification of human reliability data for use in PSA, 1998 [12].

#### I. Introduction

Accident management tasks contained in the accident management procedure (AMP) comprise mostly human cognitive tasks such as monitoring of instruments, identifying plant state, selection of an appropriate strategy, evaluation of the positive and negative effects relevant to the strategy and decision-making on whether to implement the strategy or not. The qualitative assessment (of accident management tasks) refers to the identification of human error causes and error types predictively by analysing relevant tasks and the given situation. The quantitative assessment calculates the frequency of human error occurrence.

SLIM is selected for quantitative assessment because SLIM is considered more appropriate than other methods for the cognitive error assessment. SLIM does not give strict guidance and this can be advantageous as it enables the analyst to select appropriate PSFs as per the task characteristics, in his/her own judgement.

The study assesses some task procedures of the reactor cavity flooding tasks.

#### II. Description of accident management tasks

The task associated with the reactor cavity flooding strategy selected for the case application is adapted from Severe Accident Guideline - 4 (SAG - 4) in Severe Accident Management Guidance (SAMG), INJECT INTO CONTAINMENT, from among the eight SAGs.

The task procedures were divided into 3 tasks as follows.

- Task 1 : Decide whether to refer to the SAG, using the diagnostic flow chart (DFC)
- Task 2 : Identify the availability of relevant systems for implementation of the strategy in SAG - 4.
- Task 3 : Decide whether to implement the strategy by evaluating the negative impacts of implementation of the strategy and the consequences of NOT implementing the strategy.

A part of the results of the application to the Task 3 is shown. Task 3 consists of the following task steps in summary.

Summarised task steps in task 3

- (1) Evaluate the negative impacts of implementation of the strategy
- (2) Evaluate the mitigating actions for the negative impacts.

- (3) Evaluate the consequences of not implementing the strategy.
- (4) Decide whether to implement the strategy by evaluating the negative impacts from the implementation of the strategy and the consequences of not implementing the strategy.

Note : The above four task steps have been denoted as task procedures 1.1, 2.1, 3 and 4, later in the analysis

### III. Qualitative assessment

This section is not included in the excerpt given here.

### IV. Quantitative assessment.

#### (1) Description of SLIM

SLIM, developed by Embrey in 1984, is based on the structured elicitation of expert judgement. It consists of the following steps.

- (i) Select PSFs that might affect task performance
- (ii) Assign relative importance/weight  $w_i$  to each PSF
- (iii) Evaluate its rating  $r_i$ , i.e. how favourable/unfavourable the PSF is to task performance.
- (iv) Calculate  $SLI = \sum w_i \cdot r_i$
- (v) Calculate human error rate (HER) using the following relation

$$\log_{10}(\text{success rate}) = \log_{10}(1 - \text{HER}) = a \cdot \text{SLI} + b \quad \dots (1)$$

where the two coefficients a and b can be obtained by evaluating calibration tasks that have known or generally accepted error rates.

There has been a modified form of SLIM called failure likelihood index methodology (FLIM). The FLIM calculates a failure likelihood index (FLI) rather than an SLI. In FLIM, assigning the relative weight has the same meaning as in SLIM, however evaluating the rating of each PSF for potential for failure rather than the potential for success. Using FLI, equation (1) can be modified as follows.

$$\log_{10}(\text{failure rate}) = \log_{10}(\text{HER}) = a' \cdot \text{FLI} + b' \quad \dots (2)$$

PLG (Pickard, Lowe and Garrick) Inc. provided guidance to help human reliability analysts decide weights  $w_i$  and ratings  $r_i$  for use in low power and shutdown conditions. According to the guidance, the relative weights are categorised into four classes such as 0 (Insignificant), 1 (Low), 2 (Normal) and 4 (High) and the ratings are categorised into 11 classes from 0 to 10. To help the analysts' judgement, guidance or description corresponding to each class is provided.

In the study, the guidance of PLG was used for evaluating weights and ratings of PSFs.

#### (2) Application to accident management procedures

##### Selection of PSFs

Task-3 primarily consists of the cognitive activities of state identification, evaluation and decision-making. Eight PSFs are selected as shown below. The first seven of these are typically adopted in other HRA assessments. The last, "Plant Policy", is added here, as it can be a dominant factor to affect decisions required in emergency operation or accident management situations. The description of each PSF is as follows.

Preceding and concurrent actions: Existence of preceding or concurrent actions that help or hinder the current task

Adequacy of time : Time available relative to the time to complete the action.

Information and instruments : Availability of instruments, the quality of information (direct or indirect source, provision of computational aids, reliability of information).

Procedures : Availability of procedures; level of detail; procedures for specific actions.

Competence : Extent of training (classroom and simulator). Experience with respect to specific actions.

Task complexity : Level of cognitive processing (SRK), the multiplicity of requirements for success in task performance (e.g. sequencing and coordination of tasks, communication and coordination between multiple operators, and the influence of multiple objectives).

Stress : Psychological (say, fear) or mental (say, alertness) state of operators in a given environment or situation.

Plant policy : Degree of preference for or rejection of certain strategies (this is regarded as an important contributor when decision making is required).

- (3) Evaluation of weights, ratings and FLIs for each PSF for task procedures

Table 5.2.7-1 shows the weights, ratings and FLIs of each PSF for the task procedures.

**TABLE 5.2.7-1 : WEIGHTS, RATINGS AND FLIs FOR PSFs**

Task Procedure-TP	1.1			2.1			3			4		
PSF	w <sub>i</sub>	r <sub>i</sub>	FLI <sub>i</sub>	w <sub>i</sub>	r <sub>i</sub>	FLI <sub>i</sub>	w <sub>i</sub>	r <sub>i</sub>	FLI <sub>i</sub>	w <sub>i</sub>	r <sub>i</sub>	FLI <sub>i</sub>
Prcdg. Conc.Actions	0.11	3	0.33	0.09	3	0.27	0.11	3	0.33	0.09	3	0.27
Adequacy of Time	0.11	3	0.33	0.09	3	0.27	0.11	3	0.33	0.09	3	0.27
Info and Instrmntn.	0.22	5	1.10	0.18	2	0.36	0.00	-	0.00	0.00	-	0.00
Procedures	0.22	1	0.22	0.18	5	0.90	0.22	5	1.10	0.18	9	1.62
Competence	0.11	8	0.88	0.18	8	1.44	0.22	8	1.76	0.18	8	1.44
Task Complexity	0.11	5	0.55	0.18	7	1.26	0.22	7	1.54	0.18	8	1.44
Stress	0.11	8	0.88	0.09	8	0.72	0.11	8	0.88	0.09	8	0.72
Plant Policy	0.00	-	0.00	0.00	-	0.00	0.00	-	0.00	0.18	5	0.90
FLI = $\sum w_i \cdot r_i =$	4.18			5.04			5.72			6.48		

Task Procedure 1.1 is to evaluate the negative impact of ‘insufficient injection source’ by integrating two subtasks 1.1.1 and 1.1.2 comprising activities like information collection and identification. For successful completion of the given procedure, information and instruments is considered a more important factor than other PSFs. The influence levels of other PSFs are about the same. For evaluation of the rating of each PSF it is assumed the procedure is clearly described and there is indirect information to be able to identify core reflooding event. From the results of FLI<sub>i</sub>, information and instruments turned out to be the most dominant contributor to the failure likelihood.

Task Procedure 2.1 evaluates the mitigating actions for the negative impact of ‘insufficient injection source’. Since this requires high level cognitive functions of operators,

information and instrumentation, task complexity, competence and procedures are considered to be important factors. It is assumed that the procedure is available, but requires some interpretation depending on the scenarios and situations, training is carried out as an optional item annually or biannually, and task complexity is due to the knowledge-based response required. Calculation of  $FLI_i$  shows that competence and task complexity are dominant contributors to failure likelihood.

Task procedure 3 interprets the consequences of not implementing cavity flooding. This procedure belongs to the knowledge-based response class like task procedure 2.1. Information and instruments are excluded because it is not required for the action. Procedures, competence and task complexity are considered important factors. The results for  $FLI_i$  are similar to that for TP 2.1.

Task procedure 4 makes a decision on whether to implement the reactor cavity flooding strategy by comparing the negative impacts and the consequences of not implementing the strategy. Depending on the scenarios, the decision can be made prior to or at this step. In the present study, it is assumed that the decision is made at this step because of high uncertainty on the phenomena. Plant policy is added as one of the most important factors to affect making a decision, with other PSFs such as procedures, competence and task complexity. Rating for plant policy scales from 0 for dependence on the procedure to 10 for strong/total rejection of the cavity flooding strategy. In the present study, a rating of 5 is used, implying that the plant has some rejection policy on the reactor cavity flooding strategy.

The results of  $FLI_i$  show that procedures, task complexity and competence contribute to failure likelihood in that order. There are however limitations to improving the level of detail of task procedures and training operators more effectively due to lack of knowledge and uncertainty on the phenomena.

(4) Quantification of human error rates

Quantification of human error rate (HER) of each task procedure can be accomplished by searching for calibration tasks having the same profile of PSF weights as that of each task procedure, and of which HERs are known or generally accepted. As shown in the table, each task procedure has a different profile of PSFs. Therefore we should find four pairs of calibration tasks and each pair should have the same profile of PSFs. And then,  $FLI_i$ s are evaluated for all calibration tasks in the same manner as in the task procedures.

On the other hand, most of the errors related to each task procedure are cognitive errors. Calibration tasks for which cognitive reliabilities are known or generally accepted are too few.

V. Summary and conclusions

This section is not included in the excerpt given here.

5.2.7.3 Observations of the Author of this Technical Document

- (a) In the paper, a variant of the original SLIM by Chien et al [2] is used. This variant is discussed in Chapter 3 of the Technical Document. The original SLIM is often referred to as SLIM-MAUD after the interactive computer software supporting elicitation and organisation of expert opinion within the framework of SLIM. In the paper by Kim et al [12], the variant is referred to as PLG-SLIM after the consultancy that proposed it.
- (b) The main differences between SLIM MAUD and PLG SLIM are given in Table 5.2.7-2.

**TABLE 5.2.7-2 : DIFFERENCES BETWEEN SLIM-MAUD AND PLG SLIM**

Aspect	SLIM-MAUD	PLG-SLIM
Formulation of the judgement	Success space, in terms of the success likelihood index (SLI).	Failure space, in terms of failure likelihood index (FLI)
Selection of PSFs	Task experts select dominant PSFs	A set of representative PSFs is used. Experts weigh the impact of these core PSFs.
PSF rating scales	An 'ideal point' on each PSF scale (0-10) is selected by each of the judges and ratings are rescaled about this point.	The PSF scale monotonically increases towards increased failure likelihood (a rating of 10 is indicative of the 'worst' situation). Scaling guidance is available for each of the PSFs in the standard set.

Salient points

- Experts are generally better at judging increased failure rate rather than increased success rate, and particularly the low failure rates. The formulation in terms of failure likelihood index (FLI) generally employed reflects this finding.
  - With SLIM-MAUD, the experts select and use the dominant PSFs relevant to the situation. PLG-SLIM, which comes with a set of representative or core PSFs, applies a profile of PSFs, some of which are dominant. The set of representative PSFs is considered to be comprehensive for full power operation in a NPP, since they appear with a high degree of regularity. In other operating situations, say low power or shutdown, other PSFs may be required.
  - For the PSF rating scales, the original approach involved an 'ideal point' selected by the experts on the 0-10 scale, which leads to rescaling based on the distance from the ideal point. In PLG-SLIM, the scales have been defined to be uniformly increasing towards greater failure likelihood, with a rating of 10 always the worst. To improve the consistency in scaling by experts working separately, scaling guidance is provided in the form of descriptions for points on each PSF rating scale. The scaling guidance covers all seven representative PSFs. For example, for the training and experience PSF, 0 is assigned if action is normally carried out during plant trip situations, 1 if action is repeatedly carried out during simulator training, 7 if action is a non-routine action included in annual training and 10 if action is unfamiliar/contrary to normal operational practice.
- (c) In the HRA study discussed in the paper, the authors have made use of the guidance provided by PLG to help assign weights and ratings of PSFs for use in low power and shutdown situations. The relative weights are categorised into four importance classes: 0 for insignificant, 1 for low, 2 for normal and 4 for high. These weights are normalised as per practice by dividing the weight assigned by the sum of the weights. This normalization can be seen from the weight values entered into Table 5.2.7-1.
- (d) In the accident management situation considered in the paper, the authors in addition introduce plant policy as a PSF that is important in the making the decision to implement or not implement cavity flooding, by comparing the negative impacts of implementing the task with the consequences of not implementing the task. The PSF is assigned a rating of 5 as plant management has reservations with regard to the implementation of the strategy. This is contrary to what is generally accepted, in that plant policies and

procedures are meaningful only when they are strictly enforced. It is likely that this uncertainty with regard to the implementation of the cavity flooding strategy arises on account of the uncertainty of phenomena, uncertainty with regard to the negative impacts of implementation and also uncertainty in respect of the consequences of not implanting the strategy.

(e) Calibration - A central issue in SLIM based HRA.

- Failure likelihood index (FLI) is transformed into probability by selecting anchor values and using a calibration equation. The anchor values employed as upper and lower bounds on failure probabilities are to be provided by the human reliability analyst.
- Ideally, calibration in SLIM, whatever be the variant, is based on tasks with 'known' HEPs. Because of the scarcity of such tasks, in particular in the context of emergency operation in NPPs where the empirical base is limited, studies have used HEP values of similar tasks from other PSAs, for the calibration. An alternative is to derive calibration values using quantitative HRA methods.
- Although two calibration points are often used, a regression based on a larger number of points would increase confidence in the calibrated FLI-HEP relationship.
- For lack of better data many of the HRA studies using SLIM employ values from THERP handbook data. In the paper, the FLIs for the tasks have been calculated but human error rates have not been worked out. The authors mention that there is a paucity of data that can be used as reference, i.e. calibration tasks required to quantify cognitive reliability. In each task procedure most of the actions during accident management situations involve cognitive activities, such as monitoring instruments, identifying plant state, selection of an appropriate strategy, evaluation of positive and negative effects relevant to the strategy and decision making on whether to implement the strategy or not.

(f) The calculated values of FLIs given in Table 5.2.7-1 are in error. The values are 4.29 for 1.1, 5.22 for 2.1, 5.94 for 3 and 6.66 for 4 and not 4.18, 5.04, 5.72 and 6.48 as given.

5.2.8 Qualitative Analysis of Accident Management Task in PWR Using Cognitive Reliability and Error Analysis Method (CREAM)

5.2.8.1 Preamble

The aim here is to examine the qualitative analysis of an accident management task in a nuclear power plant. For this purpose, a paper on the subject, entitled 'Evaluation of three Human Error Analysis Methods through Application to Accident Management Tasks, by Jaewhan Kim et al, published in 1998, in the final report of IAEA CRP on collection and classification of human reliability data for use in PSA [12], was studied. The intention here is to illustrate the application of a second generation HRA method that has already been described in this technical document. Therefore, only the portion on the application of cognitive reliability and error analysis method (CREAM) in qualitative analysis, is extracted from the paper and reproduced below. The other two methods discussed in the paper are not considered here. The excerpts on application of CREAM reproduced here are followed by observations by the author of this technical document.

5.2.8.2 Excerpts from 'Evaluation of three Human Error Analysis Methods through Application to Accident Management Tasks', Jaewahn Kim et al, final report of IAEA CRP on collection and classification of human reliability data for use in PSA, 1998 [12].

## I. Introduction

Conventional HRA methods such as THERP, HCR and SLIM have focused on quantitative assessment of the observable aspects of human tasks. Due to this limitation, even after completion, HRA did not give any specific recommendations for error reduction. In addition, HRA without error analysis is likely, not only to give estimates lower than what they really are, but also to omit the important consequences to system or environment.

Human error assessment identifies the kinds of human error (External Error Mode/EEM), why they occur (error causes or performance shaping factors/PSFs) and how they occur (Psychological Error Mechanisms/PEMs). THERP, known as a representative HRA method, classifies EEMs into errors of omission (EEO) and errors of commission (EOC). But, with only these two EEMs, it is difficult not only to identify the underlying mechanisms of human error but also to obtain error reduction measures (ERMs).

In particular, since the functions of operators in an emergency operation or an accident management situation are mainly composed of cognitive activities such as monitoring, diagnosis decision-making and planning, cognitive error analysis becomes more important.

To follow this trend toward cognitive error, currently being developed human error analysis (HEA) methods have their focus on cognitive error analysis.

In this paper, we reviewed the currently available HEA methods, developed complement conventional HRA methods, selected three HEA methods, which are considered to be applicable to accident management tasks, and applied the three methods to one of the accident management tasks, viz., 'reactor cavity flooding'.

One of the HEA methods selected by the author of the paper, cognitive reliability and error analysis method (CREAM) is looked at in this technical document.

## II. The description of the selected HRA methods

### (1) Selection of the HEA methods

This section is not included in the excerpt given here.

### (2) Description of the selected methods

The descriptions of two of the three human error analysis methods given in the paper are not included in this excerpt.

#### CREAM (Cognitive reliability and error analysis method)

CREAM has been developed for use in both retrospective and prospective human reliability analysis. In retrospective analysis, causes of incidents or events are identified for input to system remediation. On the contrary, prospective analysis predicts the error in a given system. The output obtained from retrospective analysis can be used as evidence data for the development of a predictive analysis approach.

CREAM has been developed on the basis of two fundamental models. One is the Contextual Control Model (COCOM). COCOM regards human cognition as performed not sequentially as in Rasmussen's Step Ladder Model, but recursively. And, the control of human cognition is determined by the context (task and situation). The other is the simple model of cognition (SMoC), which views the cyclical nature of human cognition composed of four consecutive stages from observation, over interpretation and planning to execution.

CREAM provides 9 context factors named the common performance conditions (CPCs). The assessor performs Error Analysis considering these CPCs. CREAM also defines 15



cognitive activity types according to task characteristics to facilitate analysis. Each cognitive activity type has predefined cognitive stages. The cognitive function failures according to cognitive stages are shown in Table 5.2.8-1. Accordingly, the assessors should firstly assign appropriate cognitive activity type to the task procedure, then refer to the cognitive stages (functions), and finally determine the most probable cognitive function failure considering the CPCs.

(3) Comparison of the methods

This is not included in the excerpt given here.

III. Application to accident management tasks

(1) Description of the task

For a case task during the accident management situation, we selected the 'reactor cavity flooding strategy', which was suggested for the prevention or delay of the time of reactor vessel failure at the time of core damage (mentioned in the previous case study, pages 156-157).

The task associated with the reactor cavity flooding strategy selected for the case application is adapted from the SAG – 4 in SAMG, INJECT INTO CONTAINMENT, among the eight SAGs. It is Task 3: Decide whether or not to implement the strategy by evaluating the negative consequences of NOT implementing the strategy.

Summarised task steps in task 3

- Evaluate the negative impacts of implementation of the strategy.
- Evaluate the mitigating actions for the negative impacts.
- Evaluate the consequences of not implementing the strategy.
- Decide whether to implement the strategy by evaluating the negative impacts from the implementation of the strategy and the consequences of NOT implementing the strategy.

The task procedure 1 is to evaluate the negative impacts such as 'insufficient injection source' and 'containment severe challenge from a hydrogen burn'. This procedure comprises observation and system state identification stages.

The task procedure 2 is related to the evaluation of mitigation actions for negative impacts. This requires cognitive stages of evaluation and procedure selection, for the operators need to evaluate whether it is possible to take an action, from the given set of mitigating actions, in a given plant state, and make a possible effect on the plant.

The task procedure 3 is related to the evaluation of consequences of not implementing the strategy. Quantifying consequences is quite difficult due to uncertainties associated with plant phenomena as well as with the information. Since the procedure is related to the evaluation of consequences, the cognitive function is primarily performed at the interpretation stage.

The task procedure 4 is to make a decision whether to implement the strategy or not based on the above evaluations. This could be difficult depending on the event scenarios because of various uncertainties.

(2) Results of the application

The results of application of two of the three human error analysis methods given in the paper not included in this excerpt.

#### Results of CREAM application

Since the task procedure 1 comprises ‘observation’ and ‘state identification’ stages, the cognitive activity types are the kinds of ‘observe’, ‘compare’ and ‘identify’. And the cognitive function failure could be I 2 - Decision error associated with ‘state identification’.

The task procedure 2 requires the operators’ knowledge and experience to prepare the specific mitigating actions. Therefore the cognitive activity type could be ‘evaluate’ and the failure could take place in the process of formulating the relevant procedure (i.e. P 2 -Inadequate Plan Formulated).

The task procedures 3 and 4 are related to the evaluation of consequences and decision making respectively. Therefore, the cognitive activity type could be ‘evaluate’ and I 2 - decision-making failure could be dominant.

**TABLE 5.2.8-1 : POTENTIAL COGNITIVE FUNCTION FAILURES ACCORDING TO COGNITIVE FUNCTIONS IN CREAM [8]**

<b>Cognitive Functions</b>	<b>Potential Cognitive Function Failure</b>	
Observation errors	O 1	Observation of wrong object. A response is given to the wrong stimulus or event.
	O 2	Wrong identification made, e.g. due to a mistaken cue or partial identification
	O 3	Observation not made (i.e. omission), overlooking a signal or measurement.
Interpretation errors	I 1	Faulty diagnosis, i.e. either a wrong or an incomplete diagnosis
	I 2	Decision error, either not making a decision or making a wrong/incomplete decision.
	I 3	Delayed interpretation, i.e. one not made in time.
Planning errors	P 1	Error of priority, as in selecting the wrong goal
	P 2	Inadequate plan formulated; plan is incomplete or simply wrong.
Execution errors	E 1	Execution in a wrong manner; with respect to force, distance, speed or direction.
	E 2	Action performed at the wrong time, say too early or too late.
	E 3	Action on the wrong object, say on a neighbouring, similar or unrelated object.
	E 4	Action performed out of sequence, such as repetitions, jumps and reversals.
	E 5	Action missed out, not performed (i.e. omission) including an omission of the last actions in a series.

#### IV. Comparative evaluation of three methods based on the application

The excerpt below gives only the points relevant to CREAM from the paper.

CREAM is assessed to be more systematic in approach than others. At the beginning of the analysis CREAM assesses work context and then performs error analysis based on context factors, i.e. CPCs. CREAM reflects the context explicitly in the error analysis by providing

specific factors to be considered. CREAM however does not present inter-relationships between CPCs and cognitive failures. The unique feature of CREAM is that it uses a simple model of human cognition and the concept of cognitive activity type. However, the cognitive function failures are not enough in number for error analysis of accident management tasks, to give specific error types.

V. Conclusions.

The excerpt below gives only the points relevant to CREAM from the paper.

CREAM is considered more systematic in approach than others. But, for CREAM to be adequate for analysis of accident management tasks, it should have a more specific error classification system. It is also required to provide a classification system of human error causes or mechanisms.

5.2.8.3 Observations of the Author of this Technical Document

- (a) A typical HRA is concerned with finding the probabilities of events specified in the PSA Event Tree. A second generation HRA like CREAM goes beyond this and provides a detailed qualitative analysis.
- (b) In the paper, the authors refer to the Common Performance Conditions (CPCs), which characterise the context in CREAM. The CPCs referred to are as given in Table 5.2.8-2.

**TABLE 5.2.8-2 : COMMON PERFORMANCE CONDITIONS (CPCs) [8]**

<b>Adequacy of organisation</b>
Working conditions
Adequacy of MMI and operational support
Availability of procedures/plans
Number of simultaneous goals
Available time
Time of day (circadian rhythm)
Adequacy of training and preparation
Crew collaboration quality

- (c) The focus in the paper is on the application of CREAM to qualitative analysis for an accident management task. CREAM is designed to support such an analysis. Some important aspects in the analysis, which are not brought out in the paper, are delineated below [8].
  - Assessment of the CPCs: This step involves the examination and assessment of the work conditions under which the task is done. Each CPC is evaluated using its descriptors. For example, for adequacy of organisation, the descriptors are: very efficient/efficient/inefficient/deficient. The assignment of descriptors is based on the task analysis carried for the HRA and looks at the task as a whole.
  - Development of the profile of cognitive demands of the task: In this step, the cognitive activities that characterise each task are identified. The cognitive activities are used to build a cognitive profile of main task elements, based on the cognitive functions described by the underlying cognitive model. Four cognitive functions, observation, identification, planning and execution are specified by the CREAM model. There are 15 cognitive activity types in CREAM (Table 5.2.8-3) and each cognitive activity is described as a combination of cognitive functions. For example, coordination involves planning as well as execution - planning used to specify what is to be done and execution used to carry it out or perform it.

- Identification of likely cognitive function failures: Based on the phenotype-genotype classification of erroneous actions (Section 3), an exhaustive list of cognitive function failures can be produced. This list can be used as a basis for identifying the likely cognitive function failures. To make the method practical, a subset comprising a small set of generic cognitive function failures is considered in the study. In this regard, the authors of the paper do mention that the 13 cognitive function failures specified are not enough in number for error analysis of accident management task to give specific error types.
- The cognitive function failures are defined relative to the four cognitive functions mentioned above, viz. observation, identification, planning and execution. Cognitive function failures are assigned to task steps. The assignment is based on the description of the scenario and likely performance conditions. For example, consider the task step corresponding to evaluation (as a cognitive activity). Evaluation is described in terms of two cognitive functions, interpretation and planning. In assigning the likely failure mode, it is necessary to consider three possible failures of interpretation and two of planning before choosing the one most likely in the given conditions. This can be done only with information on the nature of the task and the performance conditions. The information may make it possible to determine for the specific case firstly whether a failure of interpretation is more likely than a failure of planning and secondly which specific type of failure one can reasonably expect.

**TABLE 5.2.8-3 : COGNITIVE ACTIVITY TYPES**

<b>Coordinate</b>	<b>Diagnose</b>	<b>Identify</b>	<b>Observe</b>	<b>Regulate</b>
Communicate	Evaluate	Maintain	Plan	Scan
Compare	Execute	Monitor	Record	Verify

- (d) Both this and the previous case study consider an accident management task. In accident management, the functions of operators are mainly composed of cognitive activities (monitoring, diagnosis, decision making and planning) and cognitive errors are to be considered. SLIM is a first generation method that is more appropriate than methods like THERP and ASEP for assessing cognitive errors, but the method focuses on the observable effects of human tasks. In the first case, a quantitative assessment of the accident management task is illustrated, using a set of PSFs selected by the analyst. CREAM is a second generation method that focuses on cognitive error analysis. CREAM assesses the work context and performs error analysis based on the 9 specified common performance conditions (CPCs). 15 cognitive activity types are also specified in CREAM and these are used to qualitatively assess the accident management task in the second case study.
- (e) Since the paper is concerned with the evaluation of human error analysis methods, no quantitative analysis is included. Quantification would involve the determination of specific action failure probabilities. In CREAM, once the specific cognitive function failures have been assigned for each task element, it is possible to assess the cognitive failure probability (CFP) for each cognitive failure type. These CFPs can be adjusted for the effects of the CPCs. The effect of the CPCs on the cognitive functions is specified as strong, medium or weak. A database of nominal CFPs and uncertainty bounds for most generic cognitive function failures can be compiled from a review of PSA/HRA. Established data sources are used for proceduralised behaviours like observation and execution. CFPs for interpretation and planning are mostly based on expert judgement [8]. A table of CFPs is given in Appendix-7.

## 6. STUDIES OF PLANT EVENTS TO IMPROVE SAFETY IN A REFERENCE NUCLEAR POWER PLANT (KAPS)

### 6.1 Introduction

Plant event and incident reports are sources of useful information on human error and human performance related problems that exist in an operating plant. The analysis of plant events involving human reliability problems can provide risk insights for effecting improvements in plant design and operation. This important aspect is addressed by carrying out studies of plant events in KAPS.

### 6.2 Collection and Tabulation of Data on Human errors in Significant Events in KAPS

Plant events, which have occurred in KAPS 1, 2 during the last five years of operation (i.e. 2000 - 2005), have been considered for the present study. Data on human performance was collected from the Safety Related Unusual Occurrence Reports (SRUORs)/ Significant Event Reports (SERs) and Event Reports (ERs)/Unusual Occurrence Reports (UORs), pertaining to the period. The reports were first examined and events wherein human performance related issues played a role were identified. There were eighteen such cases, out of a total of eighty-one events (comprising thirty-two significant events and forty nine other events) during the period. All eighteen events have been analysed. Concise details were gathered from the Event Reports, minutes of Station Operation Review Committee (SORC) Meetings and Root Cause Analysis Reports (where available) for the eighteen events. The details are tabulated and used in the present study.

The human performance related event causes can be grouped into eleven different classes. Some events had more than one human performance related contributory cause. There were eleven cases of maintenance related causes, four each of design and operation, three of procedure, two each of personnel performance, cognition/cognitive function failure and human factors and one case each of communication, work assignment, work schedule and documentation. There is potential for improvement in some of the areas and these have been appropriately indicated in the respective event tables.

The human performance related events in KAPS for the period 2000 - 2005 are analysed as follows.

#### 6.2.1 Reactor Trip Due to Loss of Control Power Supply to Breakers

Plant and Unit	KAPS, Unit 2
Date, time and plant state when incident occurred	09 - 03 - 2000, 05.10 hours. Unit operating at 220 MWe.
Brief description of event and operator action/s	415 V Bus D CPS Failure (Alarm). Supervision Relay in CB-351 flagged. DG-1 started and connected to Bus D. CB-351 opened. During investigation and troubleshooting, 220V D.C. positive and negative terminals were inadvertently shorted and reactor tripped due to loss of control power supply to the breaker.
Consequences of the action	The short caused fuse failure and loss of CPS to all breakers connected to Bus D. Pressurising pump tripped causing all PCPs to trip. Reactor tripped on No PCP operating (05.33 hours). CPS was normalized. Attempt to restart reactor failed and reactor poisoned out.
The Cause/s	Inadvertent shorting 220V terminals during troubleshooting.
Human/Ergonomics factors, human performance related findings	Sufficient care was not exercised in carrying out the task.
Human reliability quantification/HEPs	The inadvertent shorting was a slip error. HEP is estimated = 0.0001. Data Source: Generic evaluation of possible slip errors when a good MMI exists, page 28, IAEA-TECDOC-592.

6.2.2 Reactor Trip on Trip of One Channel on Loss of Supply and Second Channel on Actual Power > Demand Power by One Decade

Plant and Unit	KAPS, Unit 1
Date, time and plant state when incident occurred	14-09-2000, 14.10 hours. Unit operating at 220 MWe.
Brief description of event	Standby Control UPS (CUPS-4) to one channel tripped and it lost supply. A second channel also tripped on actual power > demand power by a decade. Reactor and TG tripped. Standby CUPS-4 failed due to inverter fuse failure. Trap Filter of CUPS-1 was choked. The cable connecting CUPS-1 output breaker to selector switch had burnt. The chokeup could have caused the cable to burn as well as ground fault leading to fuse failure. Loss of 240 V AC Control PS to Panel 1 caused RPS CH-D trip.
The cause/s	Inadequate maintenance of trap filter.
Human/Ergonomics factors, human performance related findings	Inadequate maintenance/maintenance not carried out.
Human reliability quantification/HEPs	Basic HEP (BHEP) for the maintenance task is taken = .03 (5) where EF=5. It is assumed that post maintenance inspection is normally carried out in the plant. In this case, it was either not done or was done incorrectly. Recovery factor (RF) for post maintenance inspection is 0.01. So HEP in this case is $0.03 \times 0.01 = 0.0003$ (10) where the EF=10 (HEP Evaluation using ASEP HRA Procedure).

6.2.3 Reactor Trip on High PHT System (PHTS) Pressure

Plant and Unit	KAPS, Unit 2
Date, time and plant state when incident occurred	03 - 01 - 2001 at 09.25 hours Unit startup
Brief description of event and operator action/s	Boron removal was in progress to make reactor critical after poison shutdown. PHTS Pressure was being maintained by wide range pressure control. Steam generator level controller hunting was observed in the control room. In order to further check the level controller, operator switched off its 240V AC power supply. Reactor tripped on high PHTS pressure.
Consequences of the action	PHTS pressure rose sharply from 20 kg/cm <sup>2</sup> to 94.9 kg/cm <sup>2</sup> . This caused IRVs to open and PSS actuated on high PHTS pressure. At the same time, coolant channel flow low, ALPAS tank level low and BCD high level window alarms appeared in control room.
The cause/s	1. MCB in 240V AC power supply to SG Level Controller also supplies power to channel C of PHTS wide range pressure control loop. As this power supply was cut off, channel C transmitter output signal (at input to median selector) became zero. Channels A and B should have continued to function undisturbed and no failure should have occurred. But a wire in channel B PHTS pressure controller was open at the controller panel terminal, with the result that the

6.2.3 Reactor Trip on High PHT System (PHTS) Pressure (Contd.)

Plant and Unit	KAPS, Unit 2
	<p>channel B signal did not extend to the median selector. Failure of two channels meant that the median selector selected a zero median, causing feed valves to fully open and bleed valves to fully close.</p> <p>2. To compound the situation, the channel A narrow range/wide range controller relay malfunctioned and the narrow range selection contacts opened out and wide range selection contacts failed to close. So the channel A wide range pressure control signal too did not extend to the median selector. The open circuited channel picked up stray voltage of 2.5 to 8 volts. This meant that prior to when the 240V power supply was switched off, channel C output (2.4V) was being selected as the median and channels A and B were ineffective. The median output became 0 when the power supply was switched off and reactor tripped.</p>
Human/ergonomics factors, human performance related findings	<p>1. There is no provision to check whether all the three controller output signals extend to the median selectors and are in the desired range (Inadequacy in Design).</p> <p>2. The power supply to SG Level controller was switched off without following proper procedure. The procedure did not include checks to confirm that the other two channels are operating as required (Procedure Not Followed /Incomplete Procedure).</p> <p>3. Channel B was open due to a cut wire. Careful post-maintenance checks could have prevented the cut wire going undetected (No Post-Maintenance Check).</p>
Recommendations of SORC, NKSC	<p>1. Provide indication to check pressure controller outputs to median selector.</p> <p>2. Adhere to procedure while switching off control power supply MCBs.</p> <p>3. Dual verification by internal QA to detect wire cut and the like.</p>
Human reliability quantification - human error probabilities (HEPs)	<p>1. Error in not following procedure. HEP = 0.003 (5) for the case when a written procedure is available but not used. Data Source: Table 20-7 of Handbook (Appendix 5).</p> <p>2. Error of incomplete procedure. HEP = 0.003 (5) for omitting a step or important instruction in a formal or ad hoc procedure. Data Source: Table 20-5 of Handbook giving estimated HEPs in the preparation of written material (Appendix 5).</p> <p>3. Post maintenance check not carried out or improperly carried out. BHEP for maintenance task = 0.03 (5). RF for post maintenance check = 0.01. So HEP = 0.03 x 0.01 = 0.0003 (10) (HEP Evaluation using ASEP HRA Procedure).</p>
Similar events which have occurred in KAPS	<p>Reactor Trip on Low PHTS Pressure in Unit 2 of KAPS at 03.42 hours on 14-02-1999.</p> <p>Unit was operating at 75 MWe. PHTS pressure dropped to 44 kg/cm<sup>2</sup> at 03.42 hours and ECCS Type I injection got initiated. Operators observed that the narrow range controller output was zero, but feed valves were not open and bleed valves were not closing.</p>

6.2.3 Reactor Trip on High PHT System (PHTS) Pressure (Contd.)

Plant and Unit	KAPS, Unit 2
	<p>Operators observed that the control signal of narrow range pressure controller remained in bleed valve range, causing PHTS pressure to drop. Channels A and C narrow to wide range changeover relay contacts were found open on investigation. This caused stray voltages to go to the median selectors and therefore the bleed valves remained in bleed range.</p> <p>Stray voltage pickup on relay malfunction occurred once again in the subsequent event in KAPS Unit I on 03-01-2001.</p>

6.2.4 Heavy Water Spill from F/M Supply Pump-3525-P2

Plant and Unit	KAPS, Unit 1
Date, time and plant state when incident occurred	27- 01- 2001, 10.20 hours Unit operating at 220 MWe
Brief description of event	3525-P2 was started at 08.30 hours. Refueling of channel D-7 done. Both seal plugs were installed. Snout plug installation was in progress. At 10.20 hours, floor beetle (103 MEL) and storage tank level low window alarms come on in CR and ST level was found to be dropping. In the field, a heavy leak of D <sub>2</sub> O from plunger gland of 3525-P2 was observed. Pump was stopped and isolated. ~5.2 tons of D <sub>2</sub> O had leaked in 7 minutes.
The cause/s	1/3 plungers' gland packing along with gland follower and springs had come out and caused the leakage of heavy water. This happened due to disengagement of gland nut locking pawl and unscrewing of gland follower.
Human/Ergonomics factors, human performance related findings	Improper maintenance of pump with post maintenance check not done or improperly done.
Human reliability quantification/HEPs	BHEP for the maintenance task is taken = .03 (5). Post maintenance check (normally carried out) was either not done or was done incorrectly. RF = 0.01. So HEP in this case is 0.03 x 0.01 = 0.0003 (10) (HEP Evaluation using ASEP HRA Procedure).

6.2.5 Reactor Trip on Moderator Level Low

Plant and Unit	KAPS, Unit 1
Date, time and plant state when incident occurred	13-02-2001 Unit operating at 220 MWe.
Brief description of event	During routine surveillance helium flow in bubblers was seen to have come down to 10 and 0 lph [ $<15$ lph, the normal value]. While trying to adjust the flow in bubbler, PSS actuated on moderator level low and the reactor tripped.
Consequences of the action	Abrupt change in flow from 0 lph caused moderator level to also change abruptly. PSS actuated on moderator level low in all three channels



6.2.5 Reactor Trip on Moderator Level Low (Contd.)

<b>Plant and Unit</b>	<b>KAPS, Unit 1</b>
	and reactor tripped. Occurrence of such spurious actuation was confirmed during the poison shutdown, which followed.
The cause/s	Improper adjustment of bubbler flow.
Human/Ergonomics factors, human performance related findings	Improper operation.
Human reliability quantification/HEPs	The operation is considered to be a dynamic action carried out under moderately high stress. HEP is estimated = 0.05 (5) (evaluation using ASEP HRA procedure, Table 8.5 - Appendix-6).

6.2.6 Reactor Trip on PHT System (PHTS) Pressure High.

<b>Plant and Unit</b>	<b>KAPS, Unit 1</b>
Date, time and plant state when incident occurred	09-03-2002, 06.53 hours. Unit operating at 220 MWe.
Brief description of event	PCP-1 tripped on differential protection followed by PCP-4 as per the designed logic. Reactor tripped on PHTS pressure high and poisoned out. During secondary injection test of motor end CT circuit, Y phase did not operate.
The cause/s	Inspection of differential protection relay cubicle located above the breaker unit revealed its locking screw to be loose. A loose module resulted in a partial short in Y phase of CT, consequent relay actuation and PCP-1 trip on differential protection.
Human/Ergonomics factors, human performance related findings	Improper maintenance with post maintenance check not done or improperly done.
Human reliability quantification/HEPs	BHEP for the maintenance task is taken = .03 (5). Post maintenance check (normally carried out) was either not done or was done incorrectly. RF = 0.01. So HEP in this case is $0.03 \times 0.01 = 0.0003$ (10) (HEP Evaluation using ASEP HRA Procedure).

6.2.7 Manual Reactor Trip Due to End Shield Coolant Outlet Temperature High

<b>Plant and Unit</b>	<b>KAPS, Unit 2</b>
Date, time and plant state when incident occurred	03-04-2002, 20.42 hours Unit operating at 220 MWe
Brief description of event and operator action	End shield coolant outlet temperature high alarm appeared at 51° C. Both North and South End Shield temperatures at PDCS were in alarm condition (> 51 ° C). Operator commenced power reduction. In the field, Active LPPW System common outlet control valve was found closed. Reactor was manually tripped at 20.56 hours. End Shield coolant outlet temperature had gone up to 55.5° C. The PW CV was opened by bleeding air, from valve positioner. End shield temperature came down to normal. In attempting to restart the reactor, it poisoned out
The cause/s	The CV positioner was malfunctioning due to choking of the fixed orifice of the flapper nozzle assembly by dust (aluminium and silica).
Human/Ergonomics factors, human performance related findings	<ol style="list-style-type: none"> <li>1. The Preventive Maintenance (PM) Procedure for CV did not include servicing of valve positioner internals (Inadequate Procedure).</li> <li>2. It took quite some time to identify and open the CV, so as to inspect valve positioner internals (Human/Ergonomics Factors).</li> </ol>
Other findings	<ol style="list-style-type: none"> <li>1. Window and alarm CRT alarms for end shield coolant temperature had their high limits set at 51 ° C. As the technical specification limit is also 51 ° C, there is no margin for operator action (Inadequate Design).</li> </ol>
Recommendations made by SORC.	<ol style="list-style-type: none"> <li>1. Revise PM Procedure for CV. Also for all other similar air operated CVs.</li> <li>2. Mark important CVs and MVs as Air to Open or Air to Close type and keep tool kits at important locations for fast response action.</li> <li>3. Set End Shield High Temperature Alarm Limits as 47 ° C on Window Annunciator and 48 ° C on Alarm CRT, to provide operator margin. Review other alarms with no margin for operator action.</li> </ol>
Human reliability quantification/HEPs	Error of inadequate preventive maintenance procedure: HEP = 0.003 (5) for omitting a step or important instruction of a formal or ad hoc procedure. Data Source: Table 20-7 of the Handbook (Appendix-5)
Comments or views on human performance	Due to the absence of clear marking on the valve and the lack of a readily accessible toolkit to open the valve body, a good amount of time was taken to open a non-functional CV in the field in order to inspect its internals. Human performance problems of this kind are due to what are called Human Engineering Discrepancies (HEDs), which may be present not only in the control room but also in other areas of the plant. A review of the Human Engineering Discrepancies (HEDs) in the plant by a team of human factors experts and operators will reveal the areas needing ergonomics improvements, which for example could include clear labeling of valves and other equipment, provision of readily accessible toolkits at different locations on site and provision of function group demarcations on control panel.

6.2.8 Turbine Trip on Steam Generator-2 High Level followed by Reactor Trip on High Steam Generator-4 Differential Temperature

Plant and Unit	KAPS, Unit 2
Date, time and plant state when incident occurred	02-01-2003, 07.30 hours Unit operating at 220 MWe.
Brief description of event and operator action	SG-2 Level High window alarm appeared at 07.30 hours in the control room. SG-2 Level was rising although the level controller output was seen to be zero. Turbine tripped on SG-2 level very high. Reactor setback on ASDV opening and power fell to 26 percent FP. One large CSDV was found to have not opened. It was opened from the control room and power was raised to 80 percent FP. But reactor tripped on SG-4 DT high and got poisoned out.
The Cause/s	<ol style="list-style-type: none"> <li>1. Field Check showed SG-2 Feed CV (Air Fail to Close), which was in service before the incident to be stuck open fully. Failure of valve positioner pneumatic relay (due to a hardened back-pressure diaphragm) led to a continuous output of air that kept valve fully open, causing failure of auto level control and turbine trip on SG-2 Level Very High.</li> <li>2. To control rising level in SG-2, the manual valve downstream of main CV was closed and manual changeover to standby CV was done. But level control output was zero due to high level in SG-2 and standby CV remained closed. Operator reverted control to main CV (with manual valve still closed) This caused feed water to SG-2 to be cut off suddenly leading to sharp drop in SG-2 <math>\Delta T</math>.</li> <li>3. The sudden reduction of feed water supply to SG-2 to zero for a brief duration led to a redistribution of flows among the SGs, a sudden large inrush of cold feed water to SG-4 and high <math>\Delta T</math> in SG-4. This in turn led to reactor trip on actuation of two RPS channels on high SG-4 <math>\Delta T</math>.</li> </ol>
Human/Ergonomics factors, human performance related findings	<ol style="list-style-type: none"> <li>1. A stuck open CV is not detectable from the control room as no indicator is provided (Inadequate Feedback to Control Room).</li> <li>2. Failure of valve positioner pneumatic relay could have been detected earlier with better scheduling of preventive maintenance (Inadequate PM Schedule).</li> <li>3. Improper Manual Control of the SG Level (Inadequate Performance of Operating Personnel).</li> </ol>
Recommendations made by SORC, RCAC	<ol style="list-style-type: none"> <li>1. Provide position indication of all 90 percent CVs in CR</li> <li>2. Replace rubber parts of components/systems in high temperature areas at least once in five years.</li> <li>3. Manual intervention/control is to be resorted to only after a careful assessment of system status. Provide training.</li> </ol>
Human reliability quantification/HEPs	<p>Inadequacy in planning preventive maintenance schedule for CV, a failure in planning, which is a cognitive function. Estimate of cognitive failure probability for planning = 0.02 (10). Data source: Table of cognitive failure probabilities in hollnagel, 1998 (Appendix-6).</p> <p>Operator reverts to main CV in SG level control without restoring manual valve (closed earlier) to open condition.</p>

6.2.8 Turbine Trip on Steam Generator-2 High Level Followed by Reactor Trip on High Steam Generator-4 Differential Temperature (Contd.)

Plant and Unit	KAPS, Unit 2
	Omission of an important step in the operation. The operation is considered to be a dynamic operation carried out under moderately high stress. HEP is estimated = 0.05 (5) (Evaluation using ASEP HRA Procedure, Table 8.5-Appendix-6).
Comments or views on human performance	The stuck open CV could have been detected if clear and unambiguous valve position feedback had been provided in the control room. As in the event above, the human performance problem arose out of a HED. Such HEDs can be weeded out by a systematic ergonomics/human

6.2.9 Reactor Trip on Steam Generator Differential Temperature High and Some Fuel Bundles Crossing Bundle Power Safety Limit

Plant and Unit	KAPS, Unit 2
Date, time and plant state when incident occurred	10 - 03 - 2004, 09.24 hours Unit operating at 170 MWe
Brief description of event and operator action	A faulty contact in power UPS (PUPS) 1 RL-A relay and malfunctioning of the static switch isolator in Y phase caused fuse failure in 415 class II power supply to all adjustor rod control units (ARCUs). Failure of fuses in ARCUs led to total power supply loss to all 16 adjustors rendering their servo amplifiers inoperable. Reactor regulation capability through adjustors was lost. The inoperability of shim rods led to loss of setback function. Operator manually inhibited ALPAS CAM on fear unwarranted addition of boron due to refueling or perceived logic failures on 48V DC trouble.
The consequence	Inhibition of auto operation of ALPAS CAM resulted in loss of chemical shim for augmenting rod worth. Inadvertent power ramp of about 25 percent FP led to reactor trip and some fuel bundles crossing the bundle power limit.
The cause/s	<ol style="list-style-type: none"> <li>1. All adjustor rods became inoperable on loss of 415 V 3 phase power supply.</li> <li>2. The inhibition of auto operation of ALPAS CAM by the operator.</li> <li>3. Trip settings on Lin N were not set conservatively.</li> </ol>
Human/Ergonomics factors, human performance related findings	<ol style="list-style-type: none"> <li>1. Relay RL-A and Static Switch Isolator in Power UPS 1 were not covered by the preventive maintenance procedure (Incomplete Procedure).</li> <li>2. Operator inhibited auto-operation mode of ALPAS-CAM, without paying attention to reactor power changes and reactor core status (Improper operator action, personnel performance, procedure not followed).</li> <li>3. Trip set points were not set conservatively, although warranted (Rules not Followed, Personnel Performance)</li> </ol>
Other findings	<ol style="list-style-type: none"> <li>1. Common fuse provided in main and back up power supplies of ARCU. Fuse failure led to non-availability back up power supply also (Inadequate Design).</li> </ol>

6.2.9 Reactor Trip on Steam Generator Differential Temperature High and Some Fuel Bundles Crossing Bundle Power Safety Limit (Contd.)

Plant and Unit	KAPS, Unit 2
	2. No alarm window in control room for annunciation of loss of power supply to ARs and ARs inoperable (Inadequate Design).
Recommendations of SORC, RCAC	<ol style="list-style-type: none"> <li>1. Working simultaneously on two jobs (on PUPS/CUPS and refueling operations in the present case) should be avoided.</li> <li>2. Impart awareness training on conservative decision making and constraints resulting from low power operation.</li> <li>3. Review maintenance procedures of all safety related equipment. Revise to cover all components.</li> <li>4. Review and improve information support to control room operators during transients by adding displays and indicators.</li> </ol>
Human reliability quantification/HEPs	<p>Error of incomplete preventive maintenance procedure: HEP = 0.003 (5) for omitting a step or important instruction in a formal or ad hoc procedure. Data Source: Table 20-7 of Handbook (Appendix-5).</p> <p>Manual inhibition of auto operation of ALPAS CAM. Error due to a failure to correctly interpret the situation (a kind of faulty diagnosis). HEP is taken to be 0.2 (LB = 0.09, UB = 0.6). Data Source: Table of cognitive failure probabilities in Hollnagel, 1998 (Appendix-7).</p> <p>Lin N trip setpoints set incorrectly. A conservative approach was not followed. Error is somewhat similar to that of writing an item incorrectly in a procedure. HEP = 0.003 (5). Data source : Table 20-5 of handbook giving estimated HEPs in the preparation of written material.</p>

6.2.10 Reactor Trip on One/More PSS Rods Leaving Parked Position During Unit Startup

Plant and Unit	KAPS, Unit 2
Date, time and plant state when incident occurred	15 - 06 - 2004, 20.50 hours Unit was under startup (power level: 1.2 percent FP)
Brief description of event	At a reactor power level < 2 percent FP, when PHT System was being hot pressurised, PSS Rod M-3 slipped from parked position and reactor tripped as per logic.
The cause/s	A check revealed that a clutch failure had occurred. The 90 V DC power supply was not getting extended to the clutch as two redundant wires were broken in the power supply connector cable near the PSS drive. PSS Rod M-3 cable clamp was loose and caused two wires of the cable, which were subjected to full tension, to break.
Human/Ergonomics factors, human performance related findings	<ol style="list-style-type: none"> <li>1. The prime cause was an inadequate preventive maintenance programme (Inadequate Preventive Maintenance).</li> <li>2. PS isolation (connector removal) and normalisation during the recent control rod drive replacement had been done by mechanical maintenance unit (MMU). Earlier, this job was being done by control maintenance unit (CMU). This was a procedural change (Inappropriate Work Assignment).</li> </ol>
Recommendations by SORC, RCAC.	<ol style="list-style-type: none"> <li>1. Modify procedures for inspection and post-maintenance checks to cover cable clamps on PSS drives.</li> </ol>

6.2.10 Reactor Trip on One/More PSS Rods Leaving Parked Position During Unit Startup (Contd.)

Plant and Unit	KAPS, Unit 2
	<p>2. Task of drive power supply isolation and normalization to revert to CMU as per earlier practice.</p> <p>Error of inadequate maintenance, post maintenance check not done. BHEP for the maintenance task is taken = .03 (5). Post maintenance check (normally carried out) was either not done or was done incorrectly. RF = 0.01. So HEP in this case is <math>0.03 \times 0.01 = 0.0003</math> (10) (evaluation using ASEP HRA Procedure).</p>
Human reliability quantification/HEPs	<p>Error of deviation in work assignment practice. As indicated in the Handbook, a nominal of 0.003 is assumed for the task assignment. Assignment to MMU was a deviation as this task is normally assigned to CMU. Assuming MMU to be less experienced in tasks of this kind, a PSF for level of experience = 2 is used to modify the BHEP to give <math>HEP = 0.003 \times 2 = .006</math>. Table 20-12 of the Handbook gives estimates of HEPs for errors of commission in operating manual controls. HEP for improperly mating a connector (including failure to test locking of connector for engagement = 0.003 (5).</p>

6.2.11 Reactor Power Rise During Refueling and Subsequent Poison Out

Plant and Unit	KAPS, Unit 1
Date, time and plant state when incident occurred	<p>14 - 06 - 2004, 15.40 hours Unit operating at 160 MWe</p>
Brief description of event and operator action/s	<ol style="list-style-type: none"> <li>1. Unit was started on 05-06-2004 after a 44 days shutdown. Estimated reactivity to start with was high due to fission product decay and Plutonium buildup. It had decreased to 0.6 mk or so on 14-06-2004 by fission product burnup and Plutonium consumption. The rate of excess reactivity reduction was not as per the expected pattern.</li> <li>2. Refuelling of channel L-11 was planned for 14-06-2004. In fuel transport system, a fault detected in PRV-50 had to be rectified. Refueling could therefore be started only at 15.00 hours, although fuel change order (FCO) had been prepared at 07.00 hours considering the reactivity at that time.</li> <li>3. Only one absorber (UNE) was in effective control range just before bundle movement, as another rod (LSW) moved out of control range when seal plug was removed and cold water got injected. All four regulating rods were fully out and on manual. The channel chosen for refueling was a central channel and therefore the rate of positive reactivity addition on bundle movement was higher. The action of UNE absorber was delayed because of a high dead band of 1 V (~ 1.33 % FP). Shim rod move earlier and faster (as dead band was 0.33 V as per design). A CAM shot was initiated by shim rod movement, but its effect was realised after the designed delay of 0.35 seconds, by which time reactivity balance had already been established. CAM injection was therefore unwarranted.</li> <li>4. Unwarranted restart of refueling under transient conditions and fast movement of the fourth bundle resulted in an increase in</li> </ol>

6.2.11 Reactor Power Rise During Refueling and Subsequent Poison Out (Contd.)

Plant and Unit	KAPS, Unit 2
	<p>power due to fast addition of reactivity and inadequate control by RRS. Maximum power went upto 81.5 % FP on PSS whereas it was 77.79 % FP on RRS (Power Mismatch). SSS power was 77.6 % FP. Power increased sharply with reactor period as low as 153 seconds for a brief period (64 % FP to 74 % FP).</p>
The cause/s	<ol style="list-style-type: none"> <li>1. Low excess reactivity in the core- reactor was operated with very low excess reactivity and degraded capacity of reactor regulation by absorber rods.</li> <li>2. Fourth bundle was moved very fast resulting fast reactivity insertion, which was beyond the regulating capacity of absorber rods.</li> </ol>
Human/Ergonomics factors, human performance related findings	<ol style="list-style-type: none"> <li>1. FCO was prepared at 07.00 hours but refueling was begun at 15.00 hours, by which time reactivity had reduced by another 4 mk further degrading the capability of RRS. No cautionary warning was included in FCO. Reactor was operated with low excess reactivity and less than adequate regulating capacity (inadequate work schedule control, lack of administrative control). central channel was selected for refueling when low excess reactivity core conditions prevailed (error of judgement).</li> <li>2. Procedures were not adhered to in refueling operations (Rules not followed).</li> </ol>
Recommendations by SORC, RCAC.	<ol style="list-style-type: none"> <li>1. Establish guidelines/procedure to maintain excess reactivity above predetermined level.</li> <li>2. Establish guidelines/procedure to maintain at least 6 control rods (AR or RR as applicable) in the predefined effective control range.</li> <li>3. FCO should be issued for a limited period. Revalidation after set period should be done after reassessment of core conditions. Refueling operations should be carried out exercising judgement and caution, taking cognizance of factors relevant to the situation.</li> </ol>
Human reliability quantification/HEPs	<p>Error of inadequate control over work schedule, a lack of administrative control. Estimated HEP for not carrying out plant policy/scheduled tasks = 0.01 (5). The lower bound value of 0.002 is selected, as the error was one of inadequate control over work schedule. Data Source: Table 20-6 of the Handbook, which gives estimated HEPs related to failure of administrative control.</p> <p>Error of omission of an important instruction in FCO. The estimated HEP = 0.003 (5). Data Source: Table 20-5 of the handbook which gives estimated HEPs for errors in preparation of written material.</p> <p>Error of judgement, leading to the wrong decision of selecting central channel for refueling when low excess reactivity core conditions prevailed. A failure in decision making, which is a cognitive function. The cognitive failure probability = 0.01 (10). Data Source: Table of cognitive failure probabilities in Hollnagel, 1998 (Appendix-7).</p> <p>Error in refueling. Fourth bundle was moved very rapidly resulting in fast reactivity addition. Rules to be followed in refueling fuel channels were not followed.</p>

6.2.11 Reactor Power Rise During Refueling and Subsequent Poison Out (Contd.)

<b>Plant and Unit</b>	<b>KAPS, Unit 2</b>
Comments or views on human performance	To avoid errors of judgement such as that which occurred when a central channel was chosen for refuelling under conditions of low excess reactivity in the core, it is necessary to provide the operators adequate training to improve mental concepts and understanding of physical phenomena, by way of classroom sessions and simulator training. It is also necessary to emphasise on operators the importance of monitoring reactor power changes at all times.

6.2.12 Manual Shutdown of Reactor on Observing Smoke/Fumes Near PCP-3

<b>Plant and Unit</b>	<b>KAPS, Unit 2</b>
Date, time and plant state when incident occurred	18 - 10 - 2004, 01.39 hours Unit operating at 174 MWe
Brief description of event	Fire alarm annunciates at 01.39 hours in control room. Detector alarms on FAS Panel indicate location to be near PCP-3 in pump room. CCTV camera indicates smoke from the same area. On 'on power' entry and investigation, smoke/fumes seen to emanate from PCP-3 casing insulation. Smoke/fumes were quenched by CO <sub>2</sub> and dry powder. Reactor was manually tripped at 02.06 hours by actuating PSS and PHTS was depressurized and cooled.
The root cause/s	Heating of oil soaked insulation on primary cooling pump
Human/Ergonomics factors, human performance related and other findings	<ol style="list-style-type: none"> <li>Oil was leaking from PCP-3 and getting collected in bearing stand-pipe. Finite leakage was considered acceptable (no maintenance planned).</li> <li>Pump casing insulation (calcium silicate) absorbed oil and caused fumes and smoke on getting heated. There is no cladding or barrier installed to prevent the oil from coming in contact with insulation (inadequate design provisions).</li> </ol>
Recommendations by SORC, RCAC	<ol style="list-style-type: none"> <li>Identify potential sources of oil leak from PCPs and carry out periodic checks as part of maintenance.</li> <li>Allow sufficient curing time for calcium silicate insulation with a view to preventing cracks that can allow passage for oil.</li> </ol>
Human reliability quantification/HEPs	<p>Finite oil leakage was considered to be acceptable as a plant policy and no maintenance had been planned. This inadequacy in planning preventive maintenance for oil leaks can be looked upon as a failure in planning, which is a cognitive function. Estimate of failure probability = 0.02 (10). Data source: Table of cognitive failure probabilities in Hollnagel, 1998 (Appendix-7).</p> <p>No clad or barrier had been installed to prevent leaking oil from soaking into the insulation, amounting to inadequate design provision.</p>
Earlier occurrence of similar event	A similar event had occurred in KAPS, Unit 2 on 21-06-2004 when the unit was operating at 130 MWe. Fire alarm was annunciates at 01.47 hours and smoke/fumes were detected to be emanating from the insulation of SDC Pump 2 suction line below PCP-3 platform. The root cause was heating of oil soaked insulation causing the oil to vaporise at high temperature. Survey of potential sources of fire did not extend to this source.



6.2.13 Reactor Trip on Spurious EMTR Signal

<b>Plant and Unit</b>	<b>KAPS, Unit 2</b>
Date, time and plant state when incident occurred	02-06-2000 Unit operating at 210 MWe.
Brief description of event	Reactor tripped on no PCP running and poisoned out. EMTR-PLC-2 malfunction generated a spurious EMTR signal. [One PLC is a hot standby to the other].
The cause/s	The PLC – 2 I/O ribbon connector was loose.
Human/Ergonomics factors, human performance related and other findings	Post maintenance check/field inspection not properly carried out.
Human reliability quantification/HEPs	Error of inadequate maintenance, post maintenance check not done. BHEP for the maintenance task is taken = .03 (5). Post maintenance check (assumed to be normally carried out) was either not done or was done incorrectly. RF=0.01. So HEP=0.03 x 0.01 = 0.0003 (10) (evaluation using ASEP HRA Procedure).

6.2.14 Reactor Trip on Spurious EMTR Signal

<b>Plant and Unit</b>	<b>KAPS</b>
Date, time and plant state when incident occurred	06-11-2000 Reactor shutdown
Brief description of event and operator action/s	A permit was issued for replacement of the diaphragms of four valves of moderator cover gas system and two valves of the bubbler system. Order to isolate was issued for moderator cover gas system and it was isolated. Bubbler system was fully pressurised. Both systems have the same USI. A mechanical maintainer opened a valve of the bubbler system, assuming it to be depressurised. Helium cover gas together with some Tritium vapour was released through the valve opening. He waited and then closed the valve, but gas release continued.
Consequences of the action	Inhalation of tritium vapour in the cover gas cause high uptake.
The cause/s	Maintainer assumed the bubbler system to be depressurised and opened its valve. The wrong valve was opened.
Human/Ergonomics factors, human performance related and other findings	Maintainer makes an error of transposition. He opens the valve of bubbler system (which was not depressurised) in place of Valve of Moderator System (which was isolated).
Human reliability quantification/HEPs	As part of the maintenance job order, moderator gas system had been isolated. In place of opening moderator system valve, maintainer wrongly opened bubbler system valve - a transposition error. HEP for selection error for locally operated valve (assumed to be one of a group of similar valves, all clearly and unambiguously labeled) = 0.003 (3). Data source: Table 20-13 of handbook giving estimated HEPs for selection errors of locally operated valves (Appendix-5).

6.2.15 Pump Room Entry on Account of Inoperable Regulating Rod

<b>Plant and Unit</b>	<b>KAPS, Units 1</b>
Date, time and plant state when incident occurred	29-08-2000
Brief description of event	A regulating rod was found inoperable.
The cause/s	Observations showed the motor to be decoupled from the ball screw drive. The grub screw holding the motor end of the coupling onto the shaft was found to be loose.
Human/Ergonomics factors, human performance related and other findings	Improper maintenance with no post maintenance check.
Human reliability quantification/HEPs	BHEP for maintenance task is taken = 0.03 (5). RF for post maintenance check 0.01. So HEP = 0.03 x 0.01 = 0.0003 (10) (evaluation using ASEP HRA procedure).

6.2.16 Reactor Trip on Low PHTS Pressure

<b>Plant and Unit</b>	<b>KAPS, Units 1</b>
Date, time and plant state when incident occurred	08-11-2000, 12.39 hours. Reactor startup
Brief description of event	The unit had been synchronised at 12.39 hours after poison shutdown and speeder gear was on manual. Reactor power was being raised when setback appeared. On ASDV opening, TG load power was increased. However, mismatch of TG Load and Reactor Power caused reactor trip on low PHTS Pressure.
The cause/s	Higher TG load and lower reactor power during power raise was due to a lack of proper communication between the control engineers manning the TG and RR panels.
Human/Ergonomics factors, human performance related and other findings	Lack of proper communication between operators.
Human reliability quantification/HEPs	General error rate for oral communication: HEP = 0.03. Data Source: Table of Generic Guideline Data [13] given on Page 93, Chapter 4 of this report.
Comments or Views on human performance	The mismatch of TG load and reactor power and consequent trip occurred due to a lack of proper communication between operator on TG panel and operator reactor regulating panel. To avoid such errors, it is important to foster teamwork. There may also be a need to improve communication protocols. A review may be carried out of operations where operator communication and coordination play a significant role and provide special training in these operations so that human performance is improved.

6.2.17 Loss of Class III 415 V Bus Potential

<b>Plant and Unit</b>	<b>KAPS, Units 1</b>
Date, time and plant state when incident occurred	02-03-2001, 13.47 hours. Unit operating at 220 MWe
Brief description of event	415 V Bus J to P tie-breaker (CB-322) was under preventive maintenance. While testing it, Bus P-1 tie-breaker CB-312 tripped causing power loss and tripping of loads on P-1, including 3211-P-1. Reactor power was lowered as moderator temperature was rising. 3211-P-3 was started manually on Bank 2 (Bus Q-1 side). Test on CB-322 was terminated. CB-312 was closed, Bus-P1 supply was normalised and all loads restarted. Reactor power was raised after completing preventive maintenance check on CB-322 protection, relay 86 and contacts. Simulation test, keeping CB-322 open, was carried out. But when relay 86 was actuated, Bus P-P1 tie-breaker tripped.
The cause/s	Investigation showed that one relay 86 X going to CB-312 circuit extended trip signal. The relay 86 X was in the circuit but not visualised since it was not included in the drawing.
Human/Ergonomics factors, human performance related and other findings	Incomplete drawing/documentation.
Human reliability quantification/HEPs	Error of omission in drawing. HEP for omission of relay in drawing can be taken to be the same as HEP for omission of a step/important instruction from a formal or ad hoc procedure, which is = 0.003 (5). Data Source: Table 20-5 of the Handbook giving estimated HEPs for errors in the preparation of written material (Appendix-5).

6.2.18 D<sub>2</sub>O Leak from North Fuelling Machine Snout Plug

<b>Plant and Unit</b>	<b>KAPS, Units 1-2</b>
Date, time and plant state when incident occurred	26-02-2002 Unit operating at 220 MWe.
Brief description of event	A high D <sub>2</sub> O leak was suspected to have occurred during refueling of Channel J-5 on 25-02-2002. High Pressure Test of both F/Ms was begun. D <sub>2</sub> O leak noticed from N F/M area during the test. Floor beetle of N F/M service area also alarmed. F/M was isolated. ~180 tons of D <sub>2</sub> O, which had spilled, was collected.
The cause/s	Inspection of N F/M was done. 'O' ring of N F/M was found to be missing. There was a loose connection in control circuit of magazine to snout valve causing it not to freely open during snout plug removal operation during the refueling. During the difficult removal of snout plug the 'O' ring is likely to have slipped out.
Human/Ergonomics factors, human performance related and other findings	Improper maintenance with post maintenance check not done or improperly done.
Human reliability quantification/HEPs	BHEP for maintenance task is taken = 0.03 (5). RF for post maintenance check 0.01. So HEP = 0.03 x 0.01 = 0.0003 (10). (Evaluation using ASEP HRA Procedure).

### 6.3 Case Studies of Detailed Human Reliability Analysis for Two Human Performance Related Events, which Occurred in KAPS.

HRA may be carried out not only as a part of PSA, but also independent of it, in order to arrive at ways to improve operational safety. In this case, the need for formal human error quantification does not necessarily arise and analysis can be a qualitative one. A qualitative analysis may involve identifying potential errors, considering their importance (e.g. by rating their consequences and approximate likelihood of occurrence) and providing error reduction guidance. Quantitative human reliability analysis may also be carried out as a non-PSA driven study by using a HRA method. As part of the study of human performance related events in KAPS, HRA using THERP handbook data is carried out for two of the eighteen events detailed in Section 6.2 above. The aim is to illustrate the application of HRA to plant events. The HRA studies are described below.

#### 6.3.1 HRA of Reactor Trip on PHT System High Pressure, KAPS 2; Date and Time of Event Occurrence : 03.01.2001, 09.25 Hours (Event 6.2.3, Section 6.2).

##### (i) Initial plant state

The plant was under startup and boron removal was in progress to make the reactor critical after poison shutdown. PHTS pressure was being maintained by wide range pressure control. Further investigation was intended to be carried out, of steam generator 4-level controller (LIC 4) hunting problem, noticed earlier during the poison shutdown.

##### (ii) Event sequence and operator actions

- (a) Operator switched off the 240 V AC power supply to LIC 4.
- (b) PHTS pressure rose sharply from 20 Kg/cm<sup>2</sup> to 94.9 kg/cm<sup>2</sup>. This caused IRV to open and PSS tripped on high PHTS pressure. At the same time, coolant channel flow low, ALPAS tank level low and BCD high level window alarms also appeared in the control room.

##### (iii) Analysis of event

- (a) MCB of 240 V AC power supply to SG 4-LIC 4 also supplied power to channel C of PHTS wide range pressure control loop. As this power supply was cut off, channel C transmitter output signal (at the input to the median selector) became zero. Channels A and B should have continued to function undisturbed and no failure should have occurred. But a wire connection in channel PHTS controller was open at the controller panel end, with the result that the channel B signal did not extend to the median selector. Failure of two channels out of three caused the median selector to select a zero median, which in turn caused the feed valves to fully open and bleed valves to fully close.
- (b) To compound the situation, the narrow range/wide range selection relay malfunctioned and the narrow range selection contacts opened out and wide range selection contacts failed to close. Therefore the channel A wide range pressure control signal too did not extend to the median selector. The resulting open circuited channel was picking up stray voltage of 2.5 to 8 volts.
- (c) All this meant that prior to when the 240 V AC power supply was switched off, channel C output (2.4 V) was the median signal and channels A and B were actually ineffective. When the power supply was switched off however, the median output became zero and the reactor tripped.

##### (iv) Human reliability analysis

###### (1) Defining human errors for quantification

- (a) Procedure not followed: The 240 V AC power supply was switched off without following proper procedure.

- (b) Incomplete procedure: The above procedure (for switching off power supply) did not include checks to confirm whether the other two channels of the control affected were functioning as required.
- (c) Post maintenance check not done: Channel B of PHTS controller was open to a cut wire, which remained undetected until event occurrence.

There is no provision made to check whether output signals of all three controllers extend to the median selector and also whether they are in desired range. This can be considered to be a deficiency in design.

(2) Evaluation of HEPs.

As in the earlier case, the HEPs for the above defined human errors are evaluated using the data tables in THERP handbook.

- (a) Procedure not followed : The procedure for switching off control power supply MCBs was not followed. A MCB generally supplies power to many instruments and checking this is an essential step. MCB - 321 supplied power not only to SG #4 level controller but also to PHTS wide range controller channel C. Table 20 - 7 of the handbook (Appendix-5) gives estimated probabilities of errors of omission per item of instruction when use of written procedures is specified. Assuming a written procedure to be available for switching off control power supply MCBs, the HEP for not using the procedure is chosen.  $HEP = 0.05$  (5).
- (b) Incomplete procedure : The procedure used was incomplete since it did not include checks to confirm whether the other two channels (of the control affected by switching of the power supply to a channel controller) are functioning normally as required. Table 20 - 5 of the handbook (Appendix-5) gives estimated HEPs in the preparation of written material. HEP for omitting a step or important instruction in a formal or ad hoc procedure = 0.003 (5), is selected for error of incomplete procedure.
- (c) Post maintenance check not done : Channel B of PHTS controller was open to a cut wire, which remained undetected until event occurrence. This could have been detected if a check had been made after carrying out the maintenance. The handbook indicates that a nominal HEP of 0.003 may be assigned to a general error of omission or commission. HEP for omitting to carry out the post maintenance check, is taken to be 0.003.

(3) PSFs, dependency relations and recovery factors

No information is available in the event report, on the basis of which the above can be assessed. Hence, these are not included in the evaluation.

(4) Overall human reliability

Level of human performance during the event, is assessed by summing the evaluated HEPs.  $Overall\ HEP = 0.05 + 0.003 + 0.003 = 0.056$ . This means that human reliability is 94.4 %. The main contribution to unreliability comes from error made in not following the procedure for switching off control power supply MCBs. Enforcement by management of strict adherence to procedure and provision of requisite training, can reduce the likelihood of error. If HEP is taken to be 0.001 (a more acceptable value), human performance reliability will increase to 99.3 %.

6.3.2 HRA of Reactor Trip on Steam Generator Differential Temperature High and Some Fuel Bundles Crossing Bundle Power Safety Limits, KAPS 1, Date and Time of Event Occurrence: 10.03.2004, 09.24 Hours (Event 6.2.9, Section 6.2).

(i) Initial plant state

The plant was operating at 170 MWe and refuelling was planned. F/M Pump #2 was operating. The fuelling machine was clamped to channel G 05 and the sequence for removal of seal plug was in progress. Preventive maintenance of PUPS #1 input and output circuit breakers and battery charge equalisation was begun.

(ii) Event sequence and operator actions

- (a) Time 09.13 hours: During isolation of PUPS #1 from field, Bus S EMTR initiated, DG #2 and DG #3 started on auto and 48V DC voltage high/low annunciation appeared. electrical maintenance initiated investigation of the problem.
- (b) Control room operators also focused their attention on the EMTR and 48V DC alarms and restoration activities. They did not notice that the 415V power supply to the ARCUs had failed and the adjustors had become inoperable. There was no alarm provided for annunciation of the situation to alert the operators.
- (c) Operators observed that all adjustor rod failed LEDs were glowing and shim rods fully out LEDs had gone off. Shim rods were at fully out position as indicated on meter.
- (d) Time 09.18 hours: Actual power > Demand power window annunciation appeared, which attracted the attention of the control engineer, who also noticed that ALPAS CAM injection LED of channel B was glowing.
- (e) Control room operator inhibited auto CAM injection by setting the hand switch to OFF-RESET position.
- (f) Control maintenance unit (CMU) personnel were called to control room for investigating the cause for adjustor rod blower failed LEDs glowing.
- (g) Channel outlet temperature (COT) high occurred at 09.19 hours, followed by COT very high at 09.22 hours.
- (h) Time 09.23 hours: Reactor setback initiated on COT very high. The condenser dump valves opened on auto due to increase in the boiler pressure control signal.
- (i) Control room operator noticed that reactor power was 83 % and not coming down, even though demand power was being driven down by reactor setback.
- (j) Control room operator was informed by CMU personnel, of the loss of power to all adjustors.
- (k) Time 09.24 hours: Reactor tripped on steam generator DT high. Fuse failure in all four panels of the ARCUs prevented the movement of all adjustors. The regulating signal was positive at the time of failure. As the regulating system's demand for inward movement of adjustors was not met, there was a rise in power. The increase in power caused xenon killing, which caused a further increase in positive reactivity. The reactor power gradually increased from 73 % to 83 % in about 8 minutes and from 93 % to 98 % in about 3 minutes (as per the PSS chart recorder) and the reactor tripped. Subsequent analysis showed that at 98 % FP 140 numbers of bundles crossed bundle power safety limit.

(iii) Human reliability analysis

(1) Defining human errors for quantification

- (a) Improper operator action: Auto action of ALPAS CAM was inhibited without taking cognizance of the reactor power changes and reactor core status.

- (b) Failure to act: Operator failed to actuate manual reactor trip although he noticed that reactor power was 83 % and not coming down by setback action.
- (c) Rules not followed: Trip set points were not set conservatively.

Other human errors included inadequate preventive maintenance procedure (for PUPS) and design deficiency (common fuse in main and backup power supply of ARCUs).

(2) Analysis using THERP handbook

The quick reference guide to data tables given in the handbook (and reproduced in Appendix-5) is used to decide which human error data table to look up. There are tables for a large number of error types. Further, for cognitive function failures, the table of cognitive failure probabilities in Hollnagel (1998), reproduced in Appendix-6 of this report is used. In general, the procedure for human reliability analysis of a task is as follows.

- (a) For each of the defined errors, a basic HEP is selected that most closely resembles the error being assessed.
- (b) Then, any PSFs related to the error and the scenario, are to be considered. The error factor associated with the basic HEP is to be applied in such a way as to modify the basic HEP.
- (c) The value of the HEP is further modified if dependence relations are present.
- (d) Assumptions made in respect of PSFs and dependency relations are to be noted.
- (e) Recovery Factors, if such recoveries are possible, are then applied.
- (f) Errors and recoveries may be represented in a HRA event tree.
- (g) Evaluation of the tree is carried out and overall level of reliability is calculated.
- (h) Sensitivity analysis may be performed if required.
- (i) Finally, the analysis is documented.

(3) Evaluation of HEPs

- (a) Improper operator action - Auto action of ALPAS CAM was inhibited without taking cognizance of the reactor power changes and reactor core status. This error can be considered to be a failure on the part of the operator to correctly assess and interpret the situation. Interpretation is a cognitive function (Hollnagel, 1998). From the table of cognitive failure probabilities (Appendix-7), HEP for interpretation failure is selected = 0.2 (Lower Bound = 0.09, Upper Bound = 0.6).
- (b) Failure to act - Operator failed to actuate manual reactor trip as a conservative safety action although he noticed that reactor power was 83 % and not coming down by setback action. This error can be considered as due to a lack of adequate training in conservative and safety oriented decision-making. Going through the tables, it is found that there is no tabled HEP for this error. Therefore, as indicated in the Handbook (Appendix-5), a nominal HEP of 0.003 is assigned for the failure of the operator to manually trip the reactor. This HEP is then modified by a PSF, of say 5, for the lack of adequate training given to the operator in conservative safety oriented decision making.  $HEP = 0.003 \times 5 = 0.015$ .
- (c) Rules not followed - Lin N trip set points were not set conservatively. The settings were for reactor operation at 90 % FP and had not been changed, although reactor power had been lowered to 70 % FP. During the incident, reactor power increased from 73 % FP to 98 % FP for a short duration. A

conservative approach was not followed, an error due to inadequate administrative control. The error can be considered to be somewhat similar to writing an item incorrectly in a procedure. From Table 20-5 (Appendix 5), which gives the estimated HEPs in the preparation of written material, HEP is selected equal to 0.003 (5).

- (d) Inadequate preventive maintenance for PUPS. Fuse failure in PUPS due to a faulty relay contact and malfunctioning switch isolator led to loss of supply to ARCUs and loss of regulation capacity through the adjustors, which became inoperable. The relay and static switch isolator were not covered in the preventive maintenance procedure, amounting to incomplete procedure error. Table 20-5 (Appendix 5), which gives the estimated HEPs in the preparation of written material. HEP for omitting a step or important instruction in a formal procedure = 0.003 (5). This can be taken as the HEP value for incomplete procedure error.

- (4) PSFs, dependency relations and recovery factors.

A PSF of 5 has been considered for less than adequate operator training in conservative safety oriented decision-making. The high value assumed signifies the importance that needs to be attached to this aspect while imparting training to operators. Dependency relations and recovery factors are not considered, as there is no information related to these aspects in the event report.

- (5) Overall human reliability

An overall human reliability value may be evaluated to give an idea of the level of human performance during the event under consideration. Overall HEP is obtained by summing the HEPs, and is equal to  $0.2 + 0.015 + 0.003 + 0.003 = 0.221$ . This means that human reliability is around 78 %. The main contribution to unreliability comes from operator error in inhibiting auto action of ALPAS CAM (for fear of adding boron when it was not warranted, as refuelling was in progress) followed by error in not manually tripping the reactor as a conservative safety action.

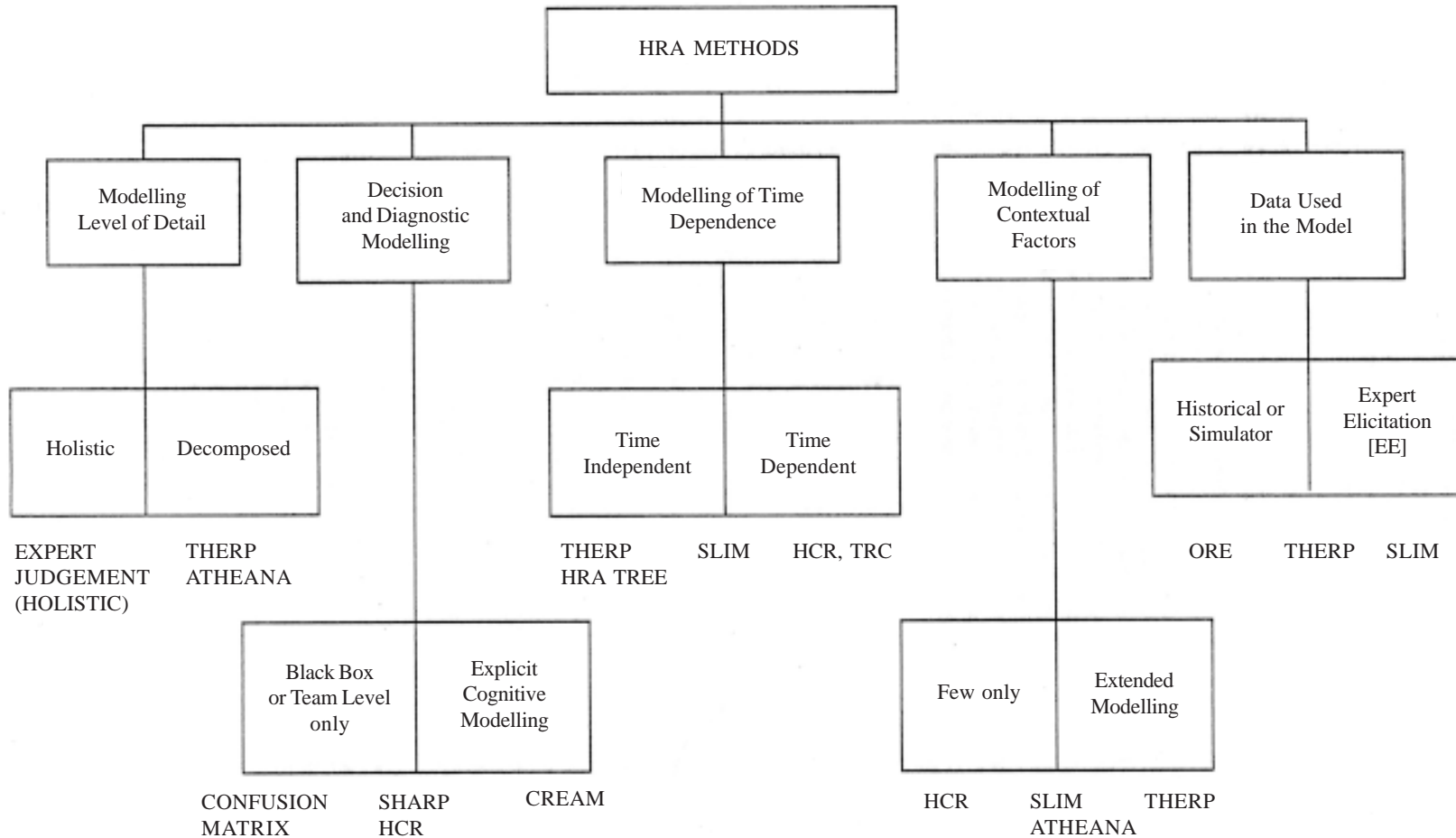
- (6) Sensitivity study

The main difficulty was in recognising that all the adjustors had become inoperable. An annunciation in the control room for loss of 415 V power supply to adjustors would have alerted the operator to their inoperability and prevented the inhibition of auto action of ALPAS CAM. This could have prevented the error from occurring. HEP then reduces to a nominal value of 0.003. In addition, adequate and periodic training in conservative safety oriented decision-making would result in the operator manually tripping the reactor whenever necessary. This HEP too can then be assigned a nominal value of 0.003. The likelihood of the other two errors could, with appropriate administrative control and checks for completeness of preventive maintenance procedures respectively, be reduced to a negligible value. Overall HEP would then become 0.006, taking the reliability of human performance to a more acceptable value of 99.4 %.



## APPENDIX-1 : CLASSIFICATION OF HRA METHODS

150



## APPENDIX-2.1

### OUTLINE OF HUMAN ERROR TAXONOMY

#### 1. Human Error Categories

1.1 Mistake - An error in establishing a course of action, e.g. an error in diagnosis, decision making or planning.

Examples

- Incorrect action arising from an incorrect diagnosis
- Incorrect choice of procedure due to an error in decision-making
- Incorrect planning, say an error in timing an action

1.2 Slip - An error in implementing a plan decision or intention or an unintended action.

Example

- Plan is correct but its execution is wrong

#### 2. Human Error Types

2.1 External error modes

2.1.1 Error of omission

Example

- Omitting a whole task or a step in a task

2.1.2 Error of commission

Examples

- Incorrect performance of an action
- Performing an inappropriate action
- Selection/Transposition error
- Advanced/Delayed action
- Sequence error
- Communication error

2.1.3 Extraneous acts

Example

- Rule violation

2.2 Internal error modes

Examples

- Detection error
- Interpretation error
- Diagnosis error
- Decision error
- Planning error

### 3. **Internal Human Error Mechanisms - Psychological Error Mechanisms (PEMs)**

Examples

- Attention failure/distraction
- Memory failure
  - Memory lapse (a failure to recall)
  - Inaccurate recall (a mistake among alternatives)
- Misdiagnosis
  - Miscuing
  - Spatial discrimination failure
- Misperception
- Misjudgement or misinferencing
- Stereotype takeover
  - Assumptions
  - Mindset
- Spatial misorientation
- Indecision
  - Lack of knowledge
- Uncertainty
- Invoking a shortcut
  - Pressure of time
- Rule violation

### 4. **Human Error Causes - Reasons for Occurrence of Error Influence by the Performance Shaping Factors. Error Causes are Generally Connoted by the PSFs.**

Examples

- Work/task complexity
- Work/task organisation/design
- Work load
- Human - machine interface design
  - Ergonomics factors, human engineering discrepancies
  - Ambiguities
- Procedures
  - Procedure correctness
  - Procedure content
  - Procedure format
  - Procedure violation
- Task criteria
  - Ambiguous/Unclear
- Inadequate supervision/inspection
  - Lack of supervisory checks

- Communication problems
- Improper or unauthorised operation
- Poor skill/inexperience/novelty of task
- Inadequate training/education
  - Refresher training

**5. Stress Factors**

- Psychological
  - Task time
  - Task load
  - Monotony of task
  - Personal factors - character, attitude, emotional state
- Physiological
  - Fatigue
  - Pain
  - Hunger, thirst
  - Temperature

**APPENDIX-2.2 : HUMAN ERROR REPORTING FORM FOR  
NUCLEAR POWER PLANTS**

<b>PLANT HUMAN ERROR REPORTING FORM</b>	
Serial No. _____	Date: _____
Nuclear Power Station: _____	
Unit No. _____	Date and time of event occurrence: _____
<b>A. PROBLEM DESCRIPTION</b>	
Details of event and human performance problem	Plant state
	Pre-event: _____
	Post-event: _____
Number of times a similar or identical problem has previously occurred: _____	
Plant _____ Unit _____ Date and Time _____	
Personnel involved (See list) :	
Hours continuously on duty prior to event : _____	

Page 1

<b>B. HUMAN ERROR DATA</b>
Relevant plant indications prior to the human interactions (signal cues):
1. Alarms: window : _____ CRT display : _____
2. Indicating meters : _____
3. Recorders : _____
4. CRT displays/CRCS : _____
5. Others: _____
Types of activity (See list): _____
Location of the activity (See list):
Time available for the activity (See list):
Type of human error (See list):
Mode of human error (See list):
Cause of human error (See list):

Page 2

**APPENDIX-2.2 : HUMAN ERROR REPORTING FORM FOR  
NUCLEAR POWER PLANTS (CONTD.)**

Effects and consequences of human error:  1. Immediate: _____  2. Long term: _____
Psychological error mechanisms (Not to be filled by the station)
Type of recovery 1. Error alarmed _____ 2. Supervisory check _____ 3. Periodic (shift/day) inspection _____ 4. Post-maintenance/test check _____ 5. Other _____
Systems affected:  USI Nos.

Page 3

Possible improvements to enhance plant operational safety
Form filled by: _____ Checked by STE: _____ Issued by TSS: _____  Approved by SORC: _____
<b>C. ANALYSIS OF THE HUMAN ERROR</b> (Not to be filled by the station)
1. Performance shaping factors: _____ 2. Recovery factors: _____ 3. Basic Human Error Probability: _____ 4. Calculated HEP: _____ 5. Other details: _____

Page 4

## CODE LISTS

<b>PERSONNEL LIST</b>	
<b>Code</b>	<b>Personnel</b>
1CM	Control operator - Main
1AM	Area operator - Main
1CF	Control operator - Fuelling
1AF	Area operator - Fuelling
2M	Control engineer - Main
2F	Control engineer - Fuelling
3M	Area engineer - Main
3F	Area engineer - Fuelling
4M	Assistant shift charge engineer (ASCE) - Main
4F	Assistant shift charge engineer (ASCE) - Fuelling
5	Shift charge engineer (SCE) - Main
6MCM	Maintenance control - Main
6MCF	Maintenance control - Fuelling
6MMM	Maintenance mechanical - Main
6MMF	Maintenance mechanical - Fuelling
6ME	Maintenance electrical
6MS	Maintenance services
7	Other (explain)

<b>ACTIVITY LIST</b>	
<b>Code</b>	<b>Activity</b>
1	Observation/Monitoring
2	Operation/Execution/Control
3	Maintenance
4	Testing
5	Checking
6	Incident/Accident response
7	Other (explain)

<b>TIME LIST</b>	
<b>Code</b>	<b>Time</b>
1	≤ 1 Minute
2	1 Minute < t = 5 Minutes
3	5 Minutes < t ≤ 10 Minutes
4	10 Minutes < t ≤ 30 Minutes
5	30 Minutes < t ≤ 60 Minutes
6	> 60 Minutes

## CODE LISTS (CONTD.)

<b>ERROR TYPE LIST</b>	
<b>Code</b>	<b>Error Type</b>
1	Omission
2	Transposition
3	Inappropriate action
4	Advanced action
5	Delayed action
6	Other (explain)

<b>ERROR MODE LIST</b>	
<b>Code</b>	<b>Error Mode</b>
1	Detection
2	Interpretation, diagnosis
3	Decision
4	Error in action
5	Communication
6	Other (explain)

<b>ERROR CAUSE LIST</b>	
<b>Code</b>	<b>Error Cause</b>
1	Complexity of task/work
2	Work/task organisation
3	Work station design, ergonomics
4	Procedure content inadequacy
5	Procedure format
6	Procedure not followed
7	Unclear task criteria
8	Inadequate supervision, inspection
9	Improper/unauthorised operation or maintenance
10	Poor skill, inadequate experience, training or education
11	Hardware problems
12	Personal (physiological or psychological) causes
13	Communication problems
14	Other (explain)



### CODE LISTS (CONTD.)

LOCATION LIST	
Code	Location
1	Control room
2	Control equipment room
3	Turbine building
4	Reactor building accessible area
5	Reactor building shutdown accessible area
6	Service building
7	Fuelling machine vault
8	MCC and Switchgear area
9	Switchyard
10	Pump house
11	Upgrading plant
12	Dm plant
13	Other (explain)

**APPENDIX-2.3**

**COMPLETED HUMAN ERROR REPORTING FORM  
FOR TYPICAL PLANT EVENT**

<b>PLANT HUMAN ERROR REPORTING FORM</b>	
Serial No.	Date:
Nuclear Power Station: Rajasthan Atomic Power Station	
Unit No. 1	Date and time of event occurrence: 16 - 07 - 1990, 22.14 hours
<b>A. PROBLEMDESCRIPTION</b>	
Details of event and human performance problem	Plant state
Unit was operating at 85 MWe. Channel D biweekly protective system testing was being carried out. While carrying out channel D primary heat transport system high-pressure test, when the channel D dump valves were open, wrongly channel E valves were also opened. Partial moderator dumping took place and reactor tripped.	Pre-event: Power Operation - 85 MWe
	Post-event: Shutdown
Number of times similar or identical problem has previously occurred: Once	
Plant : RAPS                      Unit : 2                      Year : 1983	
Personnel involved (See list): 3M (Area Engineer - Main) 1AM (Area Operator - Main)	
Hours continuously on duty prior to event	
3M (Area Engineer - Main): 6 hours, 1AM (Area Operator - Main): 8 hours or 14 hours	
<b>B. HUMANERRORDATA</b>	
Relevant indications prior to the human interactions (signal cues): Not Applicable	
1. Alarms: window: _____ CRT display _____	
2. Indicating meters: _____	
3. Recorders: _____	
3. CRT displays/CRCS: _____	
4. Others: _____	
Types of activity: 4, Testing	

**APPENDIX-2.3 (CONTD.)**

**COMPLETED HUMAN ERROR REPORTING FORM  
FOR TYPICAL PLANT EVENT**

Location of the activity: 4, Reactor building accessible area
Time available for the activity: 4, 12.5 minutes
Type of human error: 1, Omission
Mode of human error: 1, Detection (Failure to notice that the channel has not been reset).
Cause of human error: 3, Work station design, ergonomics 6, Procedure not followed  The operator omitted to reset the channel under test before proceeding with the test of the second channel. The testing task is a well-practiced task that is routinely carried out by the operator. There is little or no stress on the operator during the performance of the task.
Effects and consequences of human error 1. Immediate: Yes 2. Delayed:
Psychological error mechanisms (Not to be filled by the station) Attentional Failure
Type of recovery: Not Applicable 1. Error alarmed: _____ 2. Supervisory check: _____ 3. Periodic (shift/day) inspection: _____ 4. Post-maintenance/test check: _____ 5. Other: _____

**APPENDIX-2.3 (CONTD.)**

**COMPLETED HUMAN ERROR REPORTING FORM  
FOR TYPICAL PLANT EVENT**

<p>Systems affected: Total station trip</p> <p>USI Nos. 63700</p>
<p>Possible improvements to enhance plant operational safety</p> <ol style="list-style-type: none"><li>1. Control station improvement-channel-wise colour coding, marking of valves.</li><li>2. Aids for following procedure- inclusion of cautionary warning in the written procedure.</li></ol> <p>Form filled by: _____</p> <p>Checked by STE: _____</p> <p>Issued by TSS: _____</p> <p>Approved by SORC: _____</p>
<p><b>C. ANALYSIS OF THE HUMAN ERROR</b> (Not to be filled by the station)</p> <ol style="list-style-type: none"><li>1. Performance shaping factors: (1) Procedure not followed. (2) Quality of control station design.</li><li>2. Recovery factors : Nil</li><li>3. Basic Human Error Probability: The test procedure involves rule-based actions and a written procedure exists. Table 20-7 of the Handbook gives estimated HEPs of errors of omission per item of instruction when written procedure is specified. When a procedure with check-off provisions is incorrectly used, HEP for short list of less than ten items of instruction = 0.003 (EF=3).</li><li>4. Calculated HEP: The above HEP is doubled to 0.006 (EF=3) to take into account the quality of control station design ergonomics.</li><li>5. Other details:</li></ol>
<p><b>Calculation of HEP from plant data:</b></p> <p>A direct calculation of HEP is possible in this case as two identical human failures have occurred in the regular task of biweekly protective system testing at the station. Biweekly protective system testing frequency can be calculated, as the task is a regular task. 12 tests are carried out every month. (3 channels X 2 times a month X 2 units). This gives <math>12 \times 12 \times 2 = 2880</math> tests in 20 years of operation (~3000 opportunities for error in the task). During the period the failure has occurred twice in the station. Hence, <math>HEP = \frac{\text{number of errors}}{\text{number of opportunities for error}} = \frac{2}{3000} = 6.7 \text{ E} - 4</math>.</p>

### APPENDIX-3.1

#### TABULAR FORMAT USED FOR ORGANISING HUMAN ERROR/HUMAN PERFORMANCE EVENT DATA

**TABLE AP-3.1 : SAMPLE HUMAN ERROR/HUMAN PERFORMANCE RELATED EVENT DATA**

No.	Plant ID	HI Type A,B,C	Date, time, plant state, event and task description	Error description	Equipment or controls operated	Location and activity	Error mode - external/ internal	Internal (psychological) error mechanism	Error causes (PSFs)	HEP uncertainty bounds UCBs	Model	Reference source and data pedigree
1.	MAPS Unit 1	B	15/07/85 13.00 hrs. Operation at 233 MWe to shut down. Specific conductivity of boilers 2,3,4 was beyond tech spec limit -150 µmho/cm. During feed water chemical addition.	Instead of hydrazine dosing, phosphate dosing was done.	Phosphate dosing up operated in place of hydrazine dosing pump.	Turbine building operation	Error of commission selection error – A wrong control is selected. transposition error	Attention failure	Work station design			Event report
2.	MAPS Unit 1	B	13/02/88 10.15 hrs. Power operation to shutdown. Room painting.	Shorting of battery bank 2 bus bar terminals by metal ladder carried by painter.	Battery bank 2 bus	Battery room	Inappropriate action	Inadequate attention and care exercised	Lack of work supervision.			Event report
3.	MAPS Unit 1	B	08/01/77 Power operation to shutdown Refuelling successfully	Magazine position was wrongly interpreted, front fuel bundle	Fuelling machine controls	Control room	Error of commission inadvertent operation error in interpretation	Mis-interpretation	Tasks were complex in nature			Event report

**APPENDIX-3.1 (CONTD.)**

**TABULAR FORMAT USED FOR ORGANISING HUMAN ERROR/HUMAN PERFORMANCE EVENT DATA**

**TABLE AP-3.1 : SAMPLE HUMAN ERROR/HUMAN PERFORMANCE RELATED EVENT DATA (CONTD.)**

No.	Plant ID	HI Type A,B,C	Date, time, plant state, event and task description	Error description	Equipment or controls operated	Location and activity	Error mode - external/internal	Internal (psychological) error mechanism	Error causes (PSFs)	HEP uncertainty bounds UCBs	Model	Reference source and data pedigree
			completed. Seal plug leak test begun.	protruded out. But magazine was rotated erroneously. Necessitated complex retrieval operations.								
4.	MAPS Unit 1	B	17/10/89 11.18 hrs. Power operation to shutdown.	HS of 3211-MV-17 (east adjustor rod flow) was erroneously kept in close position.	Adjustor rod cooling flow control	Control Room	Error of Omission-HS not restored to close position.	Detection failure				Event report

## APPENDIX-3.2

### SUMMARY OF RESULTS OF ANALYSIS OF PLANT EVENT DATA

**1. Period of Analysis and Number of Events**

Plant	Period of Analysis	Number of events in the period with human error or human performance related causes
RAPS 1, 2	1972 – 1973 to 1990 – 1991	22
MAPS 1, 2	1983 – 1984 to 1992 – 1993	29

**2. Percentage Distribution of Human Errors with Respect to Activity**

Activity Plant	Operation	Maintenance	Testing
RAPS	36 %	55 %	9 %
MAPS	38 %	47 %	15 %

**3. Percentage Distribution of in terms of Errors of Omission and Errors of Commission**

Plant	Errors of Omission	Errors of Commission
RAPS	18 %	82 %
MAPS	25 %	75 %

**4. Percentage Distribution of Errors of Omission (EOO) and Errors of Commission (EOC) with respect to Activity**

Activity	Operation		Maintenance		Testing	
	RAPS	MAPS	RAPS	MAPS	RAPS	MAPS
EOO	25 %	25 %	8 %	33 %	50 %	0 %
EOC	75 %	75 %	92 %	67 %	50 %	100 %

**5. Percentage Distribution of Types of Errors of Commission (EOC) with respect to Activity**

Activity EOC	Operation		Maintenance		Testing	
	RAPS	MAPS	RAPS	MAPS	RAPS	MAPS
EOC (Total)	75%	75 %	92 %	67 %	50 %	100 %
Type of EOC						
Inappropriate/Improper Action	37%	41 %	75 %	60 %	50 %	60 %
Improper Reading of Instrument	--	--	--	7 %	--	--
Transposition Error	38%	17 %	--	--	--	40 %
Observation Error	--	17 %	--	--	--	--
Other	--	--	17 %	--	--	--

**6. Distribution of Procedural Errors**

Station	RAPS	MAPS
Procedural Errors (as a percentage of the total number of errors)	40 %	32 %

**7. Distribution of Errors with Respect to Plant State (as a percentage of the total number of errors)**

Station	RAPS	MAPS
Plant State		
Startup/Operation	73 %	70 %
Shutdown	27 %	30 %
Percentage of errors in startup/operation which led to shutdown	44 %	86 %

**8. Systemwise Distribution of Errors**

Station	RAPS	MAPS
System		
Electrical System (including TG)	13 %	29 %
PHT System, Bleed Condenser and Bleed Condenser Control	23 %	16 %
Moderator and Moderator Purification	14 %	10 %
Reactor Regulation, Liquid Poison Addition Systems	14 %	10 %
Reactor Protection System	9 %	3 %
Other Systems	27 %	32 %

**9. Locationwise Distribution of Errors**

Station	RAPS	MAPS
Plant Location		
Control Room	32 %	23 %
Turbine Building	4 %	6 %
Reactor Building Shutdown Accessible Area	32 %	13 %
MCC/Switchgear, Battery Room/Switchyard	9 %	19 %
Reactor Building	9 %	16 %
Service Building	4 %	13 %
Other 10 %	10 %	

**10. Distribution of Errors in Morning (M), Afternoon (A) and Night (N) Shifts with respect to Activity**

Station	RAPS				MAPS			
	M	A	N		M	A	N	
Error in:				Total				Total
Operation	18 %	4 %	14 %	36 %	16 %	10 %	12 %	38 %
Maintenance	18 %	18 %	18 %	54 %	17 %	16 %	13 %	46 %
Testing	5 %	5 %	-	10 %	10 %	3 %	3 %	16 %
Total	41 %	27 %	32 %	100 %	43 %	29 %	28 %	100 %

**11. Other Salient Observations**

The analysis of events in RAPS and MAPS, caused by human error/human performance problems, also revealed the following.

- (a) In both plants, internal failure mechanisms (psychological error mechanisms) for the human errors were mainly observation failure, misinterpretation, miscommunication, attention failure and sufficient care not taken.
- (b) In both plants, the main performance shaping factors, which influenced the cause of error, related to procedure (content deficiency or non-compliance), improper action or workstation design problems.



- (c) In MAPS, the largest number of trips due to human error occurred in the night shift, followed by an equal number of trips in the morning and afternoon shifts. More trips occurred in the middle four hours of each shift as compared to first or last two hours of the shift. This could be due to an increase in fatigue as a shift progressed into the middle hours. Contrary to the pattern in MAPS, in RAPS the largest number of trips occurred in the morning shift and least number in the afternoon shift.
- (d) Repeat Occurrence of Error: In both plants, there were five instances each of a repeat occurrence of the same error. The small number of repeat error occurrences indicates that the measures implemented to prevent recurrence of the error had been effective. Only one error among the five had occurred in both RAPS and MAPS.

## APPENDIX-4

### PLANT SPECIFIC HUMAN ERROR PROBABILITIES

Error case	Error event and plant	Error description	Error cause	n errors	N opportunities	HEP = n/N
1.	Error during maintenance RAPS	Spillage of oil, during the process of makeup for the PHTS pump motor bearing, causes the mineral wool insulation surrounding a pipeline to soak up oil. The wool caught fire during operation of the pump.	Carelessness. Improperly carried out maintenance job (makeup of oil in pump motor bearing oil).	2 times in 9 years	1760 (oil makeup is done once a month)	0.001
2.	Error made in operation MAPS	Moderator purification was not kept continuously on during startup from cold shutdown state, and the deuterium concentration in the cover gas went up above the technical specification limit. Reactor had therefore to be shutdown. The purification system had been kept intermittently on to prevent leaching out of boron at 0.1 % or greater FP.	Omission (to keep the moderator purification system continuously on during cold startup) due to uncertainty with respect to the consequences.	2 times	~ 400 (estimate of the number of startups from cold shutdown)	0.005
3.	Error in testing MAPS	Unintentional isolation and draining of a lube oil pressure switch in the TG system, when the intent was to carry out TG lube oil pump 'auto-start' test. The wrong pushbutton was operated.	Transposition of switches/slip due to attention failure and workstation ergonomics factors.	2 times in the station	800 (lube oil pump 'autostart' test every week if units are operating)	0.0025
4 and 5	Error in testing RAPS and MAPS	During biweekly reactor protection system testing, an inadvertent action led to 'simultaneously open' state of the moderator dump valves of the 2/3 RPS channels, and consequent trip of the unit.	Transposition or a slip on account of an attention failure and workstation ergonomics factors.	5 times (RAPS twice, MAPS thrice)	2000 (test done once every two weeks on all the three channels)	0.0025

## APPENDIX-5

### THERP HANDBOOK

There are twenty-seven data tables in the Handbook of Swain and Guttman [25], which is commonly referred to as the THERP HANDBOOK. The twenty seven data tables are reproduced in this appendix. These are for use by HRA analysts, who do not have this literature readily available.

#### 1. List of Data Tables

Table No.	Title of Table
20 - 1	Initial Screening Model of Estimated HEPs and EFs for Diagnosis within time T by control room personnel of abnormal events annunciated closely in time.
20 - 2	Initial Screening Model of Estimated HEPs and EFs for rule-based actions by control room personnel after diagnosis of an abnormal event.
20 - 3	Nominal Model of Estimated HEPs and EFs for Diagnosis within time T by control room personnel of abnormal events annunciated closely in time.
20 - 4	Number of reactor operators and advisors available to cope with an abnormal event and their related levels of dependence: assumptions for PRA.
20 - 5	Estimated HEP per item (or perceptual unit) in preparation of written material.
20 - 6	Estimated HEPs related to failure of administrative control.
20 - 7	Estimated probabilities of errors of omission per item of instruction when use of written procedures is specified.
20 - 8	Estimated probabilities of errors in recalling oral instruction items not written down.
20 - 9	Estimated probabilities of errors in selecting unannunciated displays for quantitative or qualitative readings.
20 - 10	Estimated HEPs for errors of commission in reading and recording quantitative information from unannunciated displays.
20 - 11	Estimated HEPs for errors of commission in checking-reading displays.
20 - 12	Estimated probabilities of errors of commission in operating manual controls.
20 - 13	Estimated HEPs for selection errors for locally operated valves.
20 - 14	Estimated HEPs in detecting stuck locally operated valves.
20 - 15	The four levels of tagging or locking systems.
20 - 16	Modifications of estimated HEPs for stress and experience levels.
20 - 17	Equations of conditional probabilities of success or failure for Task "N", given success or failure on preceding Task "N-1", for four levels of dependence.
20 - 18	Conditional probabilities of success or failure for Task "N" for the five levels of dependence, given FAILURE on preceding Task "N-1".
20 - 19	Conditional probabilities of success or failure for Task "N" for the five levels of dependence, given SUCCESS on preceding Task "N-1".
20 - 20	Guidelines for estimating uncertainty bounds for estimated HEPs.

## APPENDIX-5 (CONTD.)

Table No.	Title of Table
20 - 21	Approximate CHEPs and their UCBs for dependence levels given FAILURE on the preceding task.
20 - 22	Estimated probabilities that a checker will fail to detect errors made by others.
20 - 23	The Annunciator Response Model: Estimated HEPs for multiple annunciators alarming closely in time.
20 - 24	Estimated HEPs for annunciated legend lights.
20 - 25	Estimated probabilities of failure to detect one (of one) unannunciated deviant display at each scan, when scanned hourly.
20 - 26	Estimated probabilities of failing to detect at least one of one to five unannunciated deviant displays as a function of the BHEP for detection of a single deviant display during periodic scanning.
20 - 27	Estimated probabilities that the basic walk-around inspection will fail to detect a particular deviant indication of equipment outside the control room within 30 days.

### 2. List of Acronyms

The acronyms appearing in the 27 tables listed above are as follows.

HEP-Human Error Probability  
 BHEP-Basic Human Error Probability  
 CHEP-Conditional Human Error Probability  
 EF-Error Factor  
 CR-Control Room  
 RO-Reactor Operator  
 AO-Additional Operator  
 SRO-Senior Reactor Operator  
 UCB-Uncertainty Bound

### 3. The Data Tables - Salient Points

- The most frequently observed tasks are listed in the data tables.
- When a task is being evaluated for which there is no tabled HEP, a nominal HEP of 0.003 is assigned as a general error of omission or error of commission, if it is judged that there is some probability of occurrence of either type of error.
- A nominal HEP of 0.001 is assigned to those tasks for which tables indicate that the HEP is 'negligible'.
- Under normal conditions, the nominal HEP of 0.001 allows for the effects of stress that are associated with abnormal events.
- Most tasks list EFs or UCBs. For cases where they are not listed, Table 20-20 provides guidelines for estimating them. While carrying out sensitivity analysis, nominal HEP for some task may change significantly as different assumptions are evaluated. The EFs may change when a nominal HEP is changed. For example, under certain assumptions some task may have a tabled HEP, of say 0.008, with an EF of 3. If the assumptions are modified so that the HEP is doubled to 0.016, the error factor would change from 3 to 5 (See items 2 and 3 in Table 20-20). In addition stress and other PSFs may increase the EFs, as indicated in Table 20-20.

## APPENDIX-5 (CONTD.)

### 4. Quick Reference Guide to the Data Tables

SCREENING	Diagnosis - Table 1 Rule based actions - Table 2
DIAGNOSIS	Nominal diagnosis - Table 3 Post event control room staffing - Table 4
ERRORS OF OMISSION	Written materials mandated <ul style="list-style-type: none"> <li>• Preparation - Table 5</li> <li>• Administrative control - Table 6</li> <li>• Procedural items - Table 7</li> </ul> No written materials <ul style="list-style-type: none"> <li>• Administrative control - Table 6</li> <li>• Oral instruction items - Table 8</li> </ul>
ERRORS OF COMMISSION	Displays <ul style="list-style-type: none"> <li>• Display selection - Table 9</li> <li>• Read/Record quantitative - Table 10</li> <li>• Check-Read quantitative - Table 11</li> </ul> Control and MOV selection and use - Table 12 Locally operated valves <ul style="list-style-type: none"> <li>• Valve selection - Table 13</li> <li>• Stuck valve detection - Table 14</li> </ul>
PERFORMANCE SHAPING FACTORS (PSFs)	Tagging levels - Table 15 Stress/Experience - Table 16 Dependence - Tables 17, 18, 19
UNCERTAINTY BOUNDS (UCBs)	Estimation - Table 20 Conditional HEPs and UCBs - Table 21
RECOVERY FACTORS (RFs)	Errors by checker - Table 22 Annunciated cues - Tables 23, 24 Control room scanning - Tables 25, 28 Basic walk-around inspection - Table 27

### 5. The Twenty Seven Tables from Chapter 20 of the Handbook of Swain and Guttman [25] follow.

TABLES FROM CHAPTER 20 OF THERP HANDBOOK

Table 20-1. Initial-screening model of estimated HEPs and EFs for diagnosis within time T by control room personnel of abnormal events annunciated closely in time

Item	T(min) after Top	HEP for first event	EF	Item	T(min) after Top	HEP for second event	EF
(1)	1	1.0	--	(7)	1	1.0	--
(2)	10	0.5	5	(8)	10	1.0	--
(3)	20	0.1	10	(9)	20	0.5	6
(4)	30	0.01	10	(10)	30	0.1	10
				(11)	40	0.01	10
(5)	60	0.001	10	(12)	70	0.001	10
(6)	1500	0.0001	30	(13)	1510	0.0001	30

Footnotes:

| "Closely in time" refers to cases in which the annunciation of the second abnormal event occurs while CR personnel are still actively engaged in diagnosing and/or planning responses to cope with the first event. This is situation-specific, but for the initial analysis, use "within 10 minutes" as a working definition of "closely in time".

Note that this model pertains to the CR crew rather than to one individual.

| For points between the times shown, the medians and EFs may be determined from Swain and Guttman [25].

a To is a compelling signal of an abnormal situation and is usually taken as a pattern of annunciators. A probability of 1.0 is assumed for observing that there is some abnormal situation.

aa Assign HEP=1.0 for the diagnosis of the third and subsequent abnormal events annunciated closely in time.

Table 20-2. Initial-screening model of estimated HEPs and EFs for rule-based actions by control room personnel after diagnosis of an abnormal event

Item	Potential Errors	HEP	EF
	Failure to perform rule-based actions correctly when written procedures are available and used:		
(1)	Errors per critical step without recovery factors	.05	10
(2)	Errors per critical step with recovery factors	.025	10
	Failure to perform rule-based actions correctly when written procedures are not available or not used:		
(3)	Errors per critical step with or without recovery factors	1.0	--
(4)	Failure to perform an immediate emergency action for the reactor vessel/containment critical parameters, when (a) it can be judged to have been committed to memory, (b) it can be classified as skill-based actions, and there is a backup written procedure	.01	5

Footnotes:

| Note that this model pertains to the CR crew rather than to one individual.

Table 20-3. Nominal model of estimated HEPs and EFs for diagnosis within time 1 by control room personnel of abnormal events associated closely in time[\*].

Item	T(time) after Tc(1)	HEP for first event	EF	Item	T(time)** after Tc(2)	HEP for(##) second event	EF	Item	T(time)** after Tc(3)	HEP for(##) third event	EF
(1)	1	1.0	--	(7)	1	1.0	--	(14)	1	1.0	--
(2)	10	0.1	10	(8)	10	1.0	--	(15)	10	1.0	--
(3)	20	0.01	10	(9)	20	0.1	10	(16)	20	1.0	--
(4)	30	0.001	10	(10)	30	0.01	10	(17)	30	0.1	10
				(11)	40	0.001	10	(18)	40	0.01	10
				(12)	50			(19)	50	0.001	10
(5)	60	0.0001	30	(12)	70	0.0001	30	(20)	80	0.0001	30
(6)	1500	0.00001	30	(13)	1510	0.00001	30	(21)	1520	0.00001	30

Footnotes:

[\*]"Closely in time" refers to cases in which the association of the second abnormal event occurs while CR personnel are still actively engaged in diagnosing and/or planning responses to cope with the first event. This is situation-specific, but for the initial analysis, use "within 10 minutes" as a working definition of "closely in time".

Note that this model pertains to the CR crew rather than to one individual.

The nominal model for diagnosis includes the following activities: "perceive", "discriminate", "interpret", "diagnose", and the first level of "decision-making. The modeling includes those aspects of behaviour included in the Annunciator Response Model; therefore, when the nominal model for diagnosis is used, the annunciator model should not be used for the initial diagnosis. The annunciator model may be used for estimating recovery factors for an incorrect diagnosis.

[\*\*]For points between the times shown, the medians and EFs may be chosen from figure below (press F9 key to look at the figure) and interpolate between tabled values for subsequent events.

[#]To is a compelling signal of an abnormal situation and is usually taken as a pattern of annunciators. A probability of 1.0 is assumed for observing that there is some abnormal situation.

[##]Guidelines for adjusting nominal HEPs are as follows:

- (1) Use upper bound if:
  - (a) the event is not covered in training (or)
  - (b) the event is covered but not practiced except in initial training of operators for becoming licensed (or)
  - (c) the talk-through and interviews show that not all operators know the pattern of stimuli associated with the event.
- (2) Use lower bound if:
  - (a) the event is a well-recognized classic (and)
  - (b) the talk-throughs and interviews indicate that all the operators have a good verbal recognition of the relevant stimulus patterns and know what to do or which written procedures to follow.
- (3) Use nominal HEP if:
  - (a) the only practice of the event is in simulator requalification exercises and all operators have had this experience (or)
  - (b) none of the rules for the use of upper or lower bound apply.

Table 20-4. Number of reactor operators and advisors available to cope with an abnormal event and their related levels of dependence : assumptions for PRA ]

Item	Time after recognition of an abnormal event]	Operators or advisors handling unit affected <sup>a</sup>	Dependence levels with others <sup>b</sup>
(1)	0 to 1 minute	on-duty RO	
(2)	at 1 minute	on-duty RO SRD (assigned SRD or supervisor, an SRD)	high with RO
(3)	at 5 minutes	on-duty RO assigned SRD shift supervisor 1 or more AOs <sup>c</sup>	high with RO low to moderate with other operators
(4)	at 15 minutes	on-duty RO assigned SRD shift supervisor shift technical advisor  1 or more AOs	high with RO low to moderate with other operators low to moderate with others for diagnosis & major events; high to complete for detailed operations

Footnotes:

] These assumptions are nominal and can be modified for plant- and situation-specific conditions.

[For PRA, "recognition" is usually defined as the response to a compelling signal, such as the alarming of one or more annunciators.

<sup>a</sup> No credit is given for additional operators or advisors.

<sup>b</sup> This column indicates the dependence between each additional person and those already on station. The levels of dependence are assumed to remain constant with time and may be modified in a plant-specific analysis.

<sup>c</sup> Availability of other AOs after 5 minutes and related levels of dependence should be estimated on a plant- and situation-specific basis.

Table 20-5. Estimated HEP per item (or perceptual unit<sup>5</sup>) in preparation of written material]

Item	Potential Errors	HEP	EF
(1)	Omitting a step or important instruction from a formal or ad hoc procedure] or a tag from a set of tags.	.003	5
(2)	Omitting a step or important instruction from written notes taken in response to oral instructions <sup>a</sup> .	Negligible	
(3)	Writing an item incorrectly in a formal or ad hoc procedure or on a tag.	.003	5
(4)	Writing an item incorrectly in written notes made in response to oral instructions <sup>a</sup> .	Negligible	

Footnotes:

] Except for simple reading and writing errors, errors of providing incomplete or misleading technical information are not addressed in the Handbook.

The estimates are exclusive of recovery factors, which may greatly reduce the nominal HEPs.

[Formal written procedures are those intended for long-time use; ad hoc written procedures are one-of-a-kind, informally prepared procedures for some special purpose.

<sup>a</sup> A maximum of five items is assumed. If more than five items are to be written down, use .001 (EF=5) for each item in the list.

<sup>5</sup> A perceptual unit is either (1) an individual item such as a display, control, valve, etc., or (2) some functional group of items that are completely dependent and that are the equivalent of a single item with regard to EDNs. It is the operator's perception of what is functionally related that defines this unit.



Table 20-6. Estimated HEPs related to failure of administrative control.

Item	Task	HEP	EF
(1)	Carry out a plant policy or scheduled tasks such as periodic tests or maintenance performed weekly, monthly, or at longer intervals.	.01	5
(2)	Initiate a scheduled shiftily checking or inspection function. Use written operations procedures under:	.001	3
(3)	normal operating conditions	.01	3
(4)	abnormal operating conditions	.005	10
(5)	Use a valve change or restoration list.	.01	3
(6)	Use written test or calibration procedures.	.05	5
(7)	Use written maintenance procedures.	.3	5
(8)	Use a checklist properly.]	.5	5

Footnotes:

] Read a single item, perform the task, check off the item on the list. For any item in which a display reading or other entry must be written, assume correct use of the checklist for that item.

Table 20-7. Estimated probabilities of errors of omission per item of instruction when use of written procedures is specified.]

Item]	Omission of item:	HEP	EF
When procedures with checkoff provisions are correctly used:			
(1)	Short list, <= 10 items	.001	3
(2)	Long list, > 10 items	.003	3
When procedures without checkoff provisions are used, or when checkoff provisions are incorrectly used:			
(3)	Short list, <= 10 items	.003	3
(4)	Long list, > 10 items	.01	3
(5)	When written procedures are available and should be used but are not used:	.05 §	5

Footnotes:

] The estimates for each item (or perceptual unit) presume zero dependence among the items (or units) and must be modified by using the dependence model when a nonzero level of dependence is assumed.

] The term "item" for this column is the usual designator for tabled entries and does not refer to an item of instruction in a procedure.

¶ Correct use of checkoff provisions is assumed for items in which written entries such as numerical values are required of the user.

¶¶ Table 20-6 ("Administrative Control") lists the estimated probabilities of incorrect use of checkoff provisions and of nonuse of available written procedures.

§ If the task is judged to be "second nature", use the lower uncertainty bound for .05, i.e., use .01 (EF=3).

Table 20-8. Estimated probabilities of errors in recalling oral instruction items not written down. (\*\*)

HEPs as a function of number of items to be remembered(\*\*)

Item#	Number of Oral Instruction Items (Perceptual Units)	Pr[F] to recall item "M", order of recall not important		Pr[F] to recall all items, order of recall not important		Pr[F] to recall all items, order of recall is important	
		HEP	EF	HEP	EF	HEP	EF
Oral instructions are detailed:							
(1)	1(##)	.001	3	.001	3	.001	3
(2)	2	.003	3	.004	3	.006	3
(3)	3	.01	3	.02	3	.03	3
(4)	4	.03	3	.04	3	.1	3
(5)	5	.1	3	.2	3	.4	3
Oral instructions are general:							
(6)	1(##)	.001	3	.001	3	.001	3
(7)	2	.006	3	.007	3	.01	3
(8)	3	.02	3	.03	3	.06	3
(9)	4	.06	3	.09	3	.2	3
(10)	5	.2	3	.3	3	.7	3

Footnotes:

(\*) It is assumed that if more than five oral instruction items or perceptual units are to be remembered, the recipient will write them down. If oral instructions are written down, use Table 20-5 for errors in preparation of written procedures and Table 20-7 for errors in their use.

(\*\*) The first column of HEPs (a) is for individual oral instruction items, e.g., the second entry, .003 (item 2a), is the Pr[F] to recall the second of two items, given that one item was recalled, and order is not important. The HEPs in the other columns for two or more oral instruction items are joint HEPs, e.g., the .004 in the second column of HEPs is the Pr[F] to recall both of two items to be remembered, when order is not important. The .006 in the third column of HEPs is the Pr[F] to recall both of two items to be remembered in the order of performance specified.

(#) The term "item" for this column is the usual designator for tabled entries and does not refer to an oral instruction item.

(##) The Pr[F] in rows 1 and 6 are the same as the Pr[F] to initiate the task.

Table 20-9. Estimated probabilities of errors in selecting unannunciated displays or annunciated displays no longer annunciating for quantitative or qualitative readings.

Item	Selection of Wrong Display:	HEP	EF
(1)	when it is dissimilar to adjacent displays]	Negligible	
(2)	from similar-appearing displays when they are on a panel with clearly drawn mimic lines that include displays	.0005	10
(3)	from similar-appearing displays when they are part of well-delineated functional groups on a panel	.001	3
(4)	from an array of similar-appearing displays identified by labels only	.003	3

Footnotes:

| The listed HEPs are independent of recovery factors. In some cases, the content of the quantitative or qualitative indication from an incorrect display may provide immediate feedback of the selection error, and total error can be assessed as negligible.

| This assumes the operator knows the characteristics of the display for which he is searching.

Table 20-10. Estimated HEPs for errors of commission in reading and recording quantitative information from unannounced displays.

Item	Display or Task	HEP	EF
(1)	Analog meter	.003	3
(2)	Digital readout (<=4 digits)	.001	3
(3)	Chart recorder	.006	3
(4)	Printing recorder with large number of parameters	.05	5
(5)	Graphs	.01	3
(6)	Values from indicator lamps that are used as quantitative displays	.001	3
(7)	Recognize that an instrument being read is jammed, if there are no indicators to alert the user	.1	5
	Recording task: Number of digits or letters to be recorded:		
(8)	<= 3	Negligible	
(9)	> 3	.001 (per symbol)	3
(10)	Simple arithmetic calculations with or without calculators	.01	3
(11)	Detect out-of-range arithmetic calculations	.05	5

Footnotes:

| Multiply HEPs by 10 for reading quantitative values under a high level of stress if the design violates a strong populational stereotype; e.g., a horizontal analog meter in which values increase from right to left.

| In this case, "letters" refer to those that convey no meaning. Groups of letters such as MOV do convey meaning, and the recording HEP is considered to be negligible.

Table 20-11. Estimated HEPs for errors of commission in check-reading displays.

Item	Display or Task	HEP	EF
(1)	Digital indicators (these must be read, there is no true check-reading function for digital displays)	.001	3
	Analog meters:		
(2)	with easily seen limit marks	.001	3
(3)	with difficult-to-see limit marks, such as scribe lines	.002	3
(4)	without limit marks	.003	3
	Analog-type chart recorders:		
(5)	with limit marks	.002	3
(6)	without limit marks	.006	3
(7)	Confirming a status change on a status lamp	Negligible <sup>a</sup>	
(8)	Misinterpreting the indication on the indicator lamps	Negligible <sup>a</sup>	

Footnotes:

| "Check-reading means reference to a display merely to see if the indication is within allowable limits; no quantitative reading is taken. The check-reading may be done from memory or a written checklist may be used. The HEPs apply to displays that are checked individually for some specific purpose, such as a scheduled requirement, or in response to some developing situation involving that display.

| If operator must hold a switch in a spring-loaded position until a status lamp lights, use HEP=.003 (EF=3), from Table 20-12 (Errors of commission in operating manual controls), item 10.

<sup>a</sup> For levels of stress higher than optimal, use HEP=.001 (EF=3).

Table 20-12. Estimated probabilities of errors of commission in operating manual controls.]

Item	Potential Errors	HEP	EF
(1)	Inadvertent activation of a control		Situation-specific
(1A)	Select wrong control when it is dissimilar to adjacent controls Select wrong control on a panel from an array of similar-appearing controls]	Negligible	
(2)	Identified by labels only	.003	3
(3)	arranged in well-delineated functional groups	.001	3
(4)	which are part of well-defined mimic layout	.0005	10
	Turn rotary control in wrong direction [for two-position switches, see item 8):		
(5)	when there is no violation of populational stereotypes	.0005	10
(6)	when design violates a strong populational stereotype and operating conditions are normal	.05	5
(7)	when design violates a strong populational stereotype and operation is under high stress	.5	5
(8)	Turn a two-position switch in wrong direction or leave it in wrong setting	e	
(9)	Set a rotary control to an incorrect setting [for two-position switches, see item 8)	.001	10ee
(10)	Failure to complete change of state of a component if switch must be held until change is completed Select wrong circuit breaker in a group of circuit breakers]	.003	3
(11)	densely grouped and identified by labels only	.005	3
(12)	when PSFs are more favourable	.003	3
(13)	Inproperly mate a connector (this includes failure to seat connectors completely and failure to test locking features of connectors for engagement)	.003	3

Footnotes:

| The HEPs are for errors of commission only and do not include any errors of decision as to which controls to activate.

| If controls or circuit breakers are to be restored and are legged, adjust the tabled HEPs according to Table 20-15 (Tagging levels).

e Divide HEPs for rotary controls (items 5-7) by 5 (use the same EFs).

ee This error is a function of clarity with which indicator position can be determined; designs of control knobs and their position indications vary greatly. For plant specific analyses, an EF of 3 may be used.

Table 20-13. Estimated HEPs for selection errors for locally operated valves.

Item	Potential Errors	HEP	EF
	Making an error of selection in changing or restoring a locally operated valve when the valve to be manipulated is:		
(1)	Clearly and unambiguously labeled, set apart from valves that are similar in all of the following: size and shape, state, and presence of tags]	.001	3
(2)	Clearly and unambiguously labeled, part of a group of two or more valves that are similar in one of the following: size and shape, state, or presence of tags]	.003	3
(3)	Unclearly or ambiguously labeled, set apart from valves that are similar in all of the following: size and shape, state, and presence of tags]	.005	3
(4)	Unclearly or ambiguously labeled, part of a group of two or more valves that are similar in one of the following: size and shape, state, or presence of tags]	.008	3
(5)	Unclearly or ambiguously labeled, part of a group of two or more valves that are similar in all of the following: size and shape, state, and presence of tags]	.01	3

Footnotes:

| Unless otherwise specified, Level 2 tagging is presumed. If other levels of tagging are assessed, adjust the tabled HEPs according to Table 20-15 (Tagging Levels).

Table 20-14. Estimated HEPs in detecting stuck locally operated valves.

Item	Potential Errors	HEP	EF
	Given that a locally operated valve sticks as it is being changed or restored] the operator fails to notice the sticking valve, when it has:		
(1)	A position indicator]only	.001	3
(2)	A position indicator]and a rising stem	.002	3
(3)	A rising stem but no position indicator]	.005	3
(4)	Neither rising stem nor position indicator]	.01	3

Footnotes:

| Equipment reliability specialists have estimated that the probability of a valve's sticking in this manner is approximately .001 per manipulation, with an error factor of 10.

| A position indicator incorporates a scale that indicates the position of the valve relative to a fully opened or fully closed position. A rising stem qualifies as a position indicator if there is a scale associated with it.

Table 20-15. The four levels of tagging or locking systems.

Level	Description	Modifications to Nominal HEPs]
1	A specific number of tags is issued for each job. Each tag is numbered or otherwise uniquely identified. A record is kept of each tag, and a record of each tag issued is entered in a suspense sheet that indicates the expected time of return of the tag; this suspense sheet is checked each shift by the shift supervisor. An operator is assigned the job of tagging controller as a primary duty. For restoration, the numbers on the removed tags are checked against the item numbers in the records, as a recovery factor for errors of omission or selection. OR The number of keys is carefully restricted and under direct control of the shift supervisor. A signout board is used for the keys. Keys in use are tagged out, and each incoming shift supervisor takes an inventory of the keys.	Use lower UCBs
2	Tags are not accounted for individually - the operator may take an unspecified number 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. For restoration, the record keeping does not provide a thorough checking for errors of omission or selection. If an operator is assigned as tagging controller, it is a collateral duty, or the position is rotated among operators too frequently for them to maintain adequate control tags and records and to retain skill in detecting errors of omission or selection. OR The shift supervisor retains control of the keys and records their issuance but does not use visual aids such as signout boards or tags.	Use nominal HEPs
3	Tags are used, but record keeping is inadequate to provide the shift supervisor with positive knowledge of every item of equipment that should be tagged or restored. No tagging controller is assigned. OR Keys are generally available to users without logging requirements.	Use upper UCBs
4	No tagging system exists. OR No locks and keys are used.	Perform separate analysis

Footnotes:

] The nominal HEPs are those in the Handbook that relate to tasks involving the application and removal of tags and, unless otherwise specified, are based on Level 2 tagging.

Table 20-16. Modifications of estimated HEPs for effects of stress and experience levels.

Item	Stress Level	Modifiers for Nominal HEPs]	
		(a)Skilled]	(b)Novice]
(1)	Very low (Very low task load):  Optimum (Optimum task load):	x2	x2
(2)	Step-by-step	x1	x1
(3)	Dynamic	x1	x2
(4)	Moderately high (Heavy task load): Step-by-step	x2	x4
(5)	Dynamic	x5	x10
(6)	Extremely high (Threat stress) Step-by-step	x5	x10
(7)	Dynamic Diagnosis	.25 (EF=5)	.50 (EF=5)

These are the actual HEPs to use with dynamic tasks or diagnosis - they are NOT modifiers.

Footnotes:

] The nominal HEPs are those in the data tables. Error factors are listed in

Table 20-17. Equations for conditional probabilities of success and failure on Task "N", given success or failure on previous Task "N-1", for different levels of dependence.

Level of Dependence	Success Equation	Equation No.	Failure Equation	Equation No.
ZD	$P[S(N)/S(N-1)] = n$	(10-9)	$P[F(N)/F(N-1)] = N$	(10-14)
LD	$P[S(N)/S(N-1)] = (3+19n)/20$	(10-10)	$P[F(N)/F(N-1)] = (1+19N)/20$	(10-15)
MD	$P[S(N)/S(N-1)] = (3+6n)/7$	(10-11)	$P[F(N)/F(N-1)] = (1+6N)/7$	(10-16)
HD	$P[S(N)/S(N-1)] = (3+n)/2$	(10-12)	$P[F(N)/F(N-1)] = (1+N)/2$	(10-17)
CD	$P[S(N)/S(N-1)] = 1.0$	(10-13)	$P[F(N)/F(N-1)] = 1.0$	(10-18)

Table 20-18. Conditional probabilities of success or failure for Task "N" for the five levels of dependence, given FAILURE on preceding Task "N-1".

Task "N" Conditional Probabilities(\*)

Item	ZD(**)		LD		MD		HD		CD	
	S	F	S	F	S	F	S	F	S	F
	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)
(1)	.75	.25	.71	.29	.64	.36	.37	.63	0	1.0
(2)	.9	.1	.86	.14	.77	.23	.45	.55	0	1.0
(3)	.95	.05	.9	.1	.81	.19	.47	.53	0	1.0
(4)	.98	.02(0)	.94	.06	.85	.15	.49	.51	0	1.0
(5)	.995	.005	.95	.05	.86	.14	.50	.50	0	1.0
(6)	.999	.001	.95	.05	.86	.14	.50	.50	0	1.0
(7)	.9995	.0005	.95	.05	.86	.14	.50	.50	0	1.0
(8)	.9999	.0001	.95	.05	.86	.14	.50	.50	0	1.0
(9)	.99999	.00001	.95	.05	.86	.14	.50	.50	0	1.0

Footnotes:  
 (\*) All conditional probabilities are rounded. Equations 10-14 through 10-18 (Table 20-17 - Dependence Equations) were used to calculate the values in the F columns. The values in the S columns were obtained by subtraction.  
 (\*\*)The conditional probabilities given ZD are the basic probabilities for Task "N".  
 (0) For FAA purposes, it is adequate to use CEPS of .05 (for LD), .15 (for MD), and .5 (for HD) when SREP <= .01.

Table 20-19. Conditional probabilities of success or failure for Task "N" for the five levels of dependence, given SUCCESS on preceding Task "N-1".

Task "N" Conditional Probabilities(\*)

Item	ZD(**)		LD		MD		HD		CD	
	S	F	S	F	S	F	S	F	S	F
	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)
(1)	.75	.25	.76	.24	.79	.21	.87	.13	1.0	0
(2)	.9	.1	.9	.1	.91	.09	.95	.05	1.0	0
(3)	.95	.05	.95	.05	.94	.06	.97	.03	1.0	0
(4)	.99	.01	.99	.01	.991	.009	.996	.004	1.0	0
(5)	.995	.005	.995	.005	.996	.004	.997	.003	1.0	0
(6)	.999	.001	.999	.001	.999	.001	.9995	.0005	1.0	0
(7)	.9995	.0005	.9995	.0005	.9995	.0005	.9997	.0003	1.0	0
(8)	.9999	.0001	.9999	.0001	.99991	.00009	.99995	.00005	1.0	0
(9)	.99999	.00001	.99999	.00001	.999991	.000009	.999995	.000005	1.0	0

Footnotes:  
 (\*) All conditional probabilities are rounded. Equations 10-9 through 10-13 (Table 20-17 - Dependence Equations) were used to calculate the values in the S columns. The values in the F columns were obtained by subtraction.  
 (\*\*)The conditional probabilities given ZD are the basic probabilities for Task "N".

Table 20-20. General guidelines for estimating uncertainty bounds for estimated HEPs.]

Item	Task and HEP Guidelines]	E <sub>F</sub>
	Task consists of performance step-by-step procedures <sup>ee</sup> conducted under routine circumstances (e.g., a test, maintenance, or calibration task); stress level is optimal:	
(1)	Estimated HEP < .001	10
(2)	Estimated HEP .001 to .01	3
(3)	Estimated HEP > .01	5
	Task consists of performance of step-by-step procedures <sup>ee</sup> but carried out in nonroutine circumstances such as those involving a potential turbine/reactor trip; stress level is moderately high:	
(4)	Estimated HEP < .001	10
(5)	Estimated HEP <= .001	5
	Task consists of relatively dynamic <sup>ee</sup> interplay between operator and system indications, under routine conditions, e.g., increasing or reducing power; stress level is optimal:	
(6)	Estimated HEP < .001	10
(7)	Estimated HEP <= .001	5
(8)	Task consists of relatively dynamic <sup>ee</sup> interplay between operator and system indications but carried out in nonroutine circumstances; stress level is moderately high	10
(9)	Any task performed under extremely high stress conditions, e.g., large LOCA; conditions in which status of ESFs is not perfectly clear; or conditions in which the initial operator responses have proved to be inadequate and now severe time pressure is felt	5 <sup>§</sup>

Footnotes:

] The estimates in this table apply to experienced personnel.

[ For UCBs for HEPs based on the dependence model, see Table 20-21 (Conditional HEPs & UCBs).

<sup>e</sup> The highest upper bound is 1.0.

<sup>ee</sup> See Table 20-16 (Stress - Experience) for definitions of step-by-step and dynamic procedures.

<sup>§</sup> An E<sub>F</sub> of 5 is assigned for the extremely high stress conditions because the upper UCB is truncated at 1.0, and it is desirable to have a more conservative (i.e., higher) lower UCB for such tasks.

Table 20-20 (Estimate UCBs).

[ A skilled person is one with 6 months or more experience in the tasks being assessed. A novice person is one with less than 6 months experience. Both levels have the required licensing or certificates.

<sup>e</sup> Step-by-step tasks are routine, procedurally guided tasks, such as carrying out written calibration procedures. Dynamic tasks require a higher degree of man-machine interaction, such as decision-making, keeping track of several functions, controlling several functions, or any combination of these. These requirements are the basis of the distinction between step-by-step tasks and dynamic tasks, which are often involved in responding to an abnormal event.

<sup>ee</sup> Diagnosis may be carried out under varying degrees of stress, ranging from optimum to extremely high (threat stress). For threat stress, the HEP of .25 is used to estimate performance of an individual. Ordinarily, more than one person will be involved. Tables 20-1 (Diagnosis - screening model) and 20-3 (Diagnosis - seminal model) list joint HEPs based on the number of control room personnel presumed to be involved in the diagnosis of an abnormal event for various times after announcement of the event, and their presumed dependence levels, as presented in the staffing model in Table 20-4



Table 20-21. Approximate CBEPs and their UCs for dependence levels(\*) given FAILURE on the preceding task.

Item	Levels of Dependence					
	(a)	(b)	(c)	(d)	(e)	(f)
(1) ZD**	.03 (EF=3, 1.0)	.05 (EF=5)	.1 (EF=5)	.15 (EF=5)	.2 (EF=5)	.25 (EF=5)
(2) LD	.05 (.015, .16)	.1 (.04, .25)	.15 (.06, .5)	.19 (.06, .75)	.24 (.06, 1.0)	.29 (.08, 1.0)
(3) MD	.15 (.04, .5)	.19 (.07, .53)	.25 (.1, .55)	.27 (.1, .75)	.31 (.1, 1.0)	.36 (.13, 1.0)
(4) HD	.5 (.25, 1.0)	.53 (.28, 1.0)	.55 (.3, 1.0)	.58 (.34, 1.0)	.6 (.36, 1.0)	.63 (.4, 1.0)
(5) CD	1.0 (.5, 1.0)	1.0 (.53, 1.0)	1.0 (.55, 1.0)	1.0 (.58, 1.0)	1.0 (.6, 1.0)	1.0 (.63, 1.0)

Footnotes:

(\*) Values are rounded. All values are based on skill personnel (i.e., those with > 6 months experience on the task being analyzed).

(\*\*) LD = BHP. Efs for BHEPs should be based on Table 20-20 (Estimate Uncertainty Bounds).

(#) Linear interpolation between stated CBEPs (and UCs) to values of BHEPs between those listed is adequate for most PRA studies.

Table 20-22. Estimated probabilities that a checker will fail to detect errors made by others

Item	Checking operation	HEP	EF
(1)	Checking routine tasks, checker using written materials (includes over-the-shoulder inspections, verifying position of locally operated valves, switches, circuit breakers, connectors, etc., and checking written lists, tags, or procedures for accuracy)	.1	5
(2)	Same as above, but without written materials	.2	5
(3)	Special short-term, one-of-a-kind checking with alerting factors	.05	5
(4)	Checking that involves active participation, such as special measurements	.01	5
	Given that the position of a locally operated valve is checked (item 1 above), noticing that it is not completely opened or closed:		
(5)	Position indicator[only]	.1	5
(6)	Rising stem with or without position indicator]	.5	5
(7)	Neither a position indicator[nor rising stem]	.9	5
(8)	Checking by reader/checker of the task performer in a two-man team, OR checking by a second checker, routine task (no credit for more than 2 checkers)	.5	5
(9)	Checking the status of equipment if that status affects one's safety when performing his tasks	.001	5
(10)	An operator checks change or restoration tasks performed by a maintainer	Above HEPs of 2	5

Footnotes:

| This table applies to cases during normal operating conditions in which a person is directed to check the work performed by others either as the work is being performed or after its completion.

| A position indicator incorporates a scale that indicates the position of the valve relative to a fully opened or fully closed position. A rising stem qualifies as a position indicator if there is a scale associated with it.

Table 20-23. The Annunciator Response Model; estimated HEPs(\*) for multiple annunciators alarming closely in time(\*\*).

Item	Number of ANNs	Pr[F1] for each annunciator (ANN) or completely dependent set of ANNs successively addressed by the operator										Pr[F1]†	
		(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)		
(1)	1	.0001											.0001
(2)	2	.0001	.001										.0006
(3)	3	.0001	.001	.002									.001
(4)	4	.0001	.001	.002	.004								.002
(5)	5	.0001	.001	.002	.004	.008							.003
(6)	6	.0001	.001	.002	.004	.008	.016						.004
(7)	7	.0001	.001	.002	.004	.008	.016	.032					.005
(8)	8	.0001	.001	.002	.004	.008	.016	.032	.064				.02
(9)	9	.0001	.001	.002	.004	.008	.016	.032	.064	.13			.03
(10)	10	.0001	.001	.002	.004	.008	.016	.032	.064	.13	.25		.05
(11)	11-15												.10
(12)	16-20												.15
(13)	21-40												.20
(14)	>40												.25

Footnotes:

(\*) The HEPs are for the failure to initiate some kind of intended corrective action as required. The action carried out may be correct or incorrect and is analyzed using other tables. The HEPs include the effects of stress and should not be increased in consideration of stress effects. EF of 10 is assigned to each HEP. Based on computer simulation, use of EF of 10 for Pr[F1] yields approximately correct upper bounds for the 95th percentile. The corresponding lower bounds are too high; they are roughly equivalent to 25th percentile rather than the usual 5th percentile bounds. Thus, use an EF of 10 for the mean Pr[F1] values provide a conservative estimate since lower bounds are biased high.

(\*\*) "Closely in time" refers to cases in which two or more annunciators alarm within several seconds or within a time period such that the operator perceives them as a group of signals to which he must selectively respond.

(†) Pr[F1] is the expected Pr[F1] to initiate action in response to a randomly selected ANN (or completely dependent set of ANNs) in a group of ANNs competing for the operator's attention. It is the arithmetic mean of the Pr[F1]s in a row, with upper limit of .25. The column (k) assumes that all of the ANNs (or completely dependent sets of ANNs) are equal in terms of the probability of being noticed.

Table 20-24. Estimated HEPs for annunciator legend lights

Item	Task	HEP	EF
(1)	Respond to one or more annunciator legend lights	See Annunciator Response Model	
(2)	Resume attention to a legend light within 1 minute after an interruption (sound and blinking cancelled before interruption)	.001	3
(3)	Respond to a legend light if more than 1 minute elapses after an interruption (sound and blinking cancelled before interruption)	.95	5
(4)	Respond to a steady-on legend light during initial audit	.90	5
(5)	Respond to a steady-on legend light during other hourly scans	.95	5

Footnotes:

| No written materials are used.

| "Respond" means to initiate some action in response to the indicator whether or not the action is correct. It does not include the initial acts of cancelling the sound and the blinking; these are assumed to always occur.

Table 20-25. Estimated probabilities of failure to detect one (of one) unannunciated deviant display [at each scan, when scanned hourly]

Item	Display Type	[Initial Audit]							
		1	2	3	4	5	6	7	8
		(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
Analog meters:									
(1)	with limit marks	.05	.31	.50	.64	.74	.81	.86	.90
(2)	without limit marks	.15	.47	.67	.80	.87	.92	.95	.97
Analog-type chart recorders:									
(3)	with limit marks	.10	.40	.61	.74	.83	.89	.92	.95
(4)	without limit marks	.30	.58	.75	.85	.91	.94	.97	.98
(5)	Annunciator light no longer annunciating	.90	.95	.95	.95	.95	.95	.95	.95
(6)	Legend light other than annunciator light	.98	.98	.98	.98	.98	.98	.98	.98
(7)	Indicator lamp	.99	.99	.99	.99	.99	.99	.99	.99

Footnotes:

\* "One display" refers to a single display or a group of completely dependent displays, i.e., a perceptual unit.

\*\* For error factors, refer to Table 20-20 (Estimate Uncertainty bounds).

# Written materials not used.

#\* These displays are rarely scanned more than once per shift, if at all. HEPs for each are listed for completeness only.

Table 20-26. Estimated probabilities of failing to detect at least one of one to five unannunciated deviant displays as a function of the BHEP for detection of a single deviant display during periodic scanning.

Item	BHEP (a)	Number of Deviant Indications			
		2 (b)	3 (c)	4 (d)	5 (e)
		Pr[F] to detect at least one deviant display			
(1)	.99	.985	.98	.975	.97
(2)	.95	.93	.90	.88	.86
(3)	.90	.85	.81	.77	.73
(4)	.80	.72	.65	.58	.52
(5)	.70	.59	.51	.43	.37
(6)	.60	.48	.39	.31	.25
(7)	.50	.37	.28	.21	.16
(8)	.40	.28	.20	.14	.10
(9)	.30	.19	.13	.08	.05
(10)	.20	.12	.07	.04	.03
(11)	.10	.05	.03	.02	.01
(12)	.05	.03	.01	.007	.004
(13)	.01	.005	.003	.001	.001

Footnotes:

\* To estimate the HEP for failure to detect other concurrent unannunciated deviant displays when one has been detected, use the HEP for the initial audit for those displays that are not functionally related to the display detected (from Table 20-25 - Scanning - One Deviant Display) and use the Annunciator Response Model for those displays that are functionally related to the display detected (from Table 20-23 - Annunciator Response Model). The HEPs apply when no written materials are used.

\*\* For EFs, refer to Table 20-20 (Estimate Uncertainty Bound).

Table 20-27. Estimated probabilities that the basic walk around inspection will fail to detect a particular deviant indication of equipment outside the control room within 30 days]

Item	Number of days between walk-arounds per Inspector	Cumulative Pr[F] within 30 days given one inspection per shift
(1)	1 (daily walk-around for each inspector)	.52
(2)	2	.25
(3)	3	.05
(4)	4	.003
(5)	5	.0002
(6)	6	.0001
(7)	7 (weekly walk-around for each inspector)	.0001

Footnotes:

| One of the assumptions for basic walk-around inspections is that no written procedure is used; if a written procedure is used for a walk-around, use the tables related to errors of omission and commission for performance of rule-based tasks.

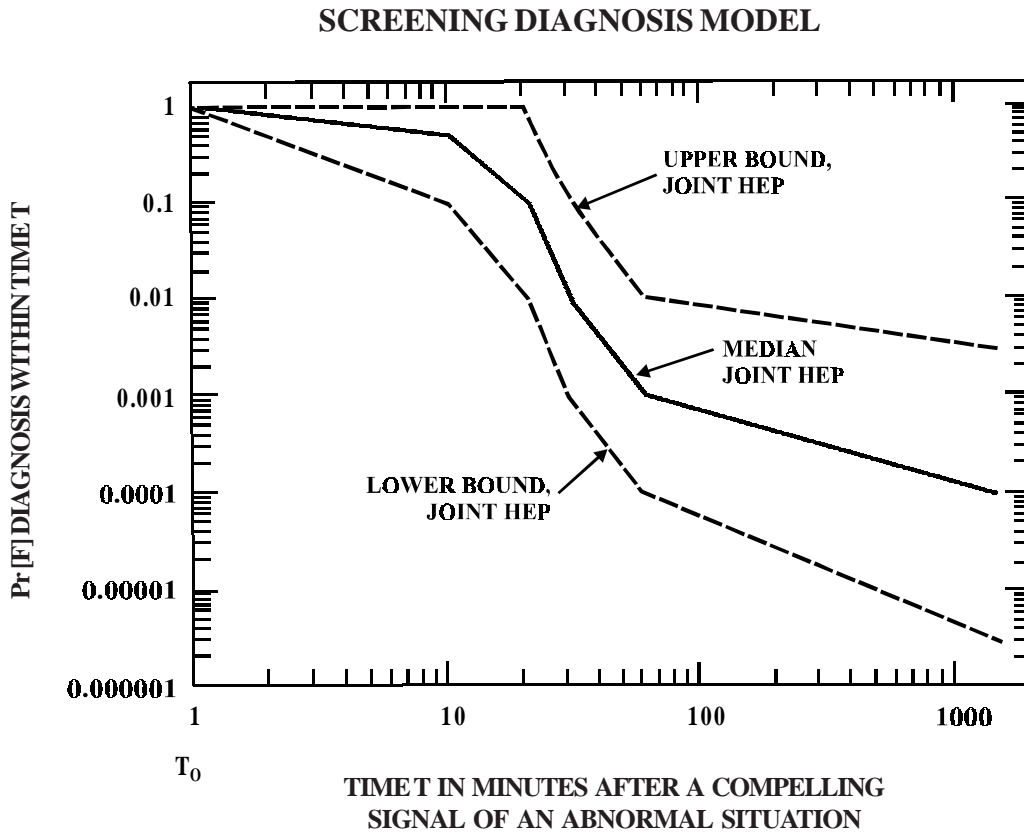
| Three shifts per day are assumed.

■ It is assumed that all inspectors have the same number of days between walk-arounds.

■ For EFs, use the procedure for UCBs propagation or use EF-10 as an approximation.

APPENDIX-6

ACCIDENT SEQUENCE EVALUATION PROGRAMME (ASEP)  
SCREENING AND NOMINAL DIAGNOSIS MODELS AND HEP TABLES,  
HCR CORRELATION AND EDF TIME RELIABILITY CURVES



**FIGURE AP6-1 : INITIAL SCREENING MODEL OF ESTIMATED HEPs AND UCBs FOR DIAGNOSIS WITHIN TIME T OF ONE ABNORMAL EVENT BY CONTROL ROOM PERSONNEL.**

APPENDIX-6 (CONTD.)

ACCIDENT SEQUENCE EVALUATION PROGRAMME (ASEP)  
SCREENING AND NOMINAL DIAGNOSIS MODELS AND HEP TABLES,  
HCR CORRELATION AND EDF TIME RELIABILITY CURVES

NOMINAL DIAGNOSIS MODEL

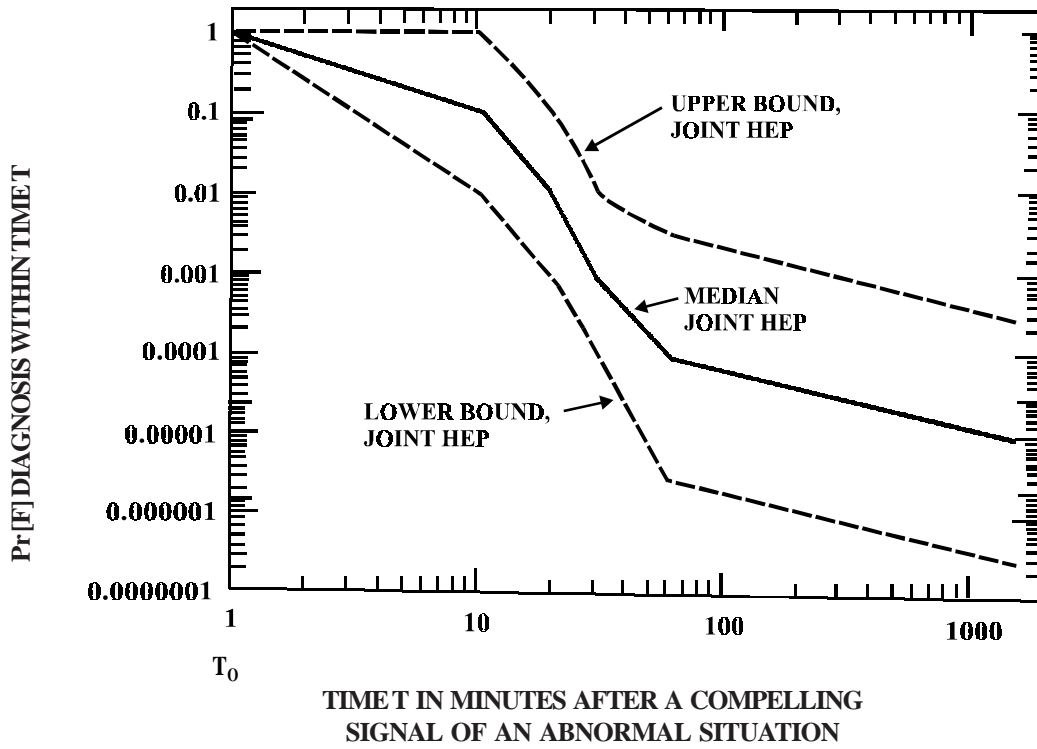


FIGURE AP6-2: NOMINAL MODEL OF ESTIMATED HEPs AND UCBs FOR DIAGNOSIS WITHIN TIME T OF ONE ABNORMAL EVENT BY CONTROL ROOM PERSONNEL

**TABLE 7.2 of [26] : INITIAL SCREENING MODEL OF ESTIMATED HEPs AND EFs FOR DIAGNOSIS WITHIN TIME T BY CONTROL ROOM PERSONNEL OF ABNORMAL EVENTS ANNUNCIATED CLOSELY IN TIME**

The above table in ASEP HRA Procedure (NUREG/CR - 4772) is identical to Table 20-1 given in Appendix-5. It is therefore not reproduced here.

**TABLE 7.3 of [26] : ASSESSMENT OF SCREENING HEPs FOR POST-ACCIDENT POST-DIAGNOSIS ACTIONS**

Item	HEP	EF	Action*
(1)	1.0	–	Perform a required action outside of control room
(2)	1.0	–	Perform a critical skill-based or rule-based action correctly when no written procedures are available. (Details of skill-based actions are not required to be written, if they can be classified as “skill-of-the-craft). This assessment is used even though it may be required for personnel to have memorised these actions. Instead they would like to refer to the written procedures at a later time during the usual checking to see that all immediate emergency actions have been performed correctly.
HEPs (3) and (4) are for performing a critical procedural action under ‘moderately high stress’ ** or ‘extremely high stress’ **. For screening, at least moderately high stress is assessed for post-accident conditions. Also for screening do not give any credit for recovery factors, e.g. a second person. Assume that only one person is available to perform post-diagnosis tasks, and no one is available to check his accuracy.			
(3)	0.05	5	Perform a critical procedural action correctly under moderately high stress.
(4)	0.25	5	Perform a critical procedural action correctly under extremely high stress.
(5)	0.02	5	Perform a post-diagnosis immediate emergency action for the reactor vessel/containment critical parameters, when (a) it can be judged to have been committed to memory (b) it can be classified as skill-based actions and (c) there is a backup written procedure.

\* The HEPs are for independent actions or independent sets of actions in which the actions making up the set can be judged to be completely dependent. Other levels of dependence among actions can be assessed by the analyst, using one or more methods for assessing dependence, described in Chapter 10 of NUREG/CR-1278.

\*\* Moderately High Stress Level - A level of disruptive stress that will result in a moderate deterioration in performance effectiveness of system required behaviour of most people. Extremely High Stress Level - A level of disruptive stress in which the performance of most people will deteriorate drastically.

**TABLE 8.2 of [26] : NOMINAL MODEL OF ESTIMATED HEPs AND EFs FOR  
DIAGNOSIS WITHIN TIME T BY CONTROL ROOM  
PERSONNEL OF ABNORMAL EVENTS ANNUNCIATED  
CLOSELY IN TIME**

The above table in ASEP HRA Procedure (NUREG /CR - 4772) is identical to Table 20-3 given in Appendix-5. It is therefore not reproduced here.

**TABLE 8.3 of [26] : GUIDELINES FOR ADJUSTING NOMINAL DIAGNOSIS  
HEPs FROM TABLE 8.2 (OR TABLE 20-3 IN APPENDIX 5)**

<b>Item</b>	<b>General Rules</b>
(1)	Use upper bound if: <ul style="list-style-type: none"> <li>(a) the event is not covered in training, or</li> <li>(b) the event is covered but not practiced except in initial training of operators for becoming licensed, or</li> <li>(c) the talk-through and interviews show that not all the operators know the pattern of stimuli associated with the event.</li> </ul>
(2)	lower bound if: <ul style="list-style-type: none"> <li>(a) the event is a well recognised classic (e.g., TMI-2 incident) and the operators have practiced the event in the simulator requalification exercises, and</li> <li>(b) the talk-through and interviews indicate that all the operators have a good verbal recognition of the relevant stimulus patterns and know what to do or which written procedures to follow.</li> </ul>
(3)	Use nominal HEP if: <ul style="list-style-type: none"> <li>(a) the only practice of the event is in simulator requalification exercises and all operators have had this experience, or</li> <li>(b) none of the rules for use of upper or lower bound apply.</li> </ul>



**TABLE 8.5 of [26] : ASSESSMENT OF NOMINAL HEPs FOR POST-ACCIDENT  
POST-DIAGNOSIS ACTIONS (PAGE 1/2)**

<b>Item</b>	<b>HEP</b>	<b>EF</b>	<b>Action*</b>
(1)	1.0	–	Perform a critical skill-based or rule-based action correctly when no written procedures are available. (Details of skill-based actions are not required to be written, if they can be classified as ‘skill-of-the-craft’). This assessment is used even though it may be required for personnel to have memorised these actions. Instead they would likely refer to the written procedures at a later time during the usual checking to see that all immediate emergency actions had been performed correctly.
(2)	var.	–	If sufficient information can be obtained per a task analysis, as described in Chapter 4 of NUREG/CR-1278, use the data tables in Chapter 20 of NUREG/CR-1278 (reproduced in Appendix-5 of this report), adjusted for the effects of dependence, stress and other performance shaping factors (PSFs) and error recovery factors (RFs). If the level of information cannot be obtained because of scheduling or other restrictions, use the remainder of this table.
Items (3), (4) and (5) present HEPs for the original performer of the action, and must be adjusted for the effects of other operators and recovery factors [Items (6) to (9)]. These HEPs are for failure to perform a critical post-diagnosis procedural action as part of a ‘step-by-step task’ ** or a ‘dynamic task’ ** done under moderately high stress or extremely high stress. It is assumed that ‘novice personnel’ would be replaced by ‘skilled personnel’ for critical actions.			
(3)	0.02	5	Perform a critical action as part of a step-by-step task done under moderately high stress.
(4)	0.05	5	Perform a critical action as part of a dynamic task done under moderately high stress or a step-by-step task done under extremely high stress.
(5)	0.25	5	Perform a critical action as part of a dynamic task done under extremely high stress.

\* The HEPs are for independent actions or independent sets of actions in which the actions making up the set can be judged to be completely dependent. Other levels of dependence among actions can be assessed by the analyst, using one or more methods for assessing dependence, described in Chapter 10 of NUREG/CR-1278.

\*\* Step-by-Step Task - A routine procedurally guided set of steps one at a time without a requirement to divide one’s attention between the task in question and other tasks. May include both pre-accident and post-accident tasks. Dynamic Task - A task that requires a higher degree of interaction between the people and the equipment in a system than is required by routine procedurally guided tasks. Dynamic tasks include decision-making, keeping track of several functions, controlling several functions or combinations of these.

**TABLE 8.5 of [26] : ASSESSMENT OF NOMINAL HEPs FOR  
POST-ACCIDENT POST-DIAGNOSIS  
ACTIONS (PAGE 2/2)**

Item	HEP	EF	Action*
If recovery of above errors made by the original performer is still possible at the point of error action, use following HEPs (6), (7) or (8) and related task and stress categories for a second person who checks the performance of the original point of error action, use following HEPs (6), (7) or (8) and related task and stress categories for a second person who checks the performance of the original former.			
(6)	0.2	5	Verify the correctness of a critical action as part of a step-by-step task under moderately high stress.
(7)	0.5	5	Verify the correctness of a critical action as part of a dynamic task done under moderately high stress or a step-by-step task done under extremely high stress.
(8)	0.5	5	Verify the correctness of a critical action as part of a dynamic task done under extremely high stress**
(9)	var.	–	If there are error recovery factors (RFs) in addition to the use of human redundancy in (6), (7) and (8), the influence of these RFs must be assessed separately. For annunciator RFs, use the Annunciator Response Model (Table 20-23 in Appendix 5).
(10)	0.001	10	Perform a post-diagnosis immediate emergency action for the reactor vessel/containment critical parameters, when (a) it can be judged to have been committed to memory, (b) it can be classified as a skill-based action and (c) there is a backup written procedure. Assume no immediate RF from a second person for each such action.

\*\* Theoretically, if the HEP for Item (7) is assessed as 0.5, the HEP for Item (8) should be larger, say 0.75. However, as 0.5 is already so large, any increase in estimated HEP is judged to be unduly conservative.

Note on Time Stress: (Item 10-g in Table 8.1 Procedure for Nominal HRA of Post Accident Tasks, ASEP HRA Procedure, NUREG/CR-4772)

If time stress is present, the doubling rule is assessed, i.e. when an operator is required to take some corrective action in moderately high to extremely high stress conditions with limited time to take the corrective action, if the first action is ineffective, the HEP for each succeeding corrective action doubles (up to the limit of 1.0). The doubling rule applies to repeated attempts to perform the same task as well as to related tasks done by a second person.

HUMAN COGNITIVE RELIABILITY (HCR) CORRELATION

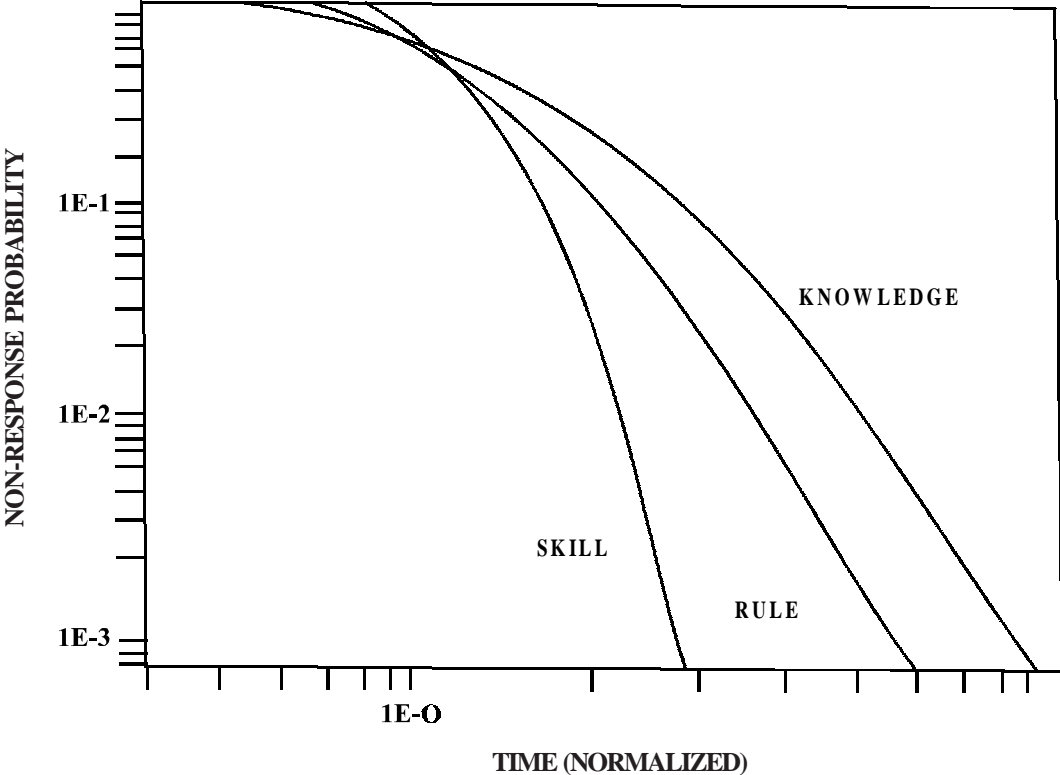
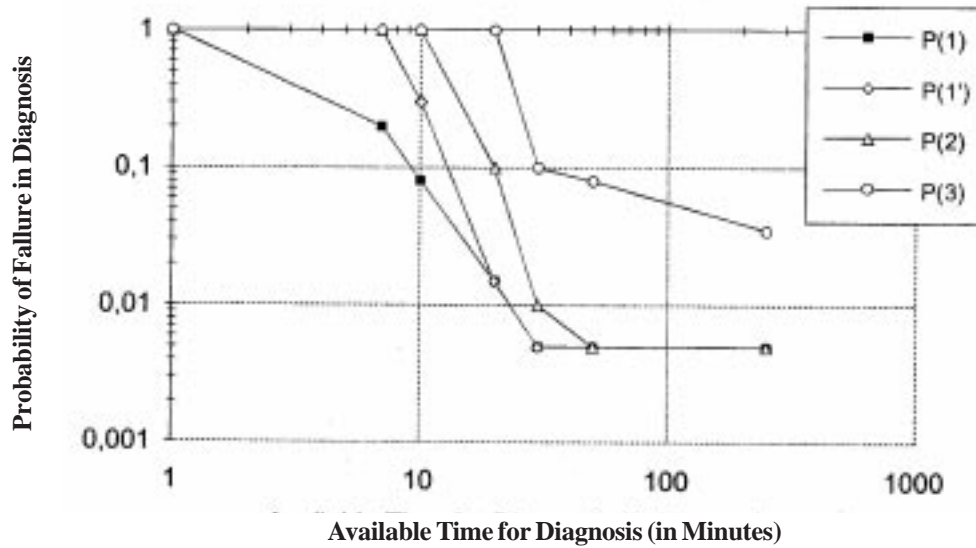


FIGURE AP6-3 : HCR CURVES FOR SKILL, RULE AND KNOWLEDGE BASED BEHAVIOURS

## ELECTRICITE DE FRANCE TRC



**FIGURE AP6-4 : TIME RELIABILITY CURVES FROM SIMULATOR EXPERIMENTS CONDUCTED BY ELECTRICITE DE FRANCE (EDF)**

**APPENDIX-7**

**TABLE OF COGNITIVE FAILURE PROBABILITIES - NOMINAL VALUES AND UNCERTAINTY BOUNDS FOR COGNITIVE FUNCTION FAILURES [8]**

<b>Cognitive Function</b>	<b>Generic Failure Type</b>	<b>Lower Bound (0.5)</b>	<b>Basic Value</b>	<b>Upper Bound (0.95)</b>
Observation	O1, Wrong object observed	3.0E-4	1.0E-3	3.0E-3
	O2, Wrong identification	2.0E-2	7.0E-2	1.7E-2
	O3, Observation not made	2.0E-2	7.0E-2	1.7E-2
Interpretation	I1, Faulty diagnosis	9.0E-2	2.0E-1	6.0E-1
	I2, Decision error	1.0E-3	1.0E-2	1.0E-1
	I3, Delayed interpretation	1.0E-3	1.0E-2	1.0E-1
Planning	P1, Priority error	1.0E-3	1.0E-2	1.0E-1
	P2, Inadequate plan	1.0E-3	1.0E-2	1.0E-1
Execution	E1, Inadequate action	1.0E-3	3.0E-3	9.0E-3
	E2, Action at wrong time	1.0E-3	3.0E-3	9.0E-3
	E3, Action on wrong object	5.0E-5	5.0E-4	5.0E-3
	E4, Action out of sequence	1.0E-3	3.0E-3	9.0E-3
	E5, Missed action	2.5E-2	3.0E-2	4.0E-2

## ANNEXURE-1

### NUCLEAR COMPUTERISED LIBRARY FOR ASSESSING REACTOR RELIABILITY (NUCLARR) - SAMPLE DATA TABLES

**TABLE AN 1-1 : SOME HEP DATA-COMPONENTS**  
(Data extracted from Table 5.2, Gertman and Blackman, 1994)

Component	Operator	Action	Mean HEP (EF)	UCB	LCB	Error Type
Circuit Breaker	AO	Opens/Closes	1.5E-2 (4)	3.8E-2	2.9E-3	O
Circuit Breaker	AO	Opens/Closes	6.0E-3 (7)	2.0E-2	4.5E-4	C
Control Rod Drive	CRO	Operates	2.7E-4 (10)	1.0E-3	1.0E-5	O
Electrical Equipment	CRO	Starts/Stops	1.8E-3 (5)	5.6E-3	2.2E-4	O
Electrical Equipment	MT	Calibrates	1.7E-1 (2)	3.1E-1	7.7E-2	O
AC Motor	CRO	Operates	8.7E-3 (2)	1.5E-2	4.3E-3	O
AC Motor	CRO	Operates	4.0E-3 (10)	1.5E-2	1.5E-4	C
Pressure Controller	MT	Calibrates	2.7E-4 (10)	1.0E-3	1.0E-5	O
Pump	CRO	Operates	2.6E-2 (5)	8.2E-2	3.2E-3	C
Valve	AO	Opens/Closes	1.3E-1 (3)	3.0E-1	3.3E-2	O
Tank	AO	Inspects	6.7E-5 (10)	2.5E-4	2.5E-6	C

Legend:

AO- Auxiliary operator, CRO-Control room operator, MT-Maintenance technician

O-Error of omission, C-Error of commission

UCB-Upper confidence bound, LCB-Lower confidence bound.

Data in Table AN1-1 are related to errors that may affect safety grade equipment. The mean HEPs are assumed to be log-normally distributed. Decision based errors are coded as errors of commission. Information on decision-based errors is contained in comment fields of individual HEP records.

To properly interpret data and to make subsequent decisions on the aggregation of these data, analysts need to go to the individual data records and determine the circumstances surrounding the failure (e.g. plant conditions, training, crew experience, interface, procedures, quality, type of task, dependency and degree of stress present at the time the error occurred).

The highest rate of error is for calibration of control rod drive mechanisms by maintenance technicians, which is equal to 1.7E-1.

**ANNEXURE-1 (CONTD.)**

**TABLE AN 1-2 : SOME HEP DATA-SYSTEMS  
(Data extracted from Table 5-3, Gertman and Blackman, 1994)**

<b>Component</b>	<b>Operator</b>	<b>Action</b>	<b>Mean HEP (EF)</b>	<b>UCB</b>	<b>LCB</b>	<b>Error Type</b>
Reactor Protection/GE	CRO	Operates	3.2E-4 (5)	1.0E-3	4.0E-5	O
Site Service Water/GE	CRO	Operates	2.0E-3(10)	7.5E-3	7.5E-5	O
Reactor Core Isolation Cooling/GE	CRO	Operates	1.6E-3 (5)	5.0E-3	2.0E-4	C
Electrical Distribution/	GEAO	Maintains	6.8E-2 (2)	1.3E-1	3.1E-2	O
High Pressure Safety Injection/B&W	CRO	Operates	1.4E-2 (2)	3.1E-2	5.3E-3	O
Decay Heat Removal/B&W	CRO	Operates	6.3E-3 (5)	2.0E-2	7.6E-4	O
DC Power/B&W	MT	Tests	3.7E-3 (2)	5.8E-3	2.0E-3	C
Emergency Core Cooling System/ B&W	AO	Maintains	2.7E-4 (10)	1.0E-3	1.0E-5	C

Legend:

GE - General Electric, W - Westinghouse, B&W-Babcock and Wilcox.

AO- Auxiliary Operator, CRO-Control Room Operator, MT-Maintenance Technician.

O-Error of Omission, C-Error of Commission

UCB-Upper Confidence Bound, LCB-Lower Confidence Bound.

HEP Source Data Calculations

In some instances, the HEP data point information considered for NUCLARR will consist of a report of the number of errors and number of opportunities for error. In these cases, confidence bounds are calculated by the NUCLARR system. In other instances, an estimate of the HEP and confidence bounds will be provided by the data source and the number of errors and opportunities for error that would give rise to these values must be computed. In addition, the NUCLARR system will calculate a mean HEP from a median HEP and confidence bounds if the mean HEP is not provided. The NUCLARR system will perform calculations of this type to provide data values missing from the original data source.

Observation of the Author of this Technical Document

In the data given in Table AN 1-1 and Table AN 1-2, the Error Factor (EF) given with the Mean HEP is seen to be calculated as equal (or very nearly equal) to the square root of the ratio UCB/LCB.

Example Calculations

- (i) In Table AN 1-1, for Circuit Breaker, Mean HEP (EF) = 1.5E-2 (4), UCB = 3.8E-2 and LCB = 2.9E-3. Here, the ratio UCB/LCB = 3.8E-2/0.29 E-2 = 13.10. Square Root of 13.10 = 3.61 ~ 4. Hence, EF = 4.
- (ii) In Table AN 1-2, for Reactor Protection, Mean HEP (EF) = 3.2E-4 (5), UCB = 1.0E-3, LCB = 4.0E-5. Here, the ratio UCB/LCB = 1.0E-3/0.04E-3 = 25. Square Root of 25 = 5. Hence, EF = 5.

## ANNEXURE-2

### TABLE OF DATA FOR PRELIMINARY QUANTIFICATION OF SIMPLE HUMAN INTERACTIONS IN PICKERING GENERATING STATION HRA [6]

Modified HEP = Unmodified HEP x Location PSF x MCR Detection (upto 2 multipliers) x Inspection Multiplier (1 only)

SI	Interaction Description	Unmodified HEP	Location PSF			MCR Detection (credit upto 2)		
			MCR	Field	Rad. Area	Ann. Wdw.	Other	None
			L=1	L=2	L=3	D=1	D=2	D=3
Ia	Component left in incorrect state after a maintenance task and not detected.	0.020	1	2	4	0.5	0.8	1
Ib	Component left in incorrect state after a test and not detected.	0.019	1	2	4	0.3	0.7	1
Ic	Component left in incorrect state after normal operation and not detected.	0.110	1	1	2	0.1	0.5	1
II	Component/system failure not detected from the available direct indications in MCR	1	1	-	-	0.05	0.5	1

Note: SI is Simple Interaction, Ia, Ib and Ic are Group I interactions and II are Group II interactions.

Inspection Factor (IF)	Means of Detection	Inspection Multiplier	For Group I, T is maintenance or test interval or interval between the normal operations, in days. For Group II, T is the average expected time in days, until discovery of the failure via an identifiable test or maintenance activity
IF = 1	MCR alarm summary at shift change (window or CRT alarms)	$0.044 + (0.24/T)$	
IF = 2	MCR indications at shift change (but no alarms)	$0.54 + (0.12/T)$	
IF = 3	Field walk around inspection	$0.13 + (1.7/T)$	
IF = 4	None	1	
IF = 5	MCR written panel check at shift change	$0.014 + (0.25/T)$	

The Inspection Multiplier is of the form  $p + (1 - p) \cdot N/T$  where p is the probability that the error or failure will not be detected by the means specified; and where the second term is necessary to account for the time delay involved in taking credit for detection at time of shift change or routine field inspection. The delay (N) is 'unavailable' time, and its effect must be included since the HEP estimate is normally used to provide an unavailability figure.



### ANNEXURE -3

#### MATRIX OF HEP DATA FOR PRELIMINARY POST-IE QUANTIFICATION IN CANDU HRA [6]

Time						
Quality of indication		T1	T2	T3	T4	Task Type 1 (straightforward and/or familiar)
	I1	0.003	0.003	0.006	1.0	
I2	0.027	0.027	0.054	1.0		
I3	0.15	0.15	0.30	1.0		
I4	1.0	1.0	1.0	1.0		
Quality of indication		T1	T2	T3	T4	Task Type 2 (average complexity and/or familiarity)
	I1	0.007	0.007	0.014	1.0	
I2	0.05	0.05	0.10	1.0		
I3				1.0		
I4	1.0	1.0	1.0	1.0		
Quality of indication		T1	T2	T3	T4	Task Type 3 (very complex or unfamiliar)
	I1	0.007	0.007	0.035	1.0	
I2	0.05	0.05	0.025	1.0		
I3				1.0		
I4	1.0	1.0	1.0	1.0		

Note: Cells that are blank are identically so in the reference from which the table is drawn

#### Legend

I1	Unambiguous indication	T1	Time available is unrestricted
I2	Interpretation required	T2	Time available is more than time required
I3	Unclear indication	T3	Time available is about equal to time required
I4	No indication	T4	Time available is less than time required

## REFERENCES

1. Bahr, N. J. (1997), *System Safety Engineering and Risk Assessment- A Practical Approach*, Taylor and Francis.
2. Chien, S.H. et al (1988), *Quantification of Human Error Rates Using a SLIM based Approach*, Proceedings of IEEE Fourth Conference on Human Factors and Power Plants, Monterey, CA, June 5-9, 1988, IEEE, N.Y.
3. Dougherty, E.M. (1990), "Human Reliability Analysis - Where Shouldst Thou Turn?" *Reliability Engineering and System Safety*, 29, pp 283-300.
4. Embrey, D.E. et al (1984), *An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement*, NUREG/CR - 3518, U.S.NRC.
5. Gertman, D.I. and Blackman (1994), H.S., *Human Reliability and Safety Analysis Data Handbook*, John Wiley and Sons.
6. Gordon, C.W. (1989), *A Course in System Reliability using the Fault Tree Method*, Bruce A Risk Analysis Fault Tree Guide, December, 1989.
7. Hannaman, G.W. and Spurgin, A.J. (1984), *Systematic Human Action Reliability Procedure (SHARP)*, EPRI-NP-3583, Electric Power Research Institute, Palo Alto, CA, U.S.A.
8. Hollnagel, E. (1998), *Cognitive Reliability and Error Analysis Method, CREAM*, Elsevier Science Ltd.
9. Hollnagel, E. (2005), *Human Reliability Assessment in Context*, *Nuclear Engineering and Technology*, Volume 37, No.2, April 2005.
10. IAEA (1991), *Case Study on the Use of PSA Methods: Human Reliability Analysis*, IAEA- TECDOC – 592.
11. IAEA (1995), *Human Reliability Analysis in PSA for Nuclear Power Plants*, Safety Series No: 50 - P- 10, IAEA, Vienna.
12. Kim, J. et al (1998), *IAEA CRP on Collection and Classification of Human Reliability Data for Use in PSA - Final Report*.
13. Kirwan, B. (1994), *A Guide to Practical Human Reliability Assessment*, Taylor and Francis.
14. Kirwan, B. (1996), *Human Reliability Assessment in the U.K. Nuclear Power and Reprocessing Industries, Human Factors in Nuclear Safety*, Taylor and Francis.
15. Kosmowski, K.T. et al (1994), *Development of Advanced Methods and Related Software for Human Reliability Evaluation within Probabilistic Safety Analysis*, Institut fur Sicherheitsforschung und Reaktor Technik, Julich, Jul - 2928, June 1994.
16. Le Bot, P. et al (1998), *MERMOS: An EDF project to update Human Reliability Assessment methodologies, Safety and Reliability*, Hansen and Sandtorv (eds), Balkema, Rotterdam.
17. Moore et al (1983), *CANDU HRA*, Page 574, IAEA - CN - 49/83.
18. Mosneron-Dupin, F et al (1991), *Probabilistic Human Reliability Analysis: The Lessons derived for Plant Operation at EDF*, IAEA-SM-321/57, PSA '91, Vienna, Austria, June 3-7, 1991.
19. Pyy, P. (2000), *Human Reliability Analysis Methods for Probabilistic Safety Assessment*, VTT Publications 422, VTT Technical Research Centre of Finland, Espoo, 2000.
20. Strater, O. (2000), *Evaluation of Human Reliability on the basis of Operational Experience*, GRS-170, GRS, August 2000.

21. Subramaniam, K. et al (1998), IAEA CRP on Collection and Classification of Human Reliability Data for Use in PSA - Final Report of a Coordinated Research Programme (1995-1998), IAEA - TECDOC - 1048, IAEA, October, 1998.
22. Subramaniam, K. et al (1999), Collection and Classification of Human Error and Human Reliability Data from Indian Nuclear Power Plants for Use in PSA, Report No. BARC/1999/E - 041, BARC.
23. Subramaniam, K. et al (2000), A Perspective on Human Reliability Analysis and Studies on the Application of HRA to Indian Pressurised Heavy Water Reactors, Report No. BARC/2000/E - 013, BARC.
24. Subramaniam, K. et al (2002), Human Reliability Analysis for Level - 1 PSA Study of Indian Nuclear Power Plants, First National Conference on Nuclear Reactor Technology, BARC, Mumbai - 400 085, November 25 - 27, 2002.
25. Swain, A.D. and Guttman, H.E. (1983), Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications: Final Report, NUREG/CR - 1278, U.S. NRC.
26. Swain, A.D. (1987), Accident Sequence Evaluation Programme HRA Procedure, NUREG/CR - 4772, U.S. NRC.
27. Taylor-Adams, S.E. (1995), An Overview of the Development of the Computerised Operator Reliability and Error Database (CORE-DATA), First Research Coordination Meeting of the IAEA CRP on Collection and Classification of Human Reliability Data for Use in PSA, April 3-7, 1995, Vienna, Austria.
28. U.S. NRC (1983), PRA Procedures Guide, NUREG/CR – 2300.
29. Wreathall, J. (1995), A Multidisciplinary Framework for Analysing Human Errors for PSA Applications, First Research Coordination Meeting of the IAEA CRP on Collection and Classification of Human Reliability Data for Use in PSA, April 3-7, 1995, Vienna, Austria.

## BIBLIOGRAPHY

1. AERB (2005), Probabilistic Safety Assessment for Nuclear Power Plants and Research Reactors, AERB/NF/SM/O-1.
2. Dougherty, Jr., E.M. and Fragola, J.R. (1998), Human Reliability Analysis: A Systems Engineering Approach with Nuclear Plant Applications, John Wiley and Sons.
3. Ericson, Jr., D.M. et al (1990), Analysis of Core Damage Frequency: Internal Events Methodology, NUREG/CR - 4550, U.S.NRC.
4. Frank, P. Lees (1996), Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control, Butterworth Heinemann.
5. Fullwood, R.R. (1999), Probabilistic Safety Assessment in Chemical and Nuclear Industries, Butterworth Heinemann.
6. IAEA (1989), Models and Data Requirements for Human Reliability Analysis, IAEA - TECDOC - 499.
7. KAPS (2000-2005), Significant Event Reports, 2000 - 2005.
8. Le Bot, P. (2004), Human reliability data, human error and accident models-illustration through the Three Mile Island accident analysis, Reliability Engineering and System Safety, 83.
9. Newton, S.L., Operating Experience Feedback - Lessons Learned Reducing Industry Events - Human Performance is the Key, INPO, U.S.A.
10. Stewart, M.G. and Melchers, R.E. (1997), Probabilistic Safety Assessment of Engineering Systems, Chapman and Hall.

## LIST OF PARTICIPANTS

### COMMITTEE ON PSA FOR NUCLEAR FACILITIES

Dates of Meetings	:	April 05, 2006
	:	April 28, 2006
	:	May 23, 2006
	:	June 14, 2006
	:	July 11, 2006
	:	May 04, 2007

#### Members and Invitees of the Committee

Shri P. Hajra	:	AERB (Former)
Dr. A.K. Ghosh	:	BARC
Shri R.K. Saraf	:	BARC (Former)
Dr. V. V. S. Sanyasi Rao	:	BARC
Dr. P.V. Varde	:	BARC
Smt. Rajee Guptan	:	NPCIL
Shri U.K. Paul	:	AERB
Shri R.B. Solanki	:	AERB
Shri Mahendra Prasad (Member-Secretary)	:	AERB
Shri K. Subramaniam*	:	BARC

\* Author of this Technical Document

**PROVISIONAL LIST OF AERB SAFETY CODES, GUIDES, MANUALS  
AND TECHNICAL DOCUMENTS ON OPERATION OF  
NUCLEAR POWER PLANTS**

Safety Series No.	Provisional Title
AERB/SC/O	Code of Practice on Safety In Nuclear Power Plant Operation.
AERB/SG/O-1	Staffing, Recruitment, Training, Qualification and Certification of Operating Personnel of Nuclear Power Plants.
AERB/SG/O-2	In-Service Inspection of Nuclear Power Plants.
AERB/SG/O-3	Operational Limits and Conditions for Nuclear Power Plants.
AERB/SG/O-4	Commissioning Procedures for Pressurised Heavy Water Reactor Based Nuclear Power Plants.
AERB/SG/O-5	Radiation Protection during Operation of Nuclear Power Plants.
AERB/SG/O-6	Preparedness of Operating Organisation for Handling Emergencies at Nuclear Power Plants.
AERB/SG/O-7	Maintenance of Nuclear Power Plants.
AERB/SG/O-8	Surveillance of Items Important to Safety in Nuclear Power Plants.
AERB/SG/O-9	Management of Nuclear Power Plants for Safe Operation.
AERB/SG/O-10A	Core Management and Fuel Handling in Operation of Pressurised Heavy Water Reactors.
AERB/SG/O-10B	Core Management and Fuel Handling in Operation of Boiling Water Reactors.
AERB/SG/O-11	Management of Radioactive Waste Arising from Operation of Pressurised Heavy Water Based Nuclear Power Plants.
AERB/SG/O-12	Renewal of Authorisation for Operation of Nuclear Power Plants.
AERB/NPP/SG/O-13	Operational Safety Experience Feedback on Nuclear Power Plants.
AERB/NPP/SG/O-14	Life Management of Nuclear Power Plants.
AERB/NPP/SG/O-15	Proof and Leakage Rate Testing of Reactor Containments.
AERB/NF/SM/O-1	Probabilistic Safety Assessment Guidelines.
AERB/NF/SM/O-2 (Rev. 4)	Radiation Protection for Nuclear Facilities
AERB/NPP/TD/O-1	Compendium of Standard Generic Reliability Database for Probabilistic Safety Assessment of Nuclear Power Plants.
AERB/NPP/TD/O-2	Human Reliability Analysis: A Compendium of Methods, Data and Event Studies for Nuclear Power Plant Applications.

**AERB TECHNICAL DOCUMENT NO. AERB/NPP/TD/O-2**

*Published by* : Atomic Energy Regulatory Board  
Niyamak Bhavan, Anushaktinagar  
Mumbai - 400 094  
INDIA.

BCS