BuMines OFR 195(2)-

PB84-126457

A mining research contract report
MAY 1983

EVALUATION OF SAFETY ASSESSMENT METHODS FOR THE MINING INDUSTRY.
Volume II.

USER'S MANUAL OF SAFETY ASSESSMENT METHODS FOR MINE SAFETY OFFICIALS

Contract J0225005
Battelle, Pacific Northwest Laboratories

Bureau of Mines Open File Report 195(2)-83

BUREAU OF MINES
UNITED STATES DEPARTMENT OF THE INTERIOR

REPRODUCED BY
NATIONAL TECHNICAL
INFORMATION SERVICE
U.S. DEPARTMENT OF COMMERCE
SPRINGFIELD, VA. 22161

LEGAL NOTICE

This report was prepared by Battelle as an account of sponsored research activities. Neither Sponsor nor Battelle nor any person acting on behalf of either:

MAKES ANY WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, process, or composition disclosed in this report may not infringe privately owned rights; or

Assumes any liabilities with respect to the use of, or for damages resulting from the use of, any information, apparatus, process, or composition disclosed in this report.

DISCLAIMER

The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies or recommendations of the Interior Department's Bureau of Mines or of the U.S. Government.

REPORT DOCUMENTATION PAGE	1. REPORT NO. BuMines OFR 195(2)-83	2.	3. Recipient's Accession No. PB84 126457
4. Title and Subtitle: Evaluation of Safety Assessment Methods for the Mining Industry. Volume II. User's Manual of Safety Assessment Methods for Mine Safety Officials			5. Report Date: May 1983 6.
7. Author(s): P. M. Daling and C. A. Geffen			8. Performing Organization Rept. No.
9. Performing Organization Name and Address: Battelle, Pacific Northwest Laboratories P.O. Box 999 Richland, WA 99352			10. Project/Task/Work Unit No. 11. Contract(C) or Grant(G) No. (C) J0225005 (G)
12. Sponsoring Organization Name and Address: Office of Assistant Director--Mining Research Bureau of Mines U.S. Department of the Interior Washington, DC 20241			13. Type of Report & Period Covered: Contract research; 8/24/82--5/24/83 14.

15. Supplementary Notes

Approved for release October 15, 1983.

16. Abstract (Limit: 200 words)

The objectives of this study were to examine a representative cross section of formal safety analysis techniques developed for the nuclear and aerospace industries, to recommend those methods that would be suitable for application to the mining industry, and to include those methods in a user's manual. Volume II of this report, the user's manual, describes several methods that were determined to be immediately transferrable to the mining industry. The handbook gives detailed instructions on appropriate application and utilization of the methods. Other techniques will require further development before they can be effectively transferred to the mining industry.

17. Document Analysis a. Descriptors

Mining research
Accident investigation
Safety analysis for mining applications
Preliminary hazards analysis
Failure modes and effects analysis
Human reliability
Computer application

b. Identifiers/Open-Ended Terms

c. COSATI Field/Group: 08I

18. Availability Statement: Release unlimited by NTIS.

19. Security Class (This Report): Unclassified

20. Security Class (This Page): Unclassified

(See ANSI-Z39.18) See Instructions on Reverse OPTIONAL FORM 272 (4-77) (Formerly NTIS-35) Department of Commerce

Preceding page blank

FOREWORD

This report was prepared by Battelle, Pacific Northwest Laboratories in Richland, Washington, under USBM contract number J0225005. The contract was initiated under the Minerals Health and Safety Technology Program. It was administered under the technical direction of the Spokane Research Center with Mr. John C. Kerkering acting as Technical Project Officer. Mr. R. J. Simonich was the contract administrator for the Bureau of Mines. This report, in two volumes, is a summary of the work recently completed as part of this contract during the period September 1982 to March 1983. This final report was submitted by the authors in May 1983.

TABLE OF CONTENTS

FOREWORD 4

INTRODUCTION 9

PRELIMINARY HAZARDS ANALYSIS 13

- Analysis Procedure 13
- Advantages and Disadvantages 18
- Example of Analysis Procedure 18
- Computer Adaptability 22
- Estimated Costs of Implementation 25

FAILURE MODES AND EFFECTS ANALYSIS 27

- Analysis Procedure 27
- Advantages and Disadvantages 31
- Example of Analysis Procedure 33
- Computer Adaptability 37
- Estimated Costs of Implementation 41

BINARY MATRICES 43

CONSEQUENCE ANALYSIS 46

MANAGEMENT OVERSIGHT AND RISK TREE (MORT) ANALYSIS 49

- Analysis Procedure 51
- Advantages and Disadvantages 61
- Example of Analysis Procedure 63
- Computer Adaptability 68
- Estimated Costs of Implementation 71

HUMAN-RELIABILITY ANALYSIS 73

- Analysis Procedure 73
  - STEP 1 - Describe the System Goals and Functions 74
  - STEP 2 - Describe the Situational Characteristics 76
  - STEP 3 - Describe the Characteristics of the Personnel . . 78
  - STEP 4 - Describe the Jobs and Tasks that the Personnel Perform 79
  - STEP 5 - Analyze the Jobs and Tasks to Identify Error-Likely Situations (ELSs) and Other Problems 81
  - STEP 6 - Suggest Changes to the System 82
- Advantages and Disadvantages 82
- Example of Analysis Procedure 84
- Computer Adaptability 91
- Estimated Costs of Implementation 94

REFERENCES 96

TABLES

1. Cross-reference of recommended safety analysis methods, their applications, and expected results 11

2. Preliminary hazards analysis format 14

3. Checklists of potential hazards 16

4. Categories for ranking the severity of hazards 17

5. Step-by-step procedure for performing a preliminary hazards analysis 18

6. Example page from a completed preliminary hazards analysis . . 21

7. Conceptual input format for a computerized, user-interactive PHA 23

8. Recommended format for guiding and recording a failure modes and effects analysis 28

9. Listing of potential component failure modes 29

10. Categories for ranking the severity or "criticality" of potential accidents 30

11. Step-by-step procedure for performing a failure modes and effects analysis 32

12. Example page from a completed failure modes and effects analysis 36

13. Example entries on the critical items list 38

14. Binary matrix for two linked flow systems with common power . . 45

15. Four-category qualitative classification scheme for consequence analysis 47

16. Expanded four-category qualitative classification scheme for consequence analysis 48

17. Listing of MORT analysis-related documents published by the System Safety Development Center (SSDC) 50

18. Energy forms present at typical mining sites 52

19. Examples of energy barriers at typical mining sites 53

20. Step-by-step procedure for performing a MORT analysis 62

21. MORT logic for muck bucket falls to bottom of shaft while hoisting personnel: example sheet 67

22. Checklist of factors that shape human performance 77

23. Recommended task analysis format for performing an HRA 80

24. A checklist for evaluating task error-likeliness 83

25. Examples of performance shaping factors that could cause a roof bolting machine operator to omit a methane check . . . 86

26. Example of a complete task analysis form 88

FIGURES

1. Mine hoisting system used in example problem 19
2. Conceptual flow chart for a computerized PHA 24
3. Block diagram of an example mine ventilation system 34
4. Conceptual flow chart for a computerized FMEA 39
5. Sample flow circuit with common power (IP) 44
6. Logic symbols used in constructing MORT-type analytical trees . 55
7. Event symbols and abbreviations used in constructing MORT-type analytical trees 57
8. Structure of the MORT-type analytical tree 59
9. General structure of the MORT diagram for the example problem . . 64
10. Example branch from the MORT diagram for the example problem . . 65
11. Conceptual flow chart for a computerized MORT analysis 69
12. Conceptual computer display for the MORT analysis procedure . . 70
13. Summary analysis procedure for the qualitative portion of a human reliability analysis 75
14. Link analysis flow diagram for the roof bolting operation . . . 85
15. Conceptual flow chart for a computerized HRA 93

INTRODUCTION

This user's manual was prepared as part of a study performed at Battelle Northwest Laboratory for the U.S. Bureau of Mines under contract No. J0225005. The overall objective of this study was to evaluate formal safety assesssment methods utilized in the nuclear and aerospace industries to determine the most useful and effective methods for technology transfer to the mining industry. Each method was evaluated relative to the safety interests, needs, and requirements of mine safety officials. This information was obtained through telephone and personal interviews with mine safety personnel and a tour of an operating underground mine. Results of the interviews were utilized to develop evaluation criteria in areas including the complexity of the methods, data and resources available at mines to perform the analyses, training and educational requirements for performing the analyses, responsiveness to mine operator safety needs, and cost-effectiveness. The evaluation criteria were used to examine and select formal system safety assessment methods that are most suitable for transfer to the mining industry at this time.

The objective of this user's manual is to present the safety techniques selected for direct application to the mining industry in a self-teaching workbook format for use by mine safety officials. The results of the interviews with mine safety officials and the evaluation of the various methods considered are contained in a separate report prepared for this project. This user's manual contains information relating to only those methods recommended for use at this time in the mining industry. Additional methods may be useful in the future as mine safety personnel gain more expertise and experience in implementing formal safety analysis technology. These methods are described in the project final report.

Sections in this manual are provided for each of the recommended safety analysis methods. Each section contains a general description of the method, a detailed discussion of the analysis procedure, advantages and disadvantages of the method, an example problem to illustrate the analysis procedure, and an estimate of the costs required to perform the analysis.

A further objective of this study was to evaluate the adaptability of the recommended methods to a user-interactive computer system. A computerized safety analysis program could benefit the mining industry by increasing the efficiency of mine safety officials, increasing the comprehensiveness of the analysis without large increases in costs, and reducing the amount of time required to perform and update the analysis. Conceptual computer flowcharts were developed for each recommended method and are described in each section.

The safety assessment methods described in this user's manual are applicable to many different mining situations and conditions. Each method contains features that make it more appropriate than others for analyzing certain situations. For example, one selected method is human reliability analysis (HRA). As its name implies, HRA is used primarily to examine the human element of a system to identify the potential causes of human performance errors. This analysis may focus on improving procedures or on a better design of the man-machine interface systems. A second selected technique is called

Management Oversight and Risk Tree (MORT) Analysis. MORT is a total safety program concept that focuses on programmatic control of industrial safety hazards. It is designed to evaluate the interactions of the complex management-worker-machine system to determine the causes of the contributing factors to potential accidents. Although MORT was originally designed as an accident investigation tool, it has also found wide application in the development and evaluation of system safety programs and procedures.

The selection of a particular safety assessment method should consider what kinds of mining situations are to be analyzed and what results are required from the analysis. Table 1 contains a listing of the recommended safety analysis methods in this user's manual, the applications each method is best designed to examine, and the expected results of the analysis methods. The reader is urged to consult this table for the purposes of choosing the most useful and appropriate system safety analysis method for specific applications.

It should be noted that the method descriptions provided in this user's manual are in some cases not sufficient for mine safety officials to perform the analyses without further information. MORT analysis and human reliability analysis techniques are complex and require significantly more information to perform them adequately than this document can provide. Therefore, the descriptions of these methods are limited to introductory-level tutorial-type information. The details of the techniques fill entire textbooks and cannot be repeated in full here. If the reader wishes further information regarding these methods, appropriate references to documents and short-courses are provided. These methods contain many subtle items and minute details that are described and discussed to a great extent in the reference documents and short-courses. A thorough understanding of these details is required to perform these methods effectively and adequately. The information presented in this user's manual for MORT and human reliability analysis is intended to summarize the most important aspects of the method and prompt the reader to obtain further information. The descriptions of preliminary hazards analysis, failure modes and effects analysis, binary matrices, and consequence analysis are sufficient for the analyst to use in performing the analyses.

One further point that should be emphasized before the methods are presented and discussed is that the methods are tools that help the analyst to organize a safety analysis. The tools are used to make a good safety official better by enhancing the completeness of the safety program and focusing further safety considerations on important areas. The safety program still requires a dedicated and knowledgeable analyst for it to be implemented successfully. Use of the methods will make the safety program more structured and thus, there will be less chance of omitting important safety concerns.

TABLE 1. - Cross-reference of recommended safety analysis methods, their applications and expected results

SAFETY ASSESSMENT METHOD	SUGGESTED APPLICATIONS	EXPECTED RESULTS
Preliminary Hazards Analysis	. Applicable to all types of mines and all mining situations. . Inexpensive but comprehensive analysis. . Identification of hazardous conditions, potential accidents and resulting effects on plant personnel and property. . Useful for identifying broad areas or functions requiring accident prevention or mitigation measures.	. Tabular compilation of hazards, potential accidents, effects, and existing and/or potential preventive or corrective measures. . Checklist or hazardous conditions. . Identification of ways to reduce occurrence of severe accidents with less emphasis on mitigation of minor accidents.
Failure Modes and Effects Analysis	. Applicable to all types of mines and all mining situations. . Hardware- and equipment-oriented approach. . Identifies effects of potential equipment malfunctions on the operation of the system and safety of personnel. . Useful for identifying detailed design areas requiring accident prevention or mitigation measures.	. Tabular compilation of the causes of equipment malfunctions and their resulting effects on the system . Checklist of critical items whose failure will produce hazardous conditions. . Identification of ways to reduce occurrence of accidents caused by equipment malfunctions.
Consequence Analysis	. Applicable to all types of mines and all mining situations. . Estimates severity of accidents . Requires other type of analysis to identify potential accident sequences.	. Estimated severity of potential accidents. . Could be qualitative or quantitative.

TABLE 1. - (continued)

Binary Matrices	• Applicable to all types of mines and all mining situations. • Identifies interactions between components or subsystems for system description purposes. • Usually applies to hardware - oriented situations but suitable for examining human interactions and task procedures. • Usually performed in conjunction with other safety analysis methods. • Useful for reviewing results from other analysis techniques to determine potential effects of accidents on other parts of a system.	• Two dimensional matrix indicating whether particular components interact with each other component in the system. • Can be used as a self-checking device to ensure that all potential interactions between components have been considered in other analysis techniques.
MORT Analysis	• Evaluation of management safety practices, specific accident control practices, task procedures, and human errors. Accident investigation technique Technique to enhance and improve safety training Helps to plan accident prevention programs	• Identification of management strengths and weaknesses in the safety area. • Identification of causes of specific accidents related to management practices, human errors, task procedure errors, and hardware failures. • Identification of potential system changes that can prevent or reduce the severity of accidents.
Human Reliability	• Applicable to mining situations where human error is a potential cause of accidents or can contribute to inadequate accident mitigation. • Applicable to all types of mines. • Identifies human and situational characteristics that can contribute to accident initiation or propagation. • Examines human performance shaping factors that can contribute to the occurrence of hazardous conditions and accidents.	• Compilation of tasks, steps in task, and performance shaping factors associated with each function in the system. • Listing of error-likely situations. • Identification of potential causes of human errors. • Identification of changes in procedures or the design of the work station (including equipment) that can reduce error-likely situations. • Identification of ways to reduce accidents involving human error, including many minor injuries and "material handling" accidents.

PRELIMINARY HAZARDS ANALYSIS

Preliminary hazards analysis (PHA) is a useful safety assessment method in which potential hazards inherent in a system and their effects are evaluated. PHA is a broad, all-encompassing study, usually performed early in the design stages of facilities to identify hazards before construction is started, thereby allowing changes for improved safety at relatively low cost before the system or component has been completed or installed. However, PHA can be performed at any time and is a particularly useful tool for identifying areas of concern for a safety program. A major goal of PHA in this application is to prevent accidents that have occurred in identical or similar systems.

The objectives of a PHA are to identify the potential hazardous conditions in a system and evaluate the significance of potential accidents. From the information developed during a PHA, design and procedural safety requirements can be established that will help prevent or control these hazardous conditions. Performance of a PHA on an operating mining system would help the mine safety officials to foresee hardware, procedural, and system interface problem areas. Results of a PHA can also help to identify areas that need further analysis and point out ways in which to mitigate hazardous conditions, thereby improving operations.

Analysis Procedure

The procedure for performing a preliminary hazards analysis is described in this section. The reader should recognize that the first step in performing a PHA, or any other safety technique, is to obtain a thorough working knowledge of the system under analysis. It is useful to break the system down into major subsystems or functions. Functional diagrams can be drawn that show the process flow of materials. For example, ore haulage at some mines consists of the following sequence of operations: (1) load ore into shuttle car, (2) move the shuttle car to dumping station, (3) dump ore into ore chute leading to hoisting bucket, (4) hoist bucket to surface, (5) dump ore into surface conveyor belt, and (6) move ore to mill or rail car loading station. Functional diagrams also show the interfaces between elements of a system. It is also useful to prepare narrative descriptions of the functions and operations of all subsystems and components. Interfaces with other subsystems and components should be clearly defined. Often, the process of going through these two system description exercises helps to identify potential safety problem areas.

The second step in the analysis procedure is to select the format for the analysis. A common format for a PHA is a columnar form with specific entries that reflect the information determined from each step of the analysis. This type of format is used because it allows a way to search and record specific information regarding the system and is also a checklist that guides and simplifies the analysis process. Information in a tabular format is easily retrievable once it has been recorded. This makes it simple to search for specific areas to record additional or updated information as it becomes available. Table 2 contains an example format for a PHA. Instructions given on Table 2 are intended to describe the information required in each column. There have been many PHA formats used in the past; some have as few as four

TABLE 2. - Preliminary hazards analysis format

COMPONENT	HAZARDOUS ELEMENT	EVENT CAUSING HAZARDOUS CONDITION	POTENTIAL HAZARDOUS CONDITION	EVENT CAUSING POTENTIAL ACCIDENT	POTENTIAL ACCIDENT	EFFECT	PREVENTIVE/CONTROL MEASURES
This column identifies the hardware or functional element being analyzed	This column identifies hazardous elements present in the hardware or function	This column identifies conditions, undesired events, or faults that could cause the hazardous element to be transformed into the identified hazardous condition	This column identifies hazardous conditions that could result from the interaction of the system and each hazardous element in the system	This column identifies undesired events or faults that could cause the hazardous condition to be transformed into the identified potential accident	This column identifies potential accidents that could result from the identified hazardous conditions	This column identifies the possible effects of the potential accident, should it occur	This column lists existing preventive or control measures that mitigate identified hazardous conditions and/or potential accidents. It may also be used for recommending measures for mitigation.
Breaking rock	Rock	Impact hammer fracturing rock	Flying rock fragments	Operator downhole	Operator hit by flying rock fragments	Injury; possible machine damage	Height of operator's cab, as well as shielding, should protect operators. Safety glasses should be worn. Machinery is designed to withstand impact from fragments.

columns and others have up to ten columns or more. It is believed that use of the 8-column format shown in Table 2 is a good trade-off between possibly oversimplifying the analysis (and therefore omitting some detail) and including such a great amount of detail that the results are difficult to locate.

Setting up the format for the analysis can be facilitated by breaking the overall system down into subsystems as was described previously. The analysis format can also follow this subdivision. In other words, the analyst breaks the mining system down into subsystems, such as ventilation, hoisting, ore haulage, railcar loading, etc., and examines each subsystem one at a time. It is useful to identify each component of each subsystem and address the hazardous conditions associated with them, no matter how unlikely or minor they appear. This is to ensure that the analyst thoroughly examines each situation and so is less likely to overlook some hidden interaction or hazard.

The next step is to begin analyzing the mining system one item at a time. The analyst begins by identifying potentially hazardous elements or components in the system. Hazardous elements are defined as any item or function which threatens something of value. The key idea is that something is at risk when the hazardous element is within the system. This something may be personnel, operating costs, property, production schedules, etc., although the method is usually used for determining the potential for injury to persons or damage to property. Hazardous elements are often categorized as either hazardous energy sources or hazardous processes and events, as shown in the checklist in Table 3 (Lambert 1975, Hammer 1972). Hazardous energy sources are hazardous by themselves when released in a system; i.e., the flow of energy from these sources causes personnel injury and property damage. Hazardous processes and events are either physical or chemical processes that produce hazardous conditions when they interact with the system. The checklists shown in Table 3 are useful tools for the identification of the basic hazards that may be associated with a mining system.

The next step in the PHA procedure is to identify events that could possibly transform the hazardous elements into potential accidents. These events are called "triggering events" or "causative factors" and can be conditions, undesired events, or faults within the system. For example, a spill of a flammable liquid such as diesel fuel oil does not cause a fire by itself. However, if an ignition source is present, such as a bare electrical wire, a spark can trigger the potential fire accident. Triggering events are important factors in a PHA. Experience in the aerospace and nuclear industries has shown that accidents often do not have a single random event as their cause, but are the result of a sequence of events which together generate the potential accident. This general principle also applies to accidents in the mining industry.

The framework for PHA often includes some evaluation of the importance of each hazard. This is commonly done by ranking hazards according to their effects. Hazards are categorized by some ranking scheme that considers the magnitude of the potential accidents. Many ranking schemes have been used in the past. Some were developed for a specific system and are not directly applicable to mining. One that is simple but still provides flexibility and is

TABLE 3. - Checklists of potential hazards

HAZARDOUS ENERGY SOURCES

1. Fuels
2. Explosive Charges
3. Charged electrical capacitors
4. Storage batteries
5. Pressure containers
6. Spring-loaded devices
7. Suspension systems
8. Mechanical equipment
9. Mine Gases
10. Electrical generators
11. Radioactive energy sources
12. Falling objects
13. Heating devices
14. Pumps, blowers, fans
15. Rotating machinery
16. Impacting machinery

HAZARDOUS PROCESSES AND EVENTS

1. Acceleration
2. Conveying
3. Corrosion
4. Electrical
   - shock
   - thermal
   - inadvertent activation
   - power source failure
   - electromagnetic radiation
5. Explosion
6. Fire
7. Heat and temperature
   - high temperature
   - low temperature
   - temperature variations
8. Drilling
9. Excavation
10. Moisture - high humidity
11. Vibration
12. Oxidation
13. Pressure
   - high pressure
   - low pressure
   - rapidly changing pressure
14. Radiation
   - thermal
   - electromagnetic
   - ionizing
   - ultraviolet
15. Mechanical shock
16. Chemical replacement, etc.
17. Hoisting (kinetic energy)
18. Climbing

useful for the mining industry is shown in Table 4. It is difficult to distinguish between some of the categories shown on this table. The boundaries between the categories are not well defined. Thus, which category a particular hazard is placed in depends upon the interpretation of the analyst. The hazard ranking is placed in the column labeled "effect."

The next step in the PHA is to determine what accident prevention measures are present, whether preventive measures should be taken, and what preventive measures could be or should be used. The ranking scheme described above shows which hazards and potential accidents should be receiving preventive or corrective action. If no preventive measures are provided for a Class III or Class IV hazard, the analyst must decide on the measures to be taken. Two courses of action are available (Lambert 1975): (1) corrective action, which

TABLE 4. - Categories for ranking the severity of hazards (James (ed) 1969)

HAZARD CATEGORY	EFFECT ON SYSTEM
Class I	Negligible - loss of function that has no effect on system
Class II	Marginal - degrades system to some extent but does not cause system to be unavailable
Class III	Critical - this hazard will completely degrade the system
Class IV	Catastrophic - this fault will produce severe consequences

can take the form of design changes, procedural changes, or changes in the mission goals (such as slowing a process down slightly to reduce traffic-related hazards), and (2) contingency action which can take the form of protective systems reacting to various accidents or training of personnel. Some examples of protective systems in the mining industry are methane detectors, oxygen detectors, fire detectors, and automatic sprinkler systems.

This essentially completes the procedure for performing a PHA. A summary of the steps involved in a PHA is shown in Table 5. It should be noted that a PHA is a dynamic, continuing process. The PHA should be updated, revised, and expanded throughout the life-cycle of the system being analyzed.

Advantages and Disadvantages

PHA has the advantage that it is a very simple safety assessment method that qualitatively considers all aspects of a system. Almost anyone with a detailed knowledge of the system being analyzed can perform a thorough, comprehensive PHA. The PHA technique is relatively cost-effective in that it is not a time-consuming approach. A further advantage is that PHA results in an easy-to-read, highly visible record of the analysis.

The greatest disadvantage of a PHA using a columnar format is that the analyst may fall into what is called a "form-filling mode." This is where the analyst is simply filling out a form. There are many subtle items and minute details that are important to the system operations that will be missed if the analyst is performing a PHA in this manner. The analyst is cautioned to thoroughly examine each entry on the PHA table in order to consider these details. A further disadvantage of PHA is that it is not quantitative. For example, the analyst will not be able to distinguish between accidents that cause one death or multiple deaths and frequent or infrequent accident occurrence rates from information on the PHA table.

TABLE 5. - Step-by-step procedure for performing a preliminary hazards analysis

Step 1:	Obtain an adequate working knowledge of the system.
Step 2:	Set up the PHA format: Dividing the large system into subsystems, such as the ventilation system, hoisting system, etc., is helpful. List the components and equipment in each subsystem.
Step 3:	Identify potentially hazardous elements or components in the system: The analyst will find that checklists are a useful tool.
Step 4:	Select a particular subsystem.
Step 5:	Identify triggering events or causative factors that could transform the hazardous elements into potential accidents. Begin with a particular component of the subsystem, analyze all hazardous elements associated with that component, and identify the triggering events. Record on PHA table.
Step 6:	Evaluate "criticality" of potential accident sequences identified in Step 5. In other words, rank the hazards into the categories shown in Table 4. Record rankings on PHA table under "effect".
Step 7:	Determine preventive or corrective measures that are present and further measures that could or should be taken. Record these measures on the PHA table.
Step 8:	Repeat steps 5, 6, and 7 for each component and hazardous element in the subsystem. The analyst should complete the examination of a particular component before continuing to the next.
Step 9:	Select a second subsystem and repeat the analysis procedure, Steps 5, 6, 7, 8.
Step 10:	Use the results to recommend design and procedural safety changes that can reduce accidents, injuries, and property damage.

Example of Analysis Procedure

Let us now consider an example to illustrate the procedure and results of a PHA. The example system used here is a mine hoisting system for haulage of men (see Figure 1). This example assumes that the hoisting system is being used during shaft sinking operations. The analyst first proceeds to list the subsystems and components that are required for the hoisting system to function. In this case, the component list includes such items as the bucket, wire rope, headframe, sheaves, hoist, shaft collar doors, and the control

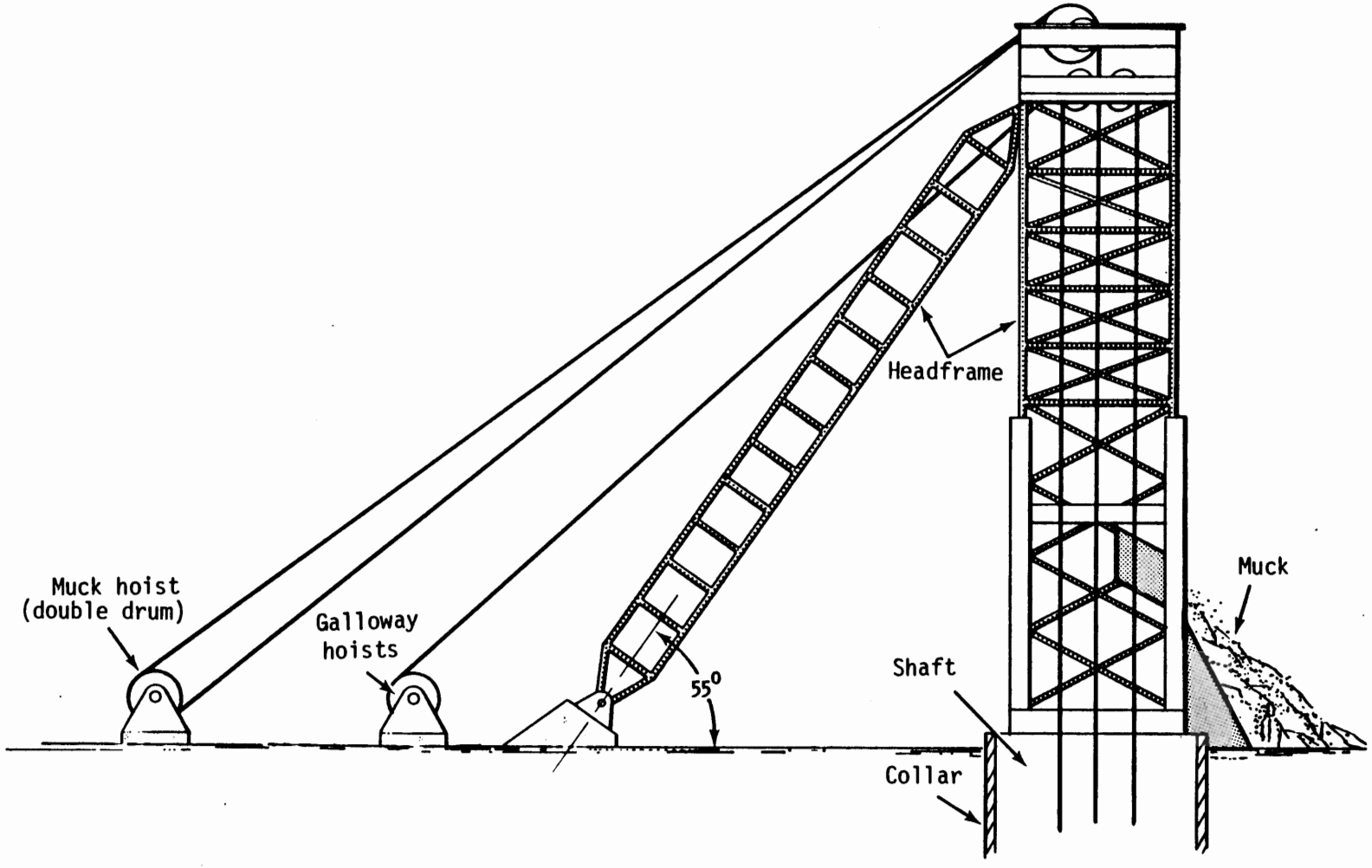


FIGURE 1. - Mine hoisting system used in example problem

subsystem. Once all of the components have been identified, the analyst consults the hazardous element checklist (see Table 3) to identify the hazardous elements associated with each component. For example, the bucket is a moving object; thus kinetic energy is one hazardous element. The bucket is also used to convey heavy objects that may fall out of the bucket. The hazardous element in this instance is potential energy. It is recommended that the analyst proceed to examine every column of the PHA one component at a time. In this manner, the analyst does not have to switch his/her thinking about a specific hazard to go on to the next component, thereby increasing the chances of omitting some details. In other words, the PHA form should be filled from left to right rather than from top to bottom.

The next step is to consider the hazardous condition and the events which could cause the hazardous condition. For the personnel bucket, lowering and raising the bucket is an event that could cause a hazardous condition only if personnel are waiting for the bucket (i.e., in the energy path). If property damage was of concern, items of interest in the path of the bucket could be a potentially hazardous condition but does not become one unless the bucket is moving. Continuing across the PHA table (see Table 2), the next two columns are for the potential accident and the event that could cause the potential accident. The event causing the potential accident is one which is required to transform the hazardous condition into an accident. For the above hazardous condition of people in the path of the bucket, and the bucket moving, the potential accident is one where the bucket strikes personnel, caused by personnel near the travel path of the bucket being unaware of an approaching bucket. This information is recorded in appropriate columns of the PHA table.

The analyst's next step is to examine the final two columns of the PHA table, effects and preventive/corrective measures of the same potential accident. Potential effects, in this case serious injury, are recorded in the former column. The latter column lists existing preventive or corrective measures that mitigate the potential hazardous conditions and/or potential accidents. In the example case, warning lights are provided that warn people of the approaching bucket. This column can also be used for recommending alternative or additional preventive/corrective measures.

The analyst continues systematically examining every hazardous element of every component under consideration. The result is a tabular listing of potential accidents and their effects, such as the example PHA shown in Table 6. The goal of this type of analysis is to identify the potential accidents which could cause serious personnel injury or death and with this information, eliminate or mitigate the hazard through training, safe operating procedures, safety equipment, design changes, or whatever means are practical. Mine safety officials, if they had the results of such an analysis, would be equipped with enough safety information and a general knowledge of the costs for improving safety in specific areas that they would be able to evaluate the costs and benefits of a particular safety feature. If the analyst wishes, cost information could be included in the column for corrective and preventive measures. One of the advantages of a PHA is that it does not involve complex mathematics or statistics and therefore can be performed adequately by the people who know the most about their specific mine, the safety officials,

TABLE 6. - Example page from a completed preliminary hazards analysis

COMPONENT	HAZARDOUS ELEMENT	EVENT CAUSING HAZARDOUS CONDITION	POTENTIAL HAZARDOUS CONDITION	EVENT CAUSING POTENTIAL ACCIDENT	POTENTIAL ACCIDENT	EFFECT	PREVENTIVE/CONTROL MEASURES
Bucket	Kinetic energy	Lowering or raising bucket	Personnel waiting for bucket	Personnel near travel path of bucket unaware of vehicle approach	Personnel struck by the bucket	Serious injury	Approach warning lights
	Potential energy	Normal bucket operation	Bucket loaded	a) Path of the bucket obstructed	Bucket tilts; men fall from bucket	Injury/death to personnel	Few perceived obstacles in pathway; bucket must tilt in excess of 60° to spill passengers.
				b) Bucket overloaded	Rope fails	Injury/death to personnel	Limited cargo space; rope safety factors.
Shaft collar doors	Electrical	Power source failure	Doors fail to open	a) Bucket (loaded) coming up	Collision of bucket with door/rope failure	Personnel injury/ death	---
				b) Bucket (loaded) going down	Collision of bucket with door	Bruises to personnel	Top lander is observing operation - can warn hoistman
Wire rope	Structural damage/ failure	1. Corrosion	Weakened rope	Loaded bucket	Rope fails; bucket and personnel fall	Injury/death to personnel; equipment damage	Daily inspection/ maintenance
		2. Overstressed	Weakened rope	Loaded bucket	Rope fails; bucket and personnel fall	Injury/death to personnel; equipment damage	Factors of safety/ load limit
Sheave	Corrosion	Moisture	Rough surface frays or pinches rope	Loaded bucket	Rope fails	Injury/death to personnel	Daily inspection/ maintenance. Test run at shift start

without a great deal of special training. Furthermore, PHA is a comprehensive analysis that can be applied to all parts of a mining system in regard to all kinds of hazardous conditions.

Computer Adaptability

It is believed that PHA is adaptable to a computer system. With today's relatively compact computer systems, a computerized PHA would, at the very least, increase the efficiency of the time safety officials spend at their desks. Moreover, with increased efficiency at their desks, the safety staff would be free to devote more time to correcting and preventing hazardous conditions at the mine. According to mine safety officials, computers are currently being used at mines for such purposes as long-term mine planning, maintenance planning, accounting, and warehousing. More extensive use of computers is being planned for the coming years. Therefore, enough computer operating and programming capability is in use at mines today to recommend that the computerized safety analysis be considered.

The authors were not able to identify any computer programs which have been written for PHA. A conceptual computer flowchart is described here for illustration purposes. More research is required for the development of this program.

As currently envisioned, the conceptual PHA computer program consists of two parts. The first part is the actual performance of a PHA on a computer and the second part is the use and updating of the results. The first part is a user-interactive scheme where the computer displays questions in their proper sequence corresponding to the labels of the columns of the PHA table. In addition to inputting the hazard information into the computer memory, the analyst is to index each component and some descriptive information (such as work environment, location, size, weight, etc.). The indexing scheme will be used in the second part of the PHA computer program.

Table 7 shows an example that illustrates how this process would work. The computer asks the analyst to input the name of the mine subsystem being analyzed (such as ventilation system, hoisting system, etc.), the component, component index number, and any important characteristics. Next, the computer asks the analyst to list the hazardous elements associated with the component being examined. The check list of hazardous elements (Table 3) could be displayed on the computer monitor to assist the analyst's selection. Then the computer asks the analyst to input the event causing the hazardous condition, the potential accident, and so on, until the analysis is complete. The result is a PHA that has been input to a computer memory and thus is available for key-word searches, updates, and modifications. A conceptual flow chart for the computerized PHA is shown in Figure 2.

The second part of the computerized PHA is the use and updating of the results. First, important results can be transferred to a special program module that selects and prints important components, characteristics, and

TABLE 7. - Conceptual input format for a computerized, user-interactive PHA

QUESTIONS ASKED BY COMPUTER	ANALYST'S RESPONSE
Subsystem name?	Example: Mine ventilation system
Component name?	Example: Ventilation fan
Component index number?	Analyst inputs a series of characters that identify the subsystem and component.
Important component characteristics?	Analyst inputs pertinent component information, including operating data and environment.
Regulations and policies regarding component?	Analyst inputs a cross-reference index of policies and regulations.
What are the hazardous elements associated with this component?	Analyst inputs hazardous elements. Computer can be programmed to display hazardous element checklist to aid the analyst.
What are the events that could cause the hazardous element to be transformed into a hazardous condition?	Analyst inputs a description of the triggering event.
(..., computer continues asking questions related to the columns of the PHA table shown in Table 4 and then returns to examine any other hazardous elements associated with this component. After completing the PHA of the first component, a second component may be examined, and a third, and so on.)	(..., analyst continues answering the questions asked by the computer.)

hazards so the analyst has a checklist that can be carried anywhere. Second, the information in the computer memory can be searched for key words and the component index number. Thus, the information is available for updates, revisions, and changes that can be input in a short period of time. Specific information regarding any component or potential hazard can be made available.

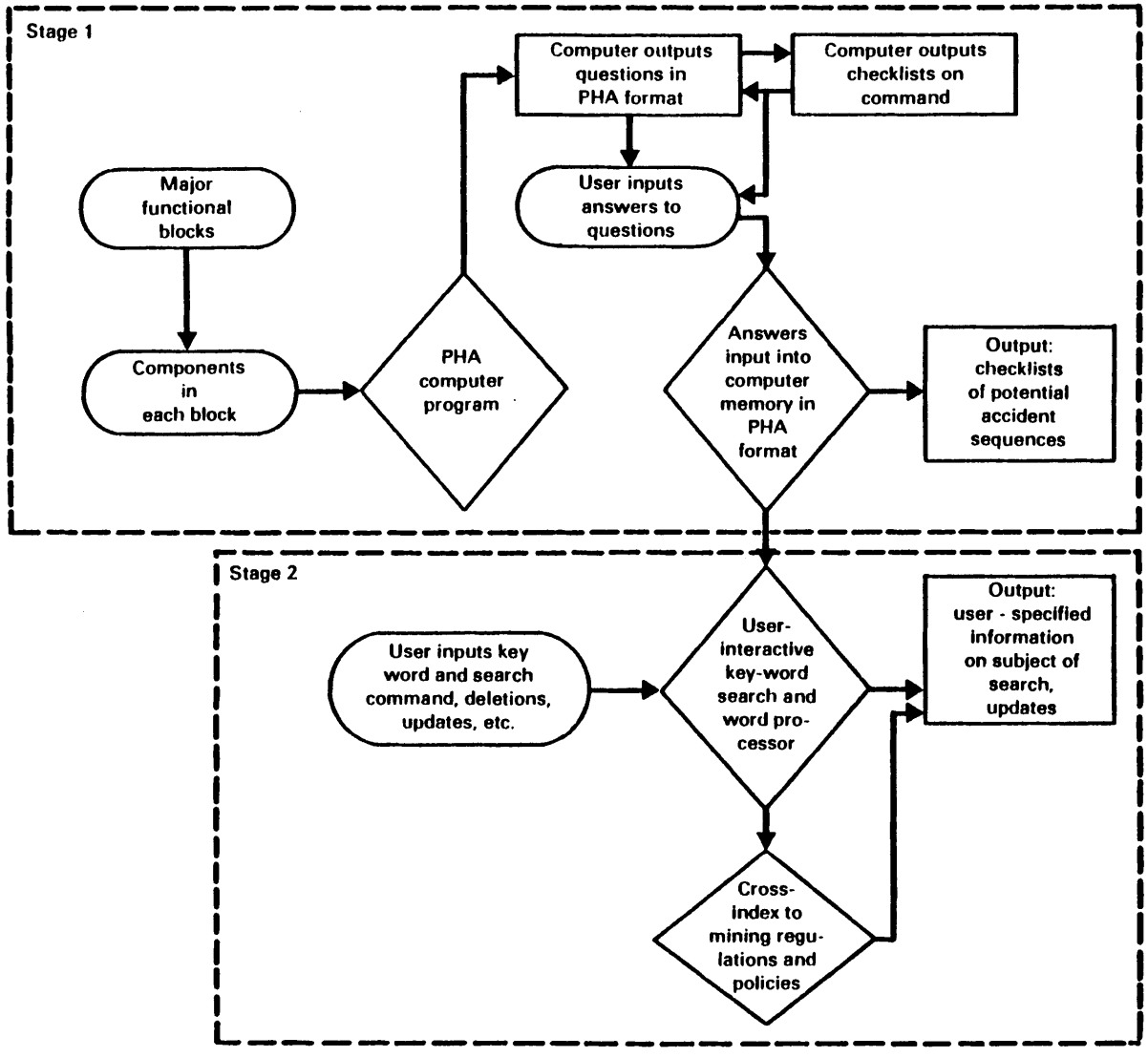


FIGURE 2. - Conceptual flow chart for a computerized PHA

A further item that mine safety officials have indicated would be useful to them is a cross-reference to mining regulations and mine policy statements. For instance, if the subject of some safety concern is fire extinguishers, the safety officials would like to be able to go to the computer and in a short time find out where to look for specific regulations and policies regarding fire extinguishers. This extra program module has been included in Table 7 and Figure 2.

Estimated Costs of Implementation

The costs for implementing a PHA safety program at a mine are estimated as follows. First, the costs for implementing a PHA-type program without computers is dominated by the costs of labor. It is estimated that a detailed PHA of a mining system would require about 0.5 man-years of safety staff labor. Assuming the unburdened safety staff labor rate is $15.00/hr and adding overhead expenses, taxes, benefits, and a large uncertainty, labor costs total $23,000 to $30,000 for performance of the PHA. Since PHA is a dynamic analysis that must be updated and revised periodically, it is estimated that 3 to 4 man-months/yr must be spent on this activity. Thus, total operating costs (including uncertainty) are estimated to be about $10,000/yr-$15,000/yr.

The estimated costs for implementing a computerized PHA includes the capital costs and installation of the computer system and software in addition to staff labor costs. Costs of computer systems were developed from a survey of available microcomputer systems and are conservatively estimated to be about $5,000, including delivery, installation and supplies. Annual supplies and maintenance costs are assumed to be 10% per year of the initial capital costs. Also included in the estimated costs for a computerized safety program are costs for the safety staff to attend short-courses on safety analysis training and computer training (including registration fees, travel, living expenses, and wages). These costs are developed in the final report of this study and the assumptions and bases will not be repeated here. The total fixed and operating costs are summarized below:

FIXED COSTS

Computer system purchase and installation	$ 5,000
Short course attendance and expenses	$ 9,000-12,000
Analyst's burdened labor costs	
Initiate Program	$10,000-15,000
Perform Analysis	$23,000-30,000
TOTAL	$47,000-62,000

ANNUAL OPERATING COSTS

Computer System Maintenance	$ 500/yr
Analyst's burdened labor costs	$10,000-15,000/yr
TOTAL	$10,500-15,500/yr

Note that these estimates do not contain the costs for developing the computer software. These costs are difficult to estimate and it is not known at this time whether they will be paid by the mining industry or by government. Therefore, software development costs will not be included in this analysis. The reader should recognize that software development costs are in addition to the estimated implementation costs presented above. It should also be noted that these costs include the wages of mine safety officials and are thus not an additional cost for mine operators. Generally, the time spent working on the safety assessment would replace the time safety officials currently spend at their desks.

FAILURE MODES AND EFFECTS ANALYSIS

Failure Modes and Effects Analysis (FMEA) is a safety assessment technique that was developed as a means of assuring that hardware and equipment are reliable (Jordan 1972). FMEA is a qualitative technique that is used to analyze the ways in which particular pieces of equipment can fail (failure modes) and the resulting effects on the system and personnel. This technique is often used to analyze a system design to enable the designer to locate and identify failure modes whose occurrence can cause loss of system function, personnel injury and death, or property damage. Once these "critical" failure modes have been identified, the designer is able to mitigate the safety problem through utilizing redundant components, providing alternate operating modes, personnel training or other available means. This technique is being used more and more extensively to evaluate existing and operating industrial processes and can be beneficial if applied to a mining system.

FMEA can be applied to all types of mines and to all mining situations. The techique is comprehensive and simple. It can be performed adequately with relatively little training. The technique requires a detailed knowledge of the system being analyzed, and thus is most suitable for the mine safety officials to perform. The technique is useful because it is a systematic method that identifies and evaluates the effects of hazardous conditions, which allows the mine safety people to plan for safety and remove or correct hazards as they are found. FMEA examines the failures of components of the mining system and evaluates the effects of failures on persons and objects at the mine. The results can be used as a checklist of hazards that the mine safety official can use to plan corrective and preventive measures that will eliminate or mitigate the hazards. For these reasons, FMEA was selected as a suitable safety analysis method for technology transfer to the mining industry.

Analysis Procedure

The purpose of this subsection is to describe the procedure for performing an FMEA. The first step in the performance of an FMEA is to obtain a thorough knowledge of the system. It is often useful in complex systems to break them down into major subsystems and components. Functional diagrams that identify the subsystems according to their purpose or function are a most useful way of defining the system under analysis. It is also extremely useful to prepare descriptions of the functions of all subsystems and components. Interfaces with other components and subsystems should also be clearly defined. The amount of detail required depends upon the uniqueness of the functions performed or the application of the particular item. An example of a functional statement is presented later in this section.

The next step is to establish the format that will be used in the analysis. The most commonly used format is a tabular format with labeled columns for specific entries. Many FMEA formats have been developed in the past and some are more useful than others. One format that is recommended for use in the mining industry is shown in Table 8. This format is relatively simple and contains the items of most interest to the mining industry. Also included on this table is a description of the information that should be

TABLE 8. - Recommended format for guiding and recording a failure modes and effects analysis

1. Item Identification	2. Function	3. Failure Mode	4. Failure Rate	5. Failure Effect	6. Criticality	7. Detection Method	8. Existing or Recommended Corrective Actions

1. Name of element or component under analysis. Can use symbols and abbreviations to identify components.
2. Concise statement of the function performed.
3. Description of the failure mode (see Table 9).
4. Estimate the failure occurrence rate. Usually this is a numerical value, although descriptive entries may be used such as frequent, infrequent, not expected to occur, etc.
5. A brief description of the effect of the failure on the system, subsystem, and plant personnel.
6. Statement of the criticality category (see Table 10).
7. A description of the methods by which occurrence of the failure mode is detected. If not readily detectable, indicate how testing or inspection could lead to detection.
8. A description of the existing or recommended corrective actions that can eliminate the failure mode or minimize its effect.

recorded in each column. This form is used as a checklist to guide the analysis and enables the analyst to systematically and thoroughly evaluate the plant or process under consideration.

The next step in the FMEA is the analysis of the failure modes and their effects. The analyst begins by selecting a specific subsystem and listing the components of the subsystem in the first column of the FMEA table. Next, the analyst picks a specific component and writes a clear, concise statement of the function the component performs in column 2. In column 3, the analyst records the specific failure modes regarding the component. This process can be aided by consulting the list of component failure modes shown in Table 9. Next, the analyst estimates the failure occurrence rate for the failure mode of the component under analysis. This can be done by referring to handbooks of failure rate data or by using a descriptive appraisal of the failure rate such as "frequent," "infrequent," "expected once per year," or "not expected to occur."

The analyst continues to column 5 of the FMEA table and records a description of the effect of the failure on the system, subsystem, and workers associated with the component. This column is particularly useful for identifying interactions and interfaces of the particular component with other aspects of the system under analysis. A detailed knowledge of the system is required for this step. It may be useful for the analyst to subdivide column 5 into three columns, one for system effects, one for subsystem effects, and one for human effects to further organize the thinking process. Next, the analyst evaluates the "criticality" or importance of the failure. This process is facilitated by the use of "criticality categories," which simply classify the severity of the effects of the failures. A hazard classification system

TABLE 9. - Listing of potential component failure modes (Garrick et al 1967)

1.	Failure to open
2.	Failure to close
3.	Failure to start
4.	Failure to continue operation
5.	Failure to stop
6.	Spurious failure, i.e., premature operation of a component when not called for
7.	Degradation
8.	Erratic operations
9.	Scheduled service
10.	Scheduled replacement

recommended for use by mine safety officials is shown in Table 10. See the section describing consequence analysis later in this manual for additional information. The analyst evaluates the failure effects and assigns each component failure to a criticality category. Then the analyst records the information in column 6 of the FMEA table. It should be noted that an FMEA does not normally consider "consequences" except in terms of system degradation. FMEA can do no more than specify the degree of system (or function) degradation. Thus, this column may be emitted to avoid confusing the analysis.

The analyst's next step is to identify and describe the methods used to detect the component failures. In some cases, the components are provided with sensors that alert operators of specific problems. In other cases, no sensing system is provided and failure is detected by inspection, testing and operator attention. In either case, the analyst should record this information in column 7. The final column of the suggested FMEA table is used to record descriptions of existing or recommended corrective actions that can eliminate the failure mode or minimize its effect. This information can be determined using the analyst's knowledge and experience, system designs, and corrective measures used in related systems. Vendor catalogs, trade shows, industry publications, such as those published by the American Institute of Mining Engineers (AIME), and engineering designs are particularly useful sources of potential preventive and corrective measures.

It is recommended that the analyst perform the FMEA steps in the following order. The table should be completed from left-to-right and not from top-to-bottom. In other words, the analyst should perform the evaluation and complete the FMEA table for one component before continuing to a second component. There are many subtle items and details that could be forgotten if the analyst switches from one component to another before completing the evaluation of the first. If a left-to-right approach is used, the analyst is

TABLE 10. - Categories for ranking the severity or "criticality" of potential accidents

HAZARD CATEGORY	EFFECT ON SYSTEM
Class I	Negligible - loss of function that has no effect on system
Class II	Marginal - degrades system to some extent but does not cause system to be unavailable
Class III	Critical - this hazard will completely degrade the system
Class IV	Catastrophic - this fault will produce severe consequences

less likely to omit subtle details, particularly the details of the component interfaces and interactions with other areas.

The next step in the performance of an FMEA is preparation of a "Critical Items List." This list facilitates communication of the significant results of the analysis to management. The Critical Items List is also useful for the safety officials to carry with them on periodic inspections of the mining system. The information placed on the list consists of components whose failure will produce hazardous conditions for the persons and property involved. This list is extremely useful for helping the mine safety official identify and correct hazardous conditions before they result in an accident, i.e., helps them to plan for safety. A typical Critical Items List contains the following information for each critical component failure:

- Item - Identify function/item by name
- Failure mode - Concise statement of failure mode(s) (see Table 8)
- Failure rate - List probability stated in FMEA, such as probable, possible, frequent, etc., or numeric failure rate data if desired. One could assign generic number ranges to these terms; e.g., probable = 0.1 to 1 occurrence per year, possible = 0.01 to 0.1 per year, etc.
- List page number of FMEA
- Criticality category - Enter the applicable criticality category stated in the FMEA
- Prevention/Correction - List existing or recommended means for eliminating the hazard or explain why the critical condition is not or cannot be eliminated or mitigated.

The preparation of the Critical Items List is the final step in performing an FMEA. The results are essentially documented as the analysis is performed. Final documentation of the FMEA process should include the detailed system description, including the functional descriptions and flow diagrams, the completed FMEA tables, and the Critical Items List. A summary of the FMEA analysis procedure is presented in Table 11. It should be noted that FMEA is a dynamic process that can and should accommodate updates and revisions to the system under analysis. Since a mining system is also constantly changing, the FMEA approach is particularly suitable for incorporating the modified information.

Advantages and Disadvantages

One of the primary advantages of the FMEA in regard to the mining industry is the simplicity of the analysis procedure. No complex mathematics or specialized training is required of the analyst. Thus, this method can be learned and performed effectively by mine safety officials in a short period of time. FMEA can be used in all types of mining systems and in reference to all kinds of safety problems. The FMEA format provides an orderly and structured

TABLE 11. - Step-by-step procedure for performing a failure modes and effects analysis

Step 1	Obtain adequate working knowledge of the system: Helpful to break system down into large blocks. Prepare functional flow diagrams and functional statements.
Step 2	Establish FMEA format: Recommended format shown in Table 1.
Step 3	Select first subsystem to be analyzed and list components of subsystem in column 1 of FMEA table.
Step 4	Select first component for analysis.
Step 5	Analyze failure modes of initial component and their effects: Complete analysis of the initial component by recording the information required in columns 2 through 8 of the FMEA table.
Step 6	Select and analyze the rest of the components of the first subsystem: Repeat step 5 for each component.
Step 7	Continue until all subsystems and components have been analyzed: Repeat steps 4, 5, and 6 for each subsystem.
Step 8	Prepare Critical Items List: For components whose failure produces detrimental effects on the subsystem function or personnel; contains information such as the critical component, failure mode, failure rate, page number where item is evaluated on the FMEA, criticality category, and preventive/corrective measures.

examination of the hazardous conditions inherent in an industrial process. The advantage here is that with the results of an FMEA, the mine safety officials may begin to plan for safety by preventing or correcting hazardous conditions before they cause accidents. FMEA results in a highly visible and orderly display of information that can accommodate updates and revisions to the system under analysis. A further advantage of FMEA is that the Critical Items List prepared from the results is a useful format for communicating hazard information to management and can also be used by mine safety officials as a checklist to assist in walk-through inspections of the mining system.

The main disadvantage of FMEA is that it considers only one failure at a time. Multiple and pre-existing failures are not normally considered. However, the analyst can enter dual component failures in column 1 of the FMEA table and proceed as with any other entry. There is no limitation on the number of components that can be considered simultaneously. The analyst is also cautioned to avoid the "form-filling mode" in which the analyst takes the attitude that he or she is simply filling out a form. Many details and subtle items are likely to be omitted if the analyst is performing the FMEA in this manner.

Example of Analysis Procedure

This section presents and discusses an example FMEA to illustrate the analysis procedure and results. The example presented is a partial analysis of an underground coal mining system. The complete FMEA cannot be shown due to its length; thus one page will be shown to illustrate the analysis of the mine ventilation system.

The first step in the analysis of the mine ventilation system is to describe the system under analysis. One useful method is to break the ventilation system down into major blocks. A block can be a large component (such as a ventilation fan including its associated connections), functional subsystem (an arrangement of components that performs a specific function; for example an electric substation or ventilation ductwork), location (such as a specific level or building of the mine), safety system, or other major part of the mine. A simplified example of a block diagram of the mine ventilation system is shown in Figure 3.

As can be seen on Figure 3, the example ventilation system operates using the exhaust principle where fresh air is drawn downward through the intake tunnel to the underground areas by the suction created by a large exhaust fan at the surface. There is one primary fan and an identical standby fan in case the primary fan fails. There is also a booster fan station at an underground level that reduces the load and power requirements of the larger primary fan The booster fan also provides chilled air via hard piping and collapsible tubing directly to the rock faces where coal is extracted. In a detailed analysis, the design of drifts and air flow separation techniques, such as regulators, overcasts, and stoppings, may be of interest. For the purposes of this illustration, the details of the underground airflow paths and the potential effects of fugitive air losses will not be examined.

It is also useful to prepare narrative descriptions of the functions of all subsystems and components. The functional statements should contain clear, concise descriptions of the operation of each item. Interfaces and interconnections with other components or subsystems are important items and should be clearly defined. An example of a functional statement is as follows:

Primary Ventilation Fan:

> Provides fresh air to miners while downhole. Also required for dilution of potentially harmful and explosive gases which are liberated by mining activities. Specifications: 240,000 cu.ft./min., 2000 hp, electric-driven, two-blade, propeller-type fan. Alarm at high motor temperature, low air flow, and electric power failure. Redundant standby fan provided. Interfaced with electric power supply (off-site and emergency standby on-site), ventilation exhaust shaft, and fan exhaust tunnel.

This information is particularly useful for evaluating the effects of component failures.

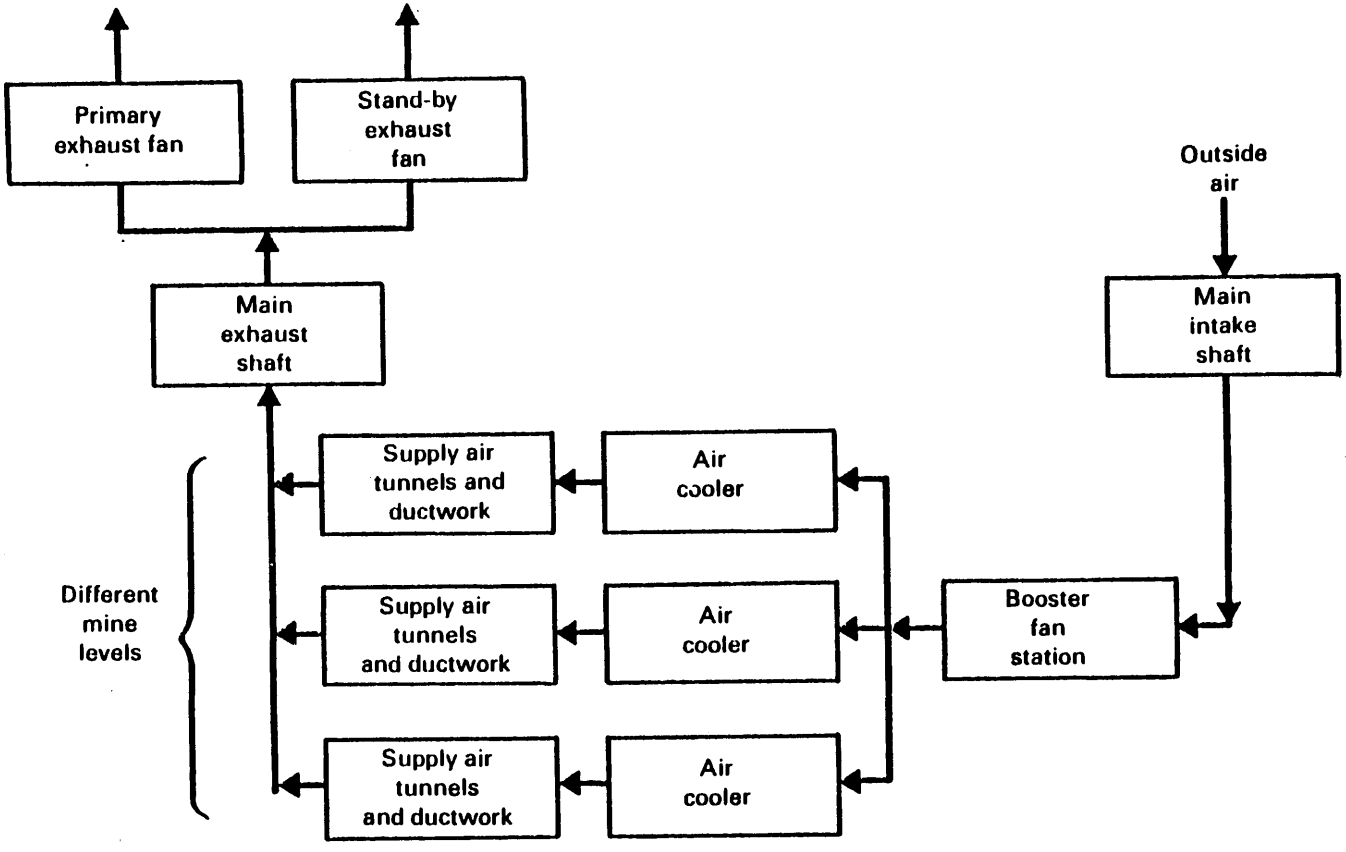


FIGURE 3. - Block diagram of an example mine ventilation system

The next step in the analysis is to establish the FMEA format to be used. The recommended format was shown in Table 8. The analyst is now ready to analyze the failure modes and their effects. The FMEA this example is based upon is shown in Table 12 for the reader to follow. The process the analyst should go through to evaluate the primary ventilation exhaust fan (first item shown on Table 12) is as follows. First, the component name is recorded in column 1. In column 2, the analyst records "Supply fresh air downhole" for the function of the fan. Next, the potential failure modes of the primary fan are identified using the checklist shown in Table 9. This fan can not be performing its intended function if it 1) does not continue to operate or 2) is down for service. These two failure modes are recorded in column 3. Next, the analyst evaluates the failure rate for the first failure mode of the fan. These particular fans are required to be well maintained and highly reliable so failure to continue operation is a relatively infrequent occurrence. The analyst may record "infrequent" in column 4 instead of recording actual numerical failure rates.

The analyst is now ready to examine the effects of the failure mode. In the example case, a brief period of time would elapse after the primary fan stopped operating before the standby fan is started. If this period of time is short, no adverse consequences are likely to occur. If the standby fan cannot be started for a relatively long period of time, the temperature and humidity downhole can build up to uncomfortable levels, oxygen may become depleted, and potentially harmful or explosive mine gases can reach dangerous concentrations. However, it is extremely unlikely that this failure would cause personnel injury or death because of the long time delay that can be used to evacuate the mine or repair the fans. This information is summarized and recorded in column 5 of the FMEA table. Based on the above discussion, this failure was placed in hazard category II because even though this fan is crucial to the mining operation, its failure does not directly cause injury or damage (see Table 9 for definitions of the hazard categories). The analyst must resist the temptation of considering fan failure in conjunction with the hoist failure (which would prevent evacuation of the mine). Only one failure at a time can readily be considered, using this technique. However, situations such as this should be noted by the analyst and examined more closely to determine if a single failure event could cause both systems to be inoperable simultaneously. This type of failure is called a common cause failure. Furthermore, if the analyst wishes, these combined failures could be entered as one time on the FMEA so that they could be considered.

The final two items on the FMEA table are for the method(s) of detecting fan failure and preventive/corrective meausures. Several methods are available that detect and warn operators of the fan failing to continue operating. Often fans are equipped with temperature sensors, air-flow indicators, and other sensing devices that are connected to an alarm or annunciator system. These fans are also large enough and create so much noise that their failure would be immediately noticed by operators. Detection methods are recorded in column 7. Column 8 is for the analyst to record existing measures which are employed to eliminate or mitigate the hazardous condition. The hazardous condition of a lack of fresh air downhole can be corrected by simply starting the standby fan. This hazardous condition is also prevented as much as practical by

TABLE 12. - Example page from a completed failure modes and effects analysis

Item 1.	Function 2.	Failure Mode 3.	Failure Rate 4.	Failure Effect 5.	Criticality 6.	Detection Method 7.	Prev/Corr Measures 8.
Ventilation System							
Primary Exhaust Fan	Supply fresh air downhole	Failure to continue operation	Infrequent	Loss of fresh air downhole, buildup of harmful/explosive mine gases (if both fans fail)	Class II if one fan fails, Class III if both fail	Alarm for fan failure, oxygen and combustible gas detectors downhole	Redundant fan system and emergency power supply
		Scheduled Service	Monthly	Loss of redundant fan, no effect if other fan operates	Class I	Alarm when backup fan stops	Periodic testing and maintenance of backup fan
Backup exhaust fan	Standby in case of failure of standby	Failure to Start	Infrequent	Loss of fresh air, build-up of mine gases	Class II or Class III	Alarm when fan stops, oxygen and combustible gas detectors	Redundant fan system, emergency power supply
		Scheduled Service	Monthly	Loss of redundant fan for duration of service, no effect if primary fan operates	Class II	Alarm when primary fan stops	Periodic testing and maintenance of primary fan
		Failure to stop	Infrequent	Pressure surge in ductwork may damage metal ducts and tear collapsible tubing	Class I	Air leak in duct is audible	Repair ductwork with tape
Underground booster fan	Boosts intake air flow, reduces load on primary	Failure to continue operation	Infrequent	Potential overheat and failure of primary fan	Class II	Alarm when booster fan stops, temperature sensor on primary fan motor	Long time period before booster failure causes overheat
Air intake tunnel	Fresh air pulled downhole through this tunnel	Plugged	Not expected to occur	Potential overheat of booster fan, loss of fresh air downhole, buildup of harmful/ explosive gases	Class II	Oxygen and combustible gas detectors, fan temperature sensor	Screened and grated opening
Downhole heat exchangers	Cools air downhole	Failure to continue operation	Probable	Temperature rise on mine levels, uncomfortable working conditions	Class I, if repaired in 24 hrs. Class II if repair is longer	Personnel attention	Reliable heat exchangers
		Scheduled service	Quarterly	Temperature rise downhole	Class I	Personnel attention	Service usually requires on a few hours

periodic testing and maintenance of both the primary and standby fans. In addition, in the event of loss of off-site electric power, these fans receive high priority for the electricity generated by the emergency diesel electric power supply system.

This completes the analysis of the failure of the primary fan to continue operation. The analyst continues examining the next failure mode of the ventilation fan, i.e., scheduled service. The process for completing the FMEA is repeated for this mode of fan failure. When all of the failure modes of the primary fan have been examined, the analyst continues to the next component, and so on, until all items associated with the underground ventilation system have been examined. Then the analyst can continue the analysis by examining other subsystems, one at a time, until the entire mine system has been analyzed.

This example has served to illustrate the procedure for performing an FMEA and recording the results. The next step is to develop a Critical Items List from the FMEA results. This list consists of components whose failure will produce hazardous conditions, or in other words, potentially dangerous situations for the persons or property involved. The format for displaying this information was shown previously and includes the item name, function, failure mode, failure rate, page number where found on the FMEA tables, criticality category, and preventive/corrective measures. The Critical Items List serves two purposes. First, it is a tool to be used for communicating significant results of the analysis to management. Second, it can be used as a checklist for mine safety officials to carry with them on inspections. Used in this manner, the checklist is a tool that helps mine safety officials and management to plan and execute a hazard prevention program. Some example entries on a Critical Items List are shown in Table 13. It is also beneficial to show if failures of additional items in conjunction with the critical item could potentially have severe consequences, such as failure of both the primary and standby fans in conjunction with failure of the hoisting system. Again, multiple failures can be handled directly as a single item in the FMEA.

Computer Adaptability

Results of the evaluation of the adaptability of FMEA to a user-interactive computer program indicate that it is possible and desirable to do so. No complex mathematics or logic is required to perform an FMEA so it is believed that it would be relatively simple to develop this computer program. Furthermore, it is believed that development of a user-interactive program as a guide to the performance of the FMEA would simplify the analysis procedure. There are no FMEA computer programs at this time to draw conclusions about their utility and effectiveness. However, it is believed that implementation of an FMEA computer program will increase the efficiency of the time safety officials spend at their desks, thus allowing more time to be spent preventing or correcting hazardous conditions at the mine. In addition, the FMEA and related Critical Items List provide new insights to the mine safety officials and management on the causes of potential accidents, and thus can lead to elimination or reductions of the accidents by eliminating their causes.

TABLE 13. - Example entries on the critical items list

Item/function:	Primary ventilation fan/provides fresh air to miners and dilution of mine gases
Failure Mode:	Failure to continue operation
Failure Rate:	Infrequent
FMEA Page No.:	A-1
Criticality Category:	Class II; potential contributor to catastrophic accident if evacuation of mine is hindered or not possible (not likely)
Prevention/ Correction:	Redundant standby fan, reliable and well maintained primary and standby fans, failure mode readily detected
Item/function:	Vent fan electrical connections/transmits off-site power to primary and standby fans
Failure Mode:	Failure to continue operation
Failure Rate:	Infrequent
FMEA Page No.:	A-2
Criticality Category:	Class II; potential contributor to catastrophic accident if hoisting system is unavailable, although this failure has minor effects in itself
Prevention/ Correction:	Reliable equipment and off-site power supply, standby diesel generator on-site, delay time before oxygen is depleted and gases reach dangerous concentrations.

A conceptual computer program utilizing the FMEA methodology was developed for this study. A relatively small computer system is required for this conceptual program. As currently envisioned, the conceptual FMEA program consists of three stages as shown in Figure 4. Stage 1 is a user-interactive scheme that guides the analysis procedure by asking appropriate questions for the analyst to respond to. The computer displays questions in the same sequence the analyst would ask himself if he were performing the analysis without the computer. In addition, the analyst will index the components and subsystems to aid Stages II and III of the program.

An example that illustrates how the Stage I analysis will work is the same as that previously shown for a computerized preliminary hazards analysis in Table 7. The computer displays a question asking the analyst to identify a

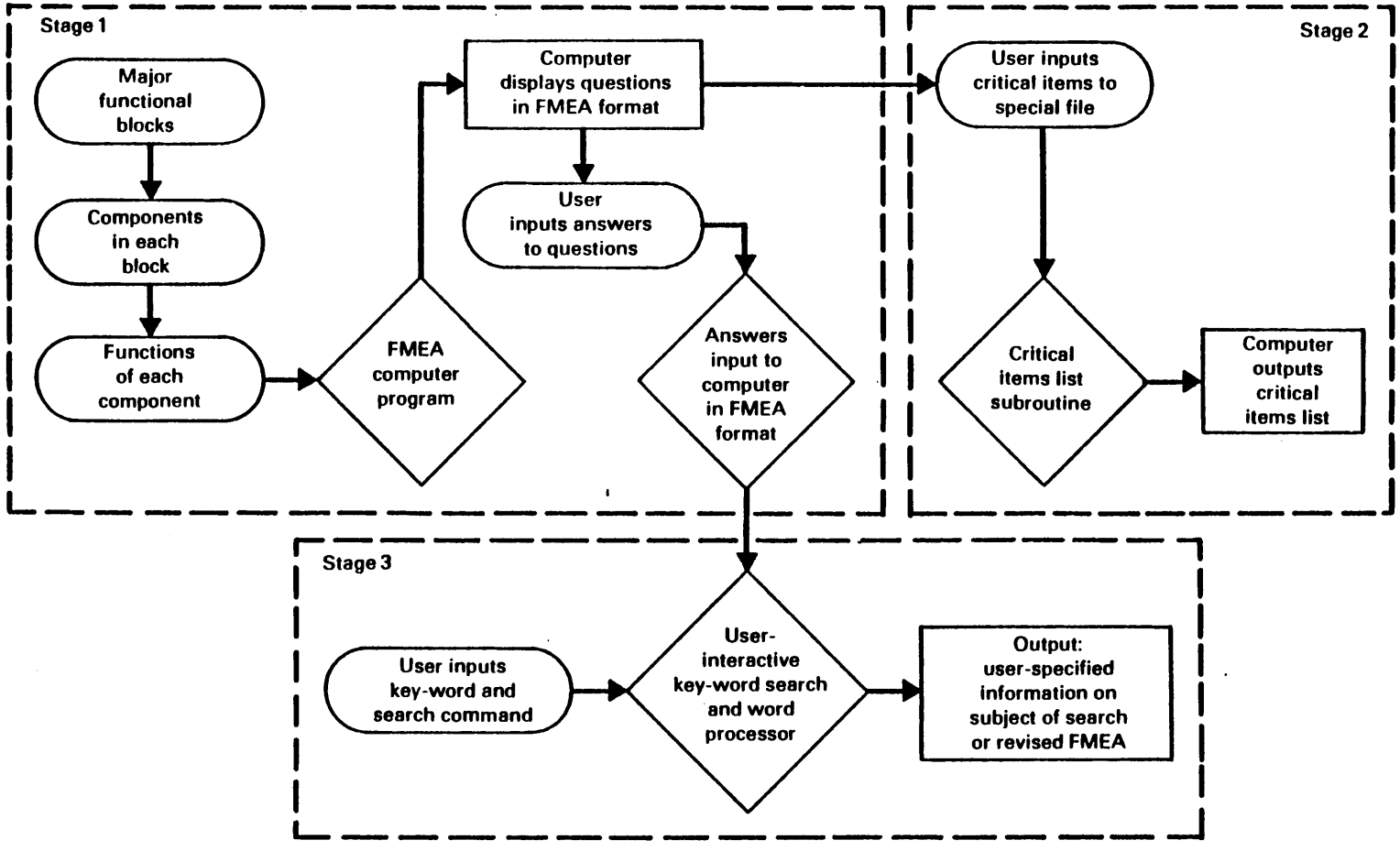


FIGURE 4. - Conceptual flow chart for a computerized FMEA

subsystem and assign an index number, such as "ventilation subsystem" and assign the letter "A" to represent this subsystem. Next, the computer will ask the analyst to identify a component of the subsystem and assign a second index to this component. For example, the analyst will input "Primary ventilation fan" and assign index A1a. The indices represent the subsystem and the component identification number, respectively. The small "a" in the index indicates there is more than one ventilation fan in the subsystem that is capable of performing the same function. If there are similar components that perform different functions, they would be assigned a separate numerical index. For example, the downhole booster fan in the example system is assigned the index number A2, rather than A1 c. The conceptual program is also capable of displaying parts of the FMEA table where the answers to the questions are being recorded. This feature enables the analyst to keep track of where his or her responses are being recorded and also to visualize the analysis as it progresses across the FMEA table.

The next questions in the conceptual FMEA computer program examine the component failure mode(s) and the failure effects. The computer will follow the analysis sequence from left-to-right on the FMEA table until an examination of a particular failure mode has been completed. Then the program returns and asks the same questions for the analyst to answer regarding the second, third, or additional failure modes. When a particular component and all of its failure modes and effects have been examined, the analyst selects a second component for analysis. This selection process can be aided by lists of components input to the computer memory before the analysis begins. The analyst would simply ask the computer to display the component list and then make a selection. A similar procedure may be used to assist in the selection of component failure modes and hazard categories (see Tables 9 and 10).

Stage II of the conceptual computer program is the use of the results. The computer can be used to search for critical items that, if they fail, can have adverse effects on personnel or property. This procedure is essentially the same as preparation of the Critical Items List. This can be done in two ways. First, the computer can perform a key word search of the criticality category and identify those items which are Class III or Class IV hazards. The analyst risks omitting some of the Class II items which are also critical items at the mine but do not have adverse consequences due to a requirement for one or more additional failures, delay time or some other mitigating condition. In the example presented, the primary ventilation exhaust fan would have been omitted because it's failure is a Class II item for the reason that there is a long delay time before failure of the fan produces personnel injury and property damage. However, the ventilation fans are critical to the mining process because without them, production must be interrupted until repair is effected. The second way to prepare the Critical Items List is for the analyst to indicate which items should be included on the list as the analysis progresses. In fact, the user-interactive computer program can be instructed to ask the analyst if a particular component is to be included on the list after each failure mode is evaluated. If the component and failure mode are judged to be critical, the computer automatically commits this to memory. Once the analysis has beem completed, the analyst would input a command to display

or print the Critical Items List and the computer would scan its memory and output this list. The computer can also be programmed to display or print all component details on the Critical Items List format, shown previously.

FMEA, like many safety analysis techniques, is a dynamic process. Therefore, the conceptual computer program should include a means to revise, update, and modify the FMEA of the mining system. Stage III of the conceptual computer program combines key-word search capabilities and deletion/correction capabilities of current micro-computer systems to accomplish this. The analyst will simply input a key-word or component identification number and input the "search" command. Then the computer will scan its memory for the appropriate combinations of letters and symbols and display exactly where they were found. Then the analyst can have these entries displayed on a monitor and using the deletion/correction capabilities of modern word processing software, make the revisions or modifications in appropriate locations.

Estimated Costs of Implementation

This section contains estimates of the costs for implementing an FMEA-type safety program at a typical mining system. Estimated costs were developed for two cases: 1) for an FMEA-type paper study and, 2) for a computerized FMEA program. The bases for these cost estimates are contained in the final report for this study and will not be repeated here.

The estimated costs for implementing a paper-study FMEA safety program are dominated by the costs of labor. It is estimated that approximately 1.0 man-year is required to perform a thorough FMEA of a mining system. Assuming the mine safety officials are paid about $15.00/hr, and adding a 50% burden for overheads, occasional overtime, and supplies, the estimated direct labor costs, including uncertainty, are between $45,000 and $65,000. It is estimated that 3 to 4 man-months/yr are required to periodically review, update, and revise the information on the FMEA tables. Thus, total operating costs are estimated to be about $10,000-$15,000/yr.

The estimated costs for implementing a computerized safety program based on the FMEA technique include the capital and installation costs of the computer system in addition to the staff labor costs. Costs of potential computer systems are estimated at $5,000, but this can most likely be reduced to about $3,000 due to the relatively small computer capabilities required for this type of analysis. The $5,000 estimated cost includes purchase of the complete computer system (including the processor, monitor, disk drive, keyboard, and printer), delivery, installation, and supplies. Annual maintenance costs are assumed to be 10% of the initial capital costs per year. Also included in the estimated costs for a computerized FMEA safety program are the costs for the safety staff to attend short-courses on computer training and safety analysis training (including registration fees, wages, living expenses, and travel costs). These costs are developed in the companion document to this user's manual and will not be repeated here. The estimated total fixed and operating costs are summarized below:

FIXED COSTS

Computer system purchase and installation	$ 5,000
Short course attendance and expenses	$ 9,000-12,000
Analyst's burdened labor charges	
Initiate program	$10,000-15,000
Perform analysis	$45,000-65,000
TOTAL	$69,000-78,000

OPERATING COSTS

Computer system maintenance	$ 500/yr
Analyst's burdened labor charges	$10,000-15,000/yr
TOTAL	$10,500-15,500/yr

Note that these estimates do not contain the costs for development of the computer program. These costs are difficult to estimate and it is not known whether the computer software will be developed by the government or the mining industry. Thus, the reader should be aware that software development costs are in addition to the estimated implementation costs presented above. Also, these costs do not represent the additional costs for implementing a formal safety program. Mine safety officials would be performing the safety assessment rather than their current duties in some instances and thus the actual additional costs that would be paid by mine operators are less than the costs presented here.

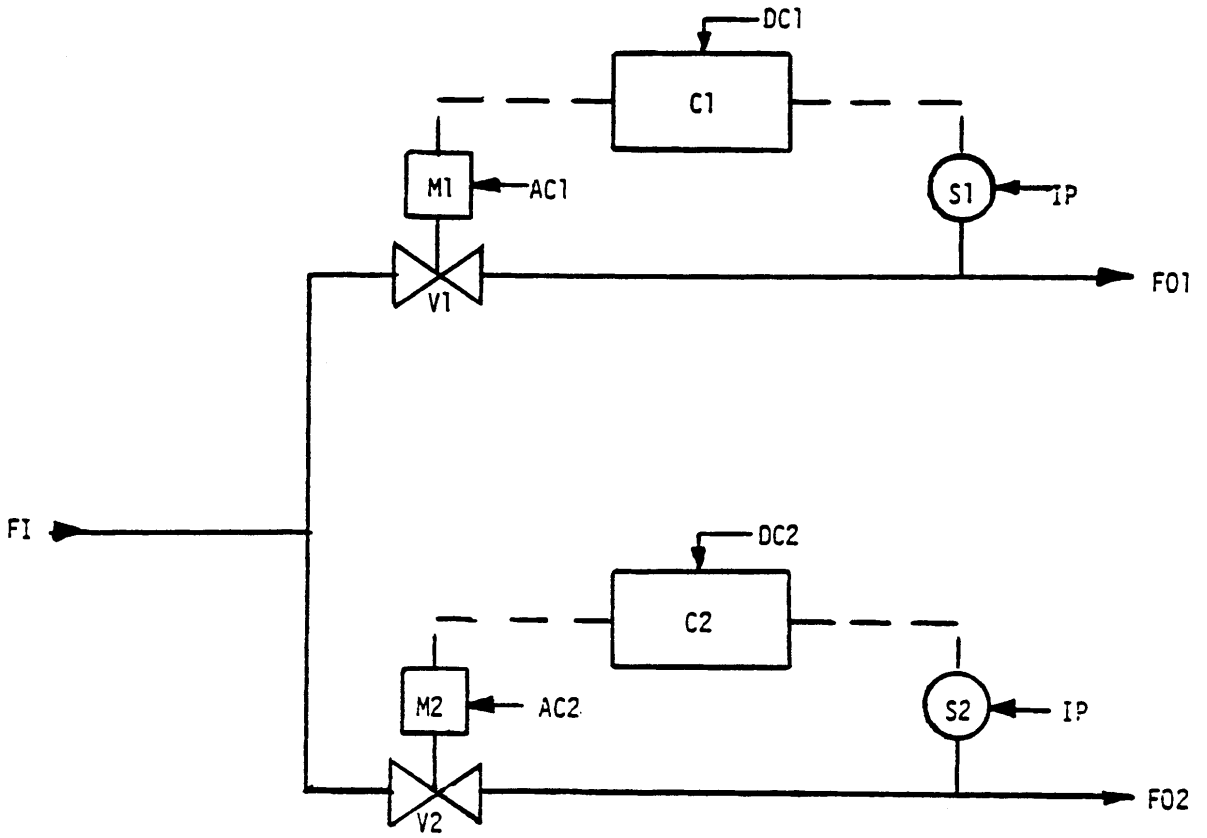
BINARY MATRICES

Many systems safety analysis techniques do not adequately address interactions among the components or subsystems of an overall system. A binary matrix (Cybulskis, et al 1981) represents a logical, qualitative approach to help identify systems interactions. This analysis tool can be applied during the system description stage of safety analysis or as a final checkpoint in an FMEA or PHA to ensure that all important systems dependencies have been addressed in the analysis.

The specific tool utilized in this technique is the binary matrix. The binary matrix contains information on the relationships between the elements of a system or systems. The purpose of the matrix is to identify the one-on-one dependencies that exist between these elements of a system. These elements can be any entities of interest to the analyst: entire systems, system functions, subsystems, components, physical locations, maintenance crews, electrical connections, etc. Elements of any level of detail can be intermixed. The important thing is to identify which elements affect others in some dependency relationship. Usually this is a "subordination" relationship where the analyst indicates the sequence of operations by identifying the events or operations that must occur prior to a specific event. This is usually done by placing a "1" in the binary matrix to indicate prior occurrence is required and a "0" to indicate there is no functional or operational relationship. Then, in performing the chosen safety analysis, when an accident sequence or failure mode has been identified for a particular system, the analyst can review the matrix to determine whether the failure under consideration can have repercussions in other parts of the overall system. In this sense, the matrix serves merely as a tool to "remind" the analyst that failures in one part of a system may affect the operation of other, seemingly unrelated, subsystems in another area.

An example of the application of the binary matrix to two simple, linked flow systems (shown in Figure 5) is presented below. In these flow systems, each flow line has a sensor (S1, S2) and a control valve (V1, V2) attached to it. The sensors rely on a common power source (IP). Attached to each valve is a motor (M1, M2), each of which has its own AC power (AC1, AC2). Each valve sensor system is controlled by a controller (C1, C2) which has its own DC power source DC1 and DC2.

Table 14 is a binary matrix that depicts the dependencies among the elements of the flow system. The relationship identified between components can be any area of interest. This dependency can be assigned by flow direction or by dependency on power sources, for example. The purpose of the matrix is to highlight for the analyst these kinds of interactions within an operating system. In this example, the analysis has been performed at the component level. Each separate component of the system is used to construct the format of the matrix. The matrix itself is filled in by placing a "1" in the matrix cell if a dependency exists between the elements and a "0" if no relationship seems to exist. In completing the matrix, one always works across the relevant rows, rather than down the vertical column. When complete, the matrix presents a useful tool in analyzing system interdependencies. For example, if one examines the row for F02 in Table 14, it becomes evident that this flow is



M1, M2	-	Motor 1, Motor 2
AC1, AC2	-	AC Power Source 1 and Source 2
C1, C2	-	Control 1 and Control 2
S1, S2	-	Sensor 1 and Sensor 2
V1, V2	-	Valve 1 and Valve 2
IP	-	Instrument Power
DC1, DC2	-	DC Power Source 1 and 2
FI	-	Flow In
FO1, FO2	-	Flow Out at 1 and at 2

FIGURE 5. - Sample flow circuit with common power (IP)

TABLE 14. - Binary matrix for two linked flow systems with common power

	FI	AC1	DC1	IP	AC2	CD2	V1	M1	C1	S1	V2	M2	C2	S2	FO1	FO2
FI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AC1	0	0	0	0	0	0.	0	0	0	0	0	0	0	0	0	0
DC1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
IP	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AC2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DC2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V1	0	1	1	1	0	0	0	1	1	1	0	0	0	0	0	0
M1	0	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0
C1	0	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0
S1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
V2	0	0	0	1	1	1	0	0	0	0	0	1	1	1	0	0
M2	0	0	0	1	1	1	0	0	0	0	0	0	1	1	0	0
C2	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0
S2	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
FO1	1	1	1	1	0	0	1	1	1	1	0	0	0	0	0	0
FO2	1	0	0	1	1	1	0	0	0	0	1	1	1	1	0	0

dependent on flow at FI (input flow occurring), power by IP, AC2 and DC2, the valve V2 operating properly, the motor M2 operating, and the control C2 and sensor S2 operating properly.

Although this example has concentrated on specific components within a particular subsystem, the analysis may also be performed at a broader level by examining functions within the system. For example, one can investigate the interactions among the different operations, locations, etc., within an overall mining system. The analysis would be performed in the same way as for the example presented above. Note that a good understanding of the system under consideration is necessary to successfully perform this analysis.

CONSEQUENCE ANALYSIS

Consequence analysis refers to the determination of a specific piece of information - the degree of severity of an accident. There is no generally applicable method for determining that information, since each specific accident may result in a different type of consequence, depending on the materials or operations involved. In addition, the analyst often specifically limits the scope of the safety analysis effort by deliberately analyzing in detail only those accident sequences that are believed to have a specific consequence of interest, e.g., injuries, fatalities, property damage in dollars, etc. Consequence analysis methods are then chosen or developed to determine the magnitude of consequence from a particular accident once the type of consequence has been decided.

Consequence analysis is one of the intermediate steps of a safety analysis. Accident sequences are usually determined initially using methods such as PHA or FMEA. Consequences are then examined for each accident, either within the scope of the originally used analysis technique or as a separate step. Finally, some measure of magnitude is assigned to the consequence and some measure of probability of occurrence to the accident sequence to prioritize system hazards and/or required mitigation measures in a meaningful way. Accident sequences with low levels of consequence may be ranked lower in overall hazards, allowing mine operators to concentrate their resources on mitigating hazards with larger potential consequence levels.

Because the methodology employed is so dependent on the type of accident sequences and consequences identified, there are no rigorous guidelines available for performing a consequence analysis. However, there are a few general approaches that may be useful in determining the potential magnitudes of identified consequences.

The primary consequences of concern in a mining system include injuries, fatalities, and losses due to property damage and operational downtime. These may be evaluated either qualitatively or in a quantitative manner. Qualitative measures can be very useful in generally determining which areas of the operation are most in need of safety improvements and for ranking of hazard types. In this method, consequences may be ranked simply as negligible, low, moderate and high, using a four-class system for all consequence types. An example of this classification scheme is shown in Table 15. Alternatively, the same method can be used with each type of consequence called out separately (see Table 16). When using this method, some quantitative or explanatory measure is necessary to properly differentiate among the four classification categories. Judgement of the analyst is then used to determine in which category each accident sequence falls. This method is useful in that it provides a ranking of hazards without requiring detailed numerical analysis of each accident sequence. For most purposes, such as identifying areas of safety improvement at a mine, this technique should prove adequate, providing meaningful results in a cost-effective manner. Often there are provisions made in preliminary hazards analysis and failure modes and effects for an evaluation of the consequences of potential hazards.

TABLE 15. - Four-category qualitative classification scheme for consequence analysis

Category of Consequence	Attributes of Category
Negligible	Minor equipment damage/downtime e.g., $100
Low	Moderate equipment damage/downtime e.g., $100-$3000; potential for minor injuries
Moderate	Moderate equipment damage/downtime; potential for major injuries/lost time
High	Major equipment damage; halt to system operation; potential for fatalities

Quantitative consequence analysis brings another level of detail to the safety assessment. This method basically assigns specific attributes of the consequence category directly to the accident sequence, rather than classifying that sequence with others in a group that all have generally the same range of attributes. This method is somewhat more complex, in that each accident sequence may have a different consequence magnitude (or even type). However, it also allows more detailed differentiation among accident sequences if this is required for the analyst's purposes. Historical accident data as catalogued at the mine or at the Mine Safety and Health Administration's Health and Safety Analysis Center in Denver, Colorado, may be used to help determine appropriate numbers for use as consequence magnitudes with specific accident sequences. Mathematical models may also be required to predict the consequences of a particular accident. These models can vary from dispersion analysis and inhalation models in the case of smoke inhalation and its effects underground to radiation dose modeling in predicting consequences of a failure in the ventilation system of a uranium mine.

The specific consequence analysis techniques chosen will be highly variable, dependent on the mine system being analyzed, the level of detail required in the analysis, and the specific accident scenarios under consideration. For most purposes, particularly when utilized in conjunction with a PHA or FMEA technique, qualitative consequence analysis should be sufficient. More detailed quantitative techniques are generally utilized in conjunction with a more detailed, quantitative safety analysis methodology, such as fault tree analysis. Education level and time requirements of consequence analysis are highly dependent on the specific requirements of the overall safety analysis task purpose, and will vary according to the complexity and degree of detail required for the analysis.

TABLE 16. - Expanded four-category qualitative classification scheme for consequence analysis

Consequence Type [a]	Consequence Categories [a]	Attributes of Category
		Average days lost [b]
PERSONNEL INJURY	Negligible (minor/or non-disabling injuries)	0-5
	Low (major injuries)	6-15
	Moderate (permanent disabilities)	16-6000
	High (fatalities)	6000 or more
		Dollars
PROPERTY DAMAGE	Negligible	100 or less
	Low	100-1000
	Moderate	1000-5000
	High	5000 or more

(a) Other consequence types and categories may be constructed as appropriate for the purposes of the analysis. Attributes of each category may be assigned based on importance for specific mining operations.

(b) This figure may be based on standard values utilized in Mine Safety and Health Administration reports.

MANAGEMENT OVERSIGHT AND RISK TREE (MORT) ANALYSIS

Management Oversight and Risk Tree (MORT) analysis is a comprehensive safety assessment method applicable to any mine safety program. MORT analysis is a very structured and formal safety technique that was designed originally as an accident investigation tool. MORT analysis has also been used as a safety program planning tool and as an aid in developing training programs. This technique was chosen for transfer to the mining industry because it requires little specialized training and could be learned and performed by mine safety officials in a relatively short period of time. MORT analysis appears to be readily adaptable to the computer, being especially valuable as a user-interactive aid to guide the analysis. For these reasons, MORT analysis is chosen for technology transfer to the mining industry.

MORT is a total safety program concept that focuses on administrative or programmatic control of hazardous conditions. This technique has been designed to identify, evaluate, and prevent safety-related oversights, errors, and omissions by management and workers that can cause accidents. MORT recognizes that in any industrial situation, there will be hazardous conditions that cannot be prevented or corrected due to economic or technological considerations. The MORT analysis technique is designed to identify this type of hazard and refer it to proper management levels. With the information obtained by MORT analysis, mine management will be able to allocate resources in a manner that will benefit the safety program the most, which is reducing injuries to the mining personnel and downtime due to equipment damage and accidents.

The MORT technique is the most optimum safety assessment method that is suitable for evaluating the three main factors that affect safety in an industrial situation; technological factors (such as the plant and hardware), human factors (such as personal abilities and training), and organizational factors (such as management controls and procedures). MORT analysis evaluates these factors both individually and as they interact together in a safety program. No other safety technique, by itself, has this capability.

The MORT technique is based primarily on a document written by W. R. Johnson (1973), hereinafter referred to as the "MORT text." The MORT text contains many safety system concepts and safety program elements which together produce the MORT safety program model. The MORT model is composed of safety concepts and elements such as human factors, hazard analysis, management systems, information systems, inspection and maintenance programs, and services. The details of these concepts fill a textbook and thus cannot be repeated here. MORT analysis cannot be performed adequately without the MORT text, so the mining industry, if they wish to perform this analysis themselves, will most likely have to obtain this document. It is available from National Technical Information Service in Springfield, Virginia. Supplementary MORT-related documents are listed in Table 17. These documents are extremely useful for helping to explain the analysis technique and specific safety program concepts. In addition to these documents, a one-week short-course on MORT analysis is taught under the sponsorship of the System Safety Development Center, operated for the Department of Energy by E.G. and G. Idaho, Inc. It is recommended that the mine safety officials who may be performing this

TABLE 17. - Listing of MORT analysis-related documents published by the system safety development center (SSDC)[a]

DOCUMENT NUMBER		TITLE
ERDA-76-45-1	SSDC-1	Occupancy-Use Readiness Manual
ERDA-76-45-2	SSDC-2	Human Factors in Design
ERDA-76-45-3	SSDC-3	A Contractor Guide to Advance Preparation for Accident Investigation
ERDA-76-45-4	SSDC-4	MORT User's Manual
ERDA-76-45-5	SSDC-5	Reported Significant Observation (RSO) Studies
ERDA-76-45-6	SSDC-6	Training as Related to Behavioral Change
ERDA-76-45-7	SSDC-7	ERDA Guide to the Classification of Occupational Injuries & Illnesses
ERDA-76-45-8	SSDC-8	Standardization Guide for Construction & Use of MORT-Type Analytic Trees
ERDA-76-45-9	SSDC-9	Safety Information System Guide
ERDA-76-45-10	SSDC-10	Safety Information System Cataloging
ERDA-76-45-11	SSDC-11	Risk Management Guide
DOE-76-45-12	SSDC-12	Safety Considerations in Evaluation of Maintenance Programs
DOE-76-45-13	SSDC-13	Management Factors in Accident/Incidents (Including Management Self-Evaluation Checksheets)
DOE-76-45-14	SSDC-14	Events & Causal Factors Charting
DOE-76-45-15	SSDC-15	Work Process Control Guide
DOE-76-45-16	SSDC-16	SPRO Drilling & Completion Operations
DOE-76-45-17	SSDC-17	Applications of MORT to Review of Safety Analyses
DOE-76-45-18	SSDC-18	Safety Performance Measurement System
DOE-76-45-18	SSDC-19	Job Safety Analysis
DOE-76-45-20	SSDC-20	Management Evaluation & Control of Release of Hazardous Materials
DOE-76-45-21	SSDC-21	Change Control and Analysis
DOE-76-45-22	SSDC-22	Reliability & Fault Tree Analysis

(a) SSDC is currently operated for the U.S. Department of Energy by E.G. and G. Idaho, Inc., Idaho Falls, Idaho.

analysis on their mines have copies of these documents and attend the short course. Valuable insights on the procedure and on the total safety program concept are revealed in these sources that cannot be presented in this document due to the length of the discussion.

The MORT analysis technique was originally developed as an accident investigation tool. It could be used successfully in the mining industry for this application. MORT is designed to determine the basic events associated with an accident and thus, if used in this manner, could prevent the recurrence of many mining accidents. However, MORT analysis has been increasingly utilized as a planning tool for developing safety and training programs. The MORT methodology is an integration of hundreds of safety program elements and can be used as a checklist for ensuring that as many safety concepts as possible are considered. Used in this manner, implementaton of MORT analysis techniques would benefit the mining industry by structuring the planning of an accident prevention program into a logical format. It is believed that this could reduce the numbers of both serious and minor accidents at mines which not only improves safety but also reduces the medical and lost work-time expenses paid by mine operators and increases productivity.

Analysis Procedure

The acronym MORT is the name given to the logic diagram that displays the elements and concepts of the MORT safety program. A universal logic diagram is used in MORT analysis as a master "work sheet" to examine a specific accident or to evaluate existing or developing safety programs. The MORT diagram is very large and displays over 1500 safety program elements or "basic events" in an orderly and structured manner. It identifies the details and relationships that must be considered to identify potential hazards and prevent oversights and omissions that could lead to accidents. The MORT diagram and analysis technique can be applied in some form to all types of safety concerns in all areas of the mining industry. In addition to identifying and evaluating potential safety problems, MORT analysis identifies the management system's weaknesses and strengths in regard to the safety program and provides a basis for management to make rational and informed decisions concerning accident prevention.

MORT analysis uses the concept of unwanted energy flows and barriers to the energy flows to identify the many factors contributing to a potential accident. Energy flows are normally classified into categories of energy forms, such as thermal, electrical, or kinetic. For example, if the potential accident under consideration is a person being struck by a moving front-end loader, the unwanted energy flow is a flow of kinetic energy, or the energy of moving objects. Examples of energy forms present at a mining site are shown in Table 18. Accidents are caused by some interaction of these energy flows with persons and objects. Accidents usually occur because of a lack of adequate barriers and/or controls associated with the unwanted energy flow.

This brings up the concept of barriers. Barriers are provided to prevent the transfer of unwanted energy from its source to a target (persons or objects). Some examples of energy barriers at typical mining sites are shown

TABLE 18. - Energy forms present at typical mining sites

ELECTRICAL	CORROSIVE
Transformers	Acids
Wiring	Caustics
Power tools	Natural chemicals (air, water, soil)
Pumps	Excavated material (leaching)
KINETIC/LINEAR	**POTENTIAL (Falls and Drops)**
Hoisting equipment	Human effort
Crane loads in motion	Stairs, ladders, scaffolds
Moving vehicles	Excavation
High pressure air lines	
High pressure oil lines	
KINETIC/ROTATIONAL	**POTENTIAL (Cranes and Lifts)**
Pumps	Cranes
Fans	Slings
Motors	Hoists
Rotating components	Elevators
Hoisting Equipment	
FLAMMABLE MATERIALS	**TOXIC/PATHOGENIC**
Diesel fuel (emergency generators and storage)	Carbon monoxide
	Dust and particulates
Gasoline (vehicles and storage)	Oxygen deficiency
	Radioactive particulates
Lubrication oil	Mine gases
Grease	
Rags and waste	
THERMAL	**EXPLOSIVE/PYROPHORIC**
Convection	Dynamite
Conduction	Caps
Fire	Primer Cord
	Dust
	Fuel oil and gasoline trucks
	Mine gases

in Table 19. Barriers may be physical design features, protective equipment, safety devices, warnings of hazardous conditions, safe operating procedures, and personnel experience. The MORT technique allows the analyst to evaluate the adequacy of barriers to each potential accident sequence to determine if there are failed barriers, barriers which are not provided, available barriers which were not used, or no barriers possible.

TABLE 19. - Examples of energy barriers for typical mining sites

Type	Example Barriers
Limit energy source	Motor speed controllers
Prevent build-up of energy form	Pressure relief valve, burst disc
Prevent release of energy source	Electrical insulation
Separate or channel away energy source	Electrical grounding
Physical barriers	
- Placed on source	Guards on fans, motors, etc.
- Placed between personnel and source	Rail on scaffold
- Placed on Personnel	Hard hat

In addition to examining unwanted energy flows and barriers, MORT analysis examines the third factor in a potential accident sequence, i.e., the persons/objects that may be injured/damaged by interacting with the unwanted energy. These persons/objects are said to be in the energy "channel." MORT analysis examines the functional presence of persons or objects in the energy channel, i.e., the analyst must answer the question, "For what reasons are these persons or objects involved in this location?" The MORT technique evaluates the administrative controls on and evasive actions that could be taken by particular persons or objects in the potential accident. Analysis of this third factor in a potential accident is particularly useful for identifying safe operating procedures for personnel and for evaluating one aspect of management's preparation for emergency situations where a large fraction of the mine personnel might be in the energy channel.

MORT analysis involves the use of what are called "analytical trees." These are simply a convenient way of displaying a large amount of information on a diagram. Analytical trees are shaped like trees in that they start at the top with a single undesired event and branch out below until the basic events, which are the underlying causes of the top event, are determined. In an analytical tree, the top or major event or outcome is stated. On the next lower tier are listed those events that could lead to occurrence of the top event. Each of these is broken down into more and more basic events to reveal the sources that contribute to the top event.

To illustrate the thinking process behind this logic, consider a mine ventilation system. Failure of this system to provide fresh air to miners downhole could cause suffocation and build-up of harmful or explosive gases. The top event for this illustration is assumed to be failure of the mine

ventilation system to provide sufficient fresh air downhole. The thinking process the analyst goes through to construct an analytical tree for this top event is as follows. First, the analyst considers the top event and asks the test question, "How could this happen?" Some of the answers might be failure of the electric power supply system or failure of the ventilation fan. Next, the analyst asks the test question regarding the second tier of events. The analysis continues until the specific causes and entire range of accident "sequences" have been identified.

To understand the MORT analysis procedure and the techniques for construction and use of analytical trees, the reader must become familiar with the symbols and abbreviations used in MORT analysis. The symbols (sometimes referred to as "gates") are used to represent the logic for combining events into accident sequences. For example, the mine ventilation system could fail if either electric power is unavailable OR if the fan system fails to operate. Thus a symbol is needed to represent the OR relationship, which means that the output event (i.e., mine ventilation system failure) can result if any of the input events occur. A second symbol used extensively in analytical trees is the AND symbol. This symbol represents the logic where all of the input events must occur for the output event to occur. For example, in order for a mine hoisting bucket to fall uncontrolled down the shaft (output event), the bucket's primary braking system AND the emergency braking system must both fail at the same time. Therefore, the latter two events, which are input events to the uncontrolled falling bucket event, are connected with an AND symbol. These symbols are presented and described in Figure 6.

The AND and OR symbols are used the most often when constructing analytical trees. Two other logic symbols or gates that are used occasionally in specific situations, as shown in Figure 6, are the "INHIBIT-gate" and the "DELAY-gate." The INHIBIT-gate is a special case of the AND-gate, where some qualifying condition must be satisfied before the input can produce the output. A hexagon is used to represent the INHIBIT-gate and the conditional input is spelled out in an ellipse drawn to the right of the gate. As an example of an application of this type of gate, consider the event "Fire occurs in a diesel electric generator." One of the causes of this event might be a leak in the fuel system that ignites when the generator is energized. One condition that must be satisfied in order for this fire to occur is that current must be supplied to the diesel engine starter system in order for an electrical spark to ignite the leaking fuel. This is an example of an INHIBIT-gate for illustration purposes only.

The DELAY-gate, shown in Figure 6, is represented by an ellipse attached beneath an event symbol. This gate is used to indicate that the output occurs only after a specified delay time has elapsed. To illustrate the use of this gate, consider the mine ventilation system which not only supplies breathing air for miners downhole, but also dilutes and carries away potentially explosive mine gases such as methane. Once the ventilation system has failed, it takes a period of time before the mine gases can build up to a point where they are potentially explosive mixtures. The DELAY-gate would be used in this instance to indicate the amount of time that must elapse after the ventilation system fails (input event) to produce the potential explosion of mine gases (output event).

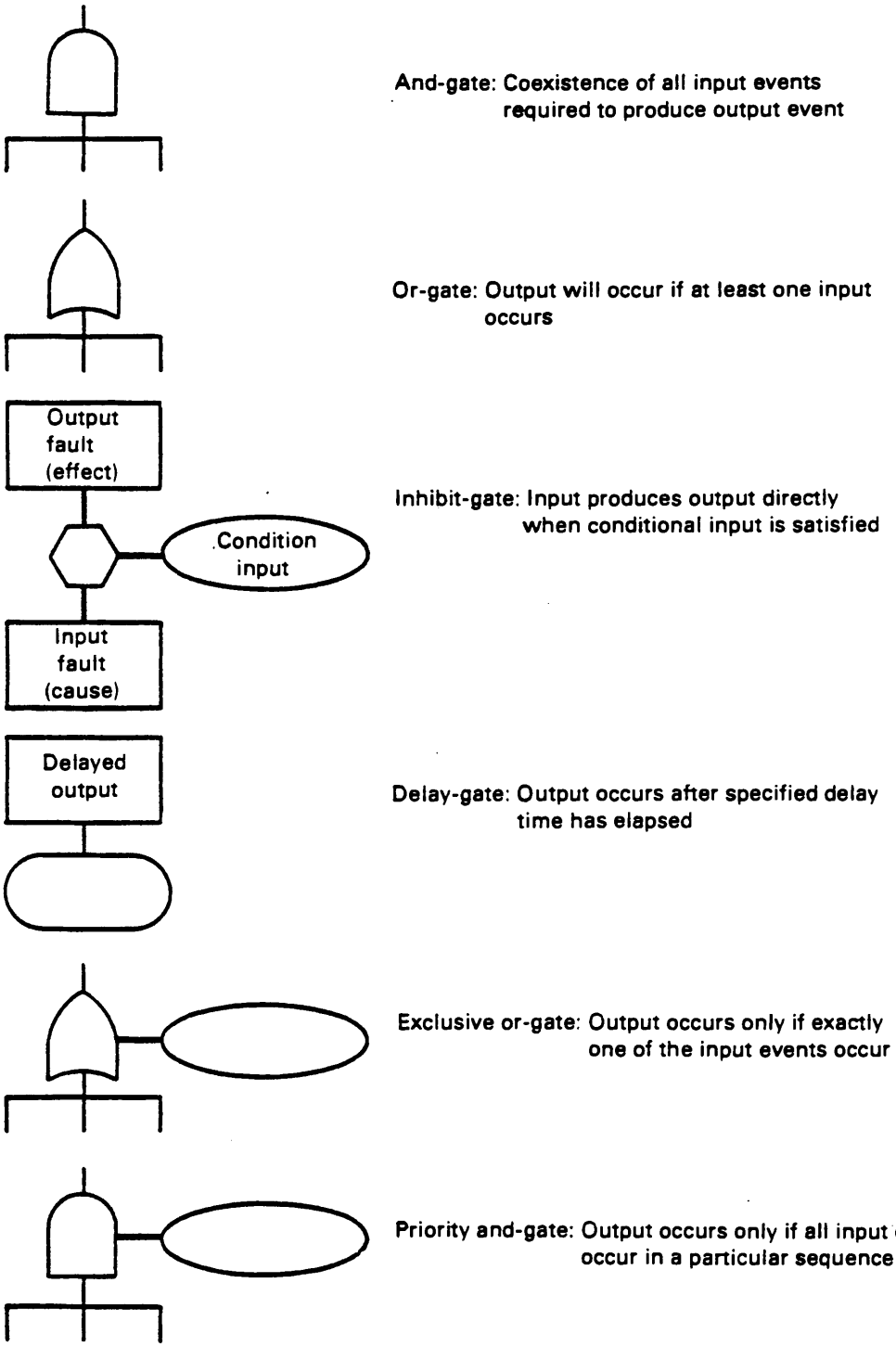
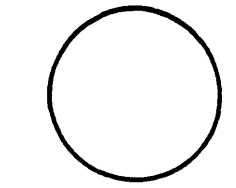


FIGURE 6. - Logic symbols used in construction MORT-type analytical trees

The ellipse symbol is used to indicate conditions or restrictions that apply to normal AND- and OR-gates. When attached to an OR-gate, the new symbol is called an "EXCLUSIVE OR-gate." This gate is used in the special case where the output event occurs only if exactly one of the inputs occur. This gate differs from the usual OR-gate in situations where the output event will not occur if more than one input event occurs at the same time. When the ellipse is attached to the normal AND-gate, the new symbol is called a "PRIORITY AND-gate." This gate is used where the output event occurs only if all input events occur in a particular sequence. The sequence is recorded within the ellipse. It is rarely necessary in practice to have to use these symbols.

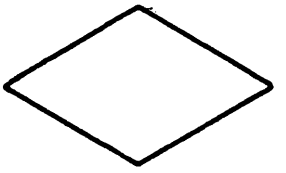
Symbols are also used to represent events. The event symbols used for constructing analytical trees are shown in Figure 7. The different event symbols are used to represent different types of events. The CIRCLE denotes a basic event that can not be developed further. These are the underlying causes of accidents that the analyst wishes to determine. Somewhat similar to the CIRCLE-symbol is the DIAMOND-symbol which also represents events that are not developed further. However, the events within a DIAMOND are not fully developed to their basic causes, either because the event is not sufficiently important or because information relevant to the event is unavailable. The HOUSE-symbol is used to signify an event that is normally expected to occur and is thus not a fault or failure event. For example, consider a fire caused by failure of the filling lines used to transport fuel from storage tanks to surface vehicles such as front-end-loaders. This fire can only occur during filling operations as these lines have fuel in them only during this time. The HOUSE-symbol is used in this situation to indicate that this fire can only occur while a vehicle is being refueled. The final event symbol on Figure 7 is the RECTANGLE which is used to identify events that are combinations of more basic events. The outputs shown above the logic gates previously discussed must be within RECTANGLE symbols.

A TRIANGLE symbol is also shown on Figure 7 but is not actually an event symbol. The TRIANGLE signifies what is called the "transfer operator." The transfer symbol is essentially a time-saving measure used to represent exact repetitions of a branch of a tree that is found elsewhere. For example, failure of the electric power supply at a mine is an event associated with many system failures, including ventilation system and hoisting system failure. Let us say, for instance, that the electric power failure event is developed as one of the causes of the ventilation system failure. By using the transfer symbol, the entire branch of the tree for electric power failure can be repeated under the hoisting system failure event without drawing the entire branch. Two TRIANGLE symbols are required for this operation; a transfer-in symbol is placed in the location where the branch of the tree will not be drawn (i.e., under the hoisting system failure in the above illustration) and the transfer-out, which is placed in the location where the branch of the tree is drawn (i.e., under the ventilation system failure, attached to the electric power failure event that is assumed to be drawn in this location). Numbers or letters are normally placed insde the triangle symbols to help the analyst keep track of the transfers.



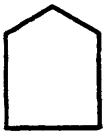
Event symbols

Circle - Denotes basic initiating event requiring no further development

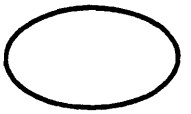


Diamond - Denotes undeveloped events which are not further developed because it is of insufficient consequence or because information is unavailable

Rectangle - Denotes an intermediate event that occurs because of one or more prior causes acting through logic gates



House - Denotes an event that is normally expected to occur



Ellipse - Denotes a conditioning event or restrictions that apply to any logic gate (used with priority and inhibit gates)

Triangle - Transfer symbols; used to represent portions of the tree developed elsewhere

*Common abbreviations used in Mort analysis

D/N	Did not	MGH	Potential energy
LTA	Less than adequate	SUPV	Supervisor
MGMT	Management	CONS	Consequent
W/	With	PREC	Precedent

FIGURE 7. - Event symbols and abbreviations used in constructing MORT-type analytical trees

Many abbreviations are used in MORT analysis to aid the analyst in fitting descriptive information into the event symbols. The most commonly used abbreviations are shown in Figure 7.

This completes the discussion of the symbols the analyst uses when constructing analytical trees. The structure of the MORT-type analytical tree, or MORT diagram, is shown in Figure 8. This figure shows the top elements of the MORT diagram which in full is a large and detailed analytical tree. A copy of the entire MORT diagram is available from the System Safety Development Center, E.G. and G., Idaho Inc., Idaho Falls, Idaho. The MORT diagram is the actual checklist of safety program concepts and elements that are examined to determine the causes of accidents. A detailed discussion of all of these concepts fills several large documents and thus cannot be repeated here. For this report, some general information concerning the three main branches of the MORT diagram is sufficient. The reader is directed to the MORT text and supporting documents for a more detailed discussion.

The structure of the top of the MORT diagram, as shown in Figure 8, is composed of three main branches. Assumed risks are shown on the right and oversights and omissions due to specific control factors and management system factor are shown on the left. The MORT technique is based on the premise that all accidents are a result of either oversights and omissions (i.e., mistakes) or assumed risks. Assumed risks are those events that have been recognized and accepted by proper levels of management as accidents or hazardous conditions that cannot be prevented due to technological or economic constraints. Unknown or unanalyzed risks cannot be considered as assumed risks. The reader should recognize by inspecton of Figure 8 that the occurrence of the top event of the tree is either the result of assumed risks or the result of oversights and omissions from a combination of less than adequate specific control factors AND management system factors, i.e., both of the latter two factors are to blame for the potential accidents under analysis.

Analysis of the specific control factors branch of the MORT diagram develops a detailed understanding of the accident sequence. This branch is used to examine the sources of unwanted energy flows to determine if specific control factors were overlooked or omitted. This branch also evaluates the adequacy of the barriers provided and the involvement of the persons and/or objects that may be injured or damaged. Finally, this branch examines the relationships between the safety management system and the accident sequence. Examples of safety program elements in this branch are inspection and maintenance plans, supervision, and technical information systems.

Oversights and omissions due to management system factors are broken down into three main sub-branches. The idea is to separately examine the management system's safety policies, the implementation or fulfillment of the policy statements, and the system used by management to assess the risk of personnel injury or property damage and take appropriate actions. The risk assessment system is used by management to determine whether a particular accident should be an assumed risk or whether preventive action is appropriate and feasible.

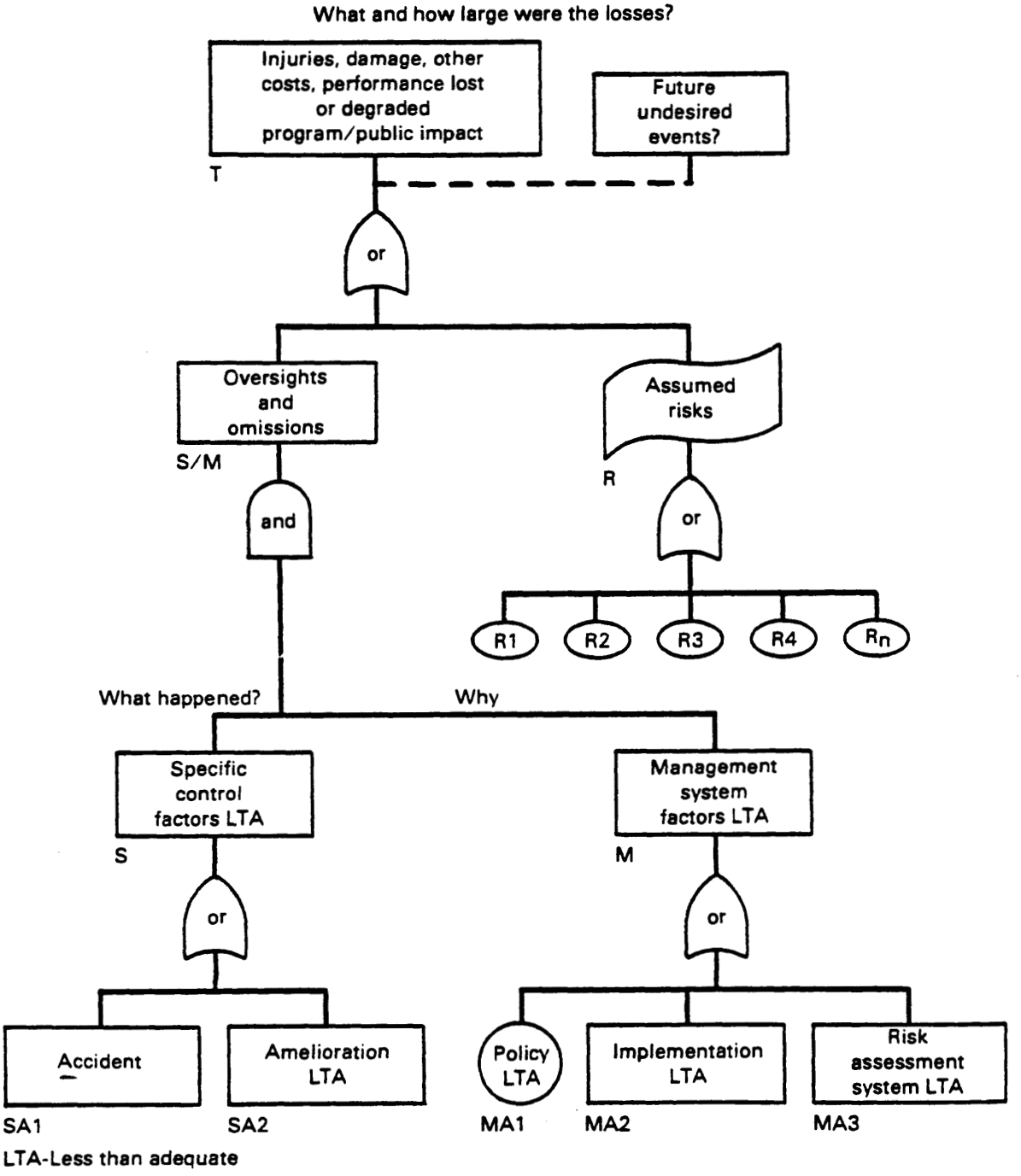


FIGURE 8. - Structure of the MORT-type analytical tree

This completes the background information regarding MORT analysis that will be discussed. This information is required to understand the analysis procedure that is the next topic of discussion.

The MORT analysis procedure involves a close, element-by-element examination of the standard MORT diagram (included inside back cover of this report). The analysis procedure discussed in this section is directed towards planning or evaluating a safety program, although MORT analysis is also used as an accident investigation tool. Before beginning the MORT analysis, the analyst must become thoroughly familiar with the system under consideration and should also obtain the MORT documents discussed previously. The analysis begins with selection of the accident to be examined. This can be postulated using the analyst's personal experience or using some other safety assessment technique, such as Preliminary Hazards Analysis. The accident sequence and associated unwanted energy flows are recorded and examined under the event "ACCIDENT" (denoted SA1) shown on Figure 8. It is likely that more than one energy flow is needed to cause the accident. In this case, the causes of each unwanted energy flow must be examined. The causes are categorized into 6 classes, labeled SD1 to SD6 on the large MORT diagram. Each of these categories is in turn broken down into more and more basic safety program elements which, if less than adequate, could contribute to the potential accident. The short statements written in the event symbols of the MORT diagram need more clarification than can be given here. The best sources for more information are the MORT User's Manual (Knox and Eicher 1976) and MORT text (Johnson 1973). The user's manual contains cross-referenced explanation of the short statements and safety program elements in the event symbols, indexed with the numbers on the MORT diagram (such as SC1, SD6, etc.) and appropriate page references to the detailed explanations presented in the MORT text. These two documents are required for the analyst to perform an effective analysis.

Causes of the unwanted energy flow(s) are one of the three specific controls associated with the potential accidents. The other two controls are less than adequate barriers (SB2) and less than adequate control of persons or objects in the energy channel (SB3). The analyst evaluates these factors by examining the safety concepts shown on the MORT diagram under these two "events." Again, the above referenced documents help to make the short "event" statements more clear. This completes the discussion of the analysis procedure for the specific control factors branch of the MORT diagram.

Management system factors that could contribute to the potential accident are examined under the branch labeled "M". The analyst considers the management system concepts, which, if less than adequately defined or implemented, could contribute to the occurrence of the accident. These factors are considered in light of the knowledge gained by analysis of the specific control factors branch. The analysis procedure for the management systems branch is identical to the procedure for the specific control factors branch. Again, detailed discussion of each management system factor is beyond the scope of this manual.

Throughout the analysis, it will become obvious that some branches of the MORT diagram are more relevant than others. The analyst can also identify safety elements which, if less than adequately implemented, could contribute to the occurrence of the potential accident. Therefore, some way of recording the information obtained is required. One method that uses the large MORT diagram as a worksheet is as follows. First, a thorough examination of the major branches of the MORT diagram will reveal branches that are not relevant to the potential accident under consideration. These branches can be marked with a large, red "X" to identify branches that need no further consideration. Next, the analyst examines the more basic safety concepts in detail. Those that are considered to be irrelevant should be identified with a red circle. Those elements and concepts that are relevant require further consideration to determine if they are contributors to the potential accident. At this point, the analyst evaluates the adequacy of the safety concepts on the diagram in regard to the potential accident. Test questions that help determine their adequacy are contained in the MORT User's Manual (Knox and Eicher 1976). Those that are not adequate and are shown to be potential contributors to the occurrence of the accident should be marked with a blue circle. It is helpful to record notes of this evaluation process to aid future use of these results. In fact, it is extremely useful to formally describe this process in a format that uses the index number of each element of the MORT diagram. An example to illustrate this is presented later in this manual.

Next, the analyst should display the results by drawing a MORT-type analytical tree that is specific to the accident being analyzed. The same format used in the large MORT diagram can be used, but only the safety elements and concepts that were determined to apply to the accident sequence and are judged to be less than adequate are included. The analyst begins at the top of the tree by identifying the consequences of the potential accident and continues downward. It will most likely require more than one page to record the entire tree so transfer symbols should be used to identify interconnections between pages. This completes the discussion of the MORT analysis procedure. The procedure is summarized in Table 20.

Advantages and Disadvantages

One advantage of MORT analysis is that it is a very comprehensive technique that attempts to evaluate all aspects of safety in any type of work. It is essentially the only method that examines all three aspects associated with an industrial system (hardware, humans, and management systems) separately and as they act together to cause accidents. MORT is a structured and systematic analysis technique although it is flexible and allows incorporation of new ideas and concepts. MORT analysis results can suggest improvements to an existing safety program which could save lives, reduce injuries, and reduce property damage. In addition, the technique is useful for identifying areas where further use of safety systems (such as safety equipment, warning signs, and training) could reduce the likelihood of accidents. Furthermore, much of the analysis has been performed for the analyst in that the MORT diagram and reference documents contain a wealth of information that could assist improving an existing safety program or developing a new one.

TABLE 20. - Step by step procedure for performing a MORT analysis

Step 1:	Obtain adequate working knowledge of the system.
Step 2:	Select the accident to be analyzed: The selection process can be aided by performing a preliminary hazards analysis to identify potential accident sequences.
Step 3:	Identify hazardous energy flows and barriers associated with the potential accident sequence: The analyst may use checklists to identify these elements.
Step 4:	Record this information in the standard MORT-type analytical tree format: The analyst should copy the structure of the standard MORT diagram and incorporate the unwanted energy flow and barrier information. This information is contained in the specific control factors branch of the MORT diagram.
Step 5:	Evaluate the causative factors of the initial unwanted energy flows: This is done by examining all safety program elements of the MORT diagram in regard to the unwanted energy flow. The technique asks questions about each safety element that the analyst is to answer.
Step 6:	Record the safety program elements which are determined to be less than adequate in regard to the unwanted energy flow: Copy the structure of the MORT diagram and include only those elements that are determined to be less than adequate.
Step 7:	Continue analyzing the safety program elements in regard to the rest of the unwanted energy flows (if any): Repeat steps 5 and 6 for every unwanted energy flow.
Step 8:	Evaluate the management system factors associated with the potential accident: Repeat steps 5 and 6 for the management system factors branch of the MORT diagram.
Step 9:	Examine the completed analysis for safety program elements thatcould reduce the likelihood of the potential accident occurring.

The MORT analysis technique has the disadvantage that it creates a vast amount of complex detail. The analyst should make a habit of recording notes throughout the analysis so he or she is not overcome by the great detail. The technique is also time-consuming, at least until the analyst has gained experience. MORT analysis is a flexible technique, thus being harder to perform than a "cookbook" type of analysis. This technique is also a difficult one because it emphasizes management's responsibility to provide a safe work place. Results of this analysis can test the understanding and commitment to safety that management must have to ensure a successful safety program.

Example of Analysis Procedure

This section presents an example to illustrate the MORT analysis procedure. The postulated accident chosen for this example is one where a hoisting bucket falls down a mine shaft. The analyst first becomes familiar with the hoisting system (see Figure 1 shown previously) and can quickly determine that this is a low probability accident because of the presence of many barriers. The postulated sequence of events leading up to rope failure and a falling bucket is as follows. First, the hoistman must be lifting personnel from the shaft bottom with defective brakes. Either the brake hydraulic pressure gauge is defective or has been disengaged resulting in the bucket being hoisted without brakes. In conjuncton with this, the emergency brakes must be inoperable. Another barrier to the accident is the overwind control, which allows the hoist to be automatically shut down when the top limit is reached, thus avoiding a collision of the bucket with the headframe and resulting rope failure. If the bucket is still being hoisted at this point, a crash bar is provided that could stop the bucket before it hits the headframe. Two additional barriers are provided in case the bucket reaches this point. First, the rope is designed with a factor of safety that could prevent its failure if the crash is not too violent. If the rope does snap, a safety catch is provided that may be capable of stopping the bucket from falling to the shaft bottom. It is due to these many safety features that this accident is assigned a low probablity of occurrence.

With the above accident sequence in mind, the analyst begins to identify and examine the unwanted energy flows that caused the accident. First, the unwanted energy that causes the bucket to fall down the shaft is potential energy or the increase in energy due to raising an object over some distance. Prior to this, the kinetic energy (energy of a moving object) of the bucket causes it to strike the headframe. Before this happens, the bucket must be in motion (kinetic energy) with defective brakes. The analyst records this information by copying the general structure of the MORT diagram and incorporating this information, as shown in Figure 9. This is drawn under the specific control factors branch of the tree. Each of the causes of the unwanted energy flows are then examined, including an assessment of the adequacy of the barriers to the energy flows. The analyst examines each safety element of the MORT diagram and indicates which could be contributing factors to the postulated accident. An example of a branch for the falling bucket accident is shown in Figure 10 for illustration purposes (note the use of the triangle transfer symbol on Figures 9 and 10). The branch of the tree shown in Figure 10 is the result of the analysis that identifies potential causes of the falling bucket accident. The analyst continues examining and recording the specific control factors shown on the large MORT diagram that could cause the unwanted energy flows. Then, with the information from this procedure, the analyst is ready to evaluate the management system factors that could contribute to the potential accident. The procedure for this is identical to the procedure used to evaluate the specific control factors branch, i.e., an element-by-element examination of the management system factors branch of the large MORT diagram.

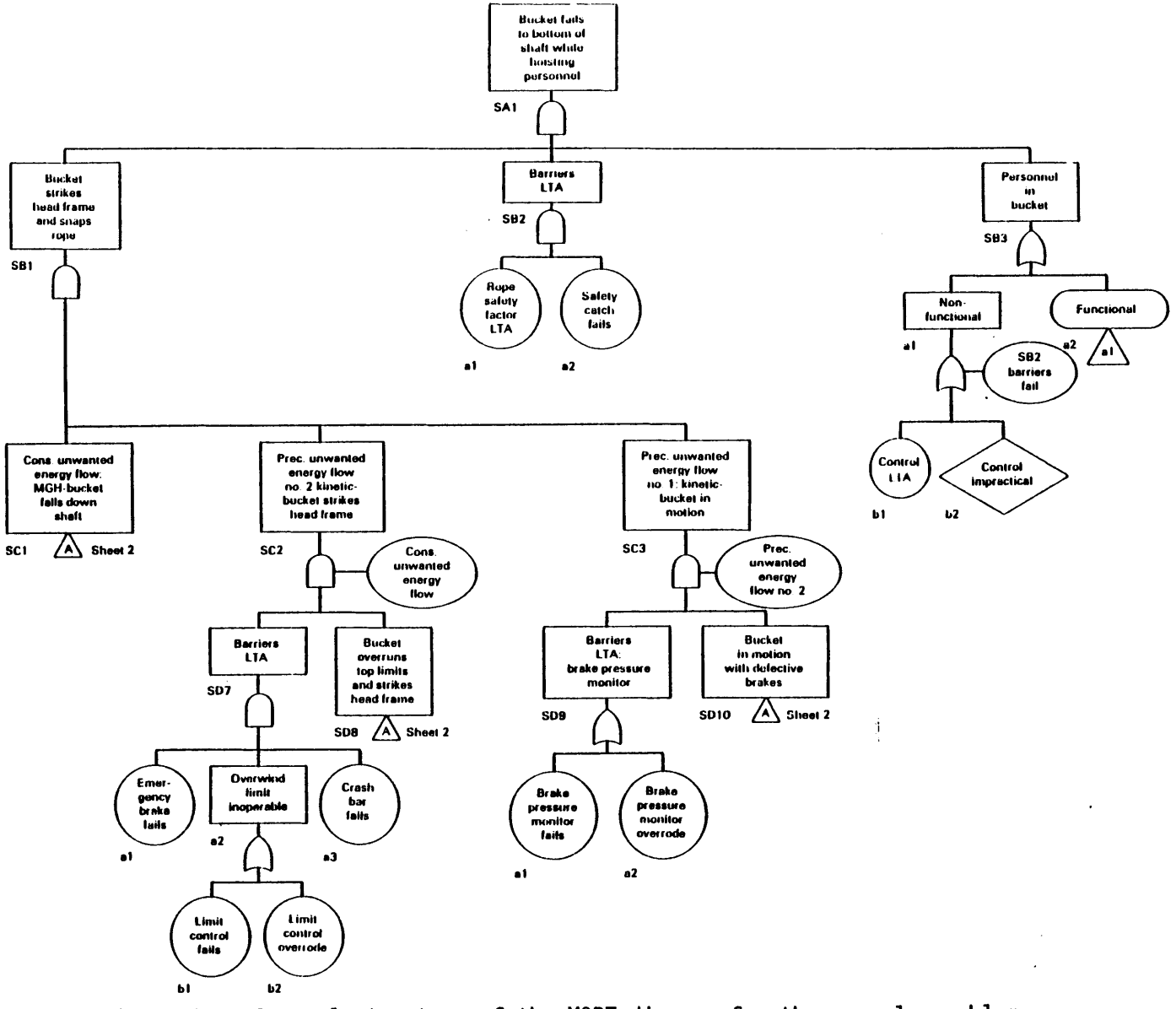


FIGURE 9. - General structure of the MORT diagram for the example problem

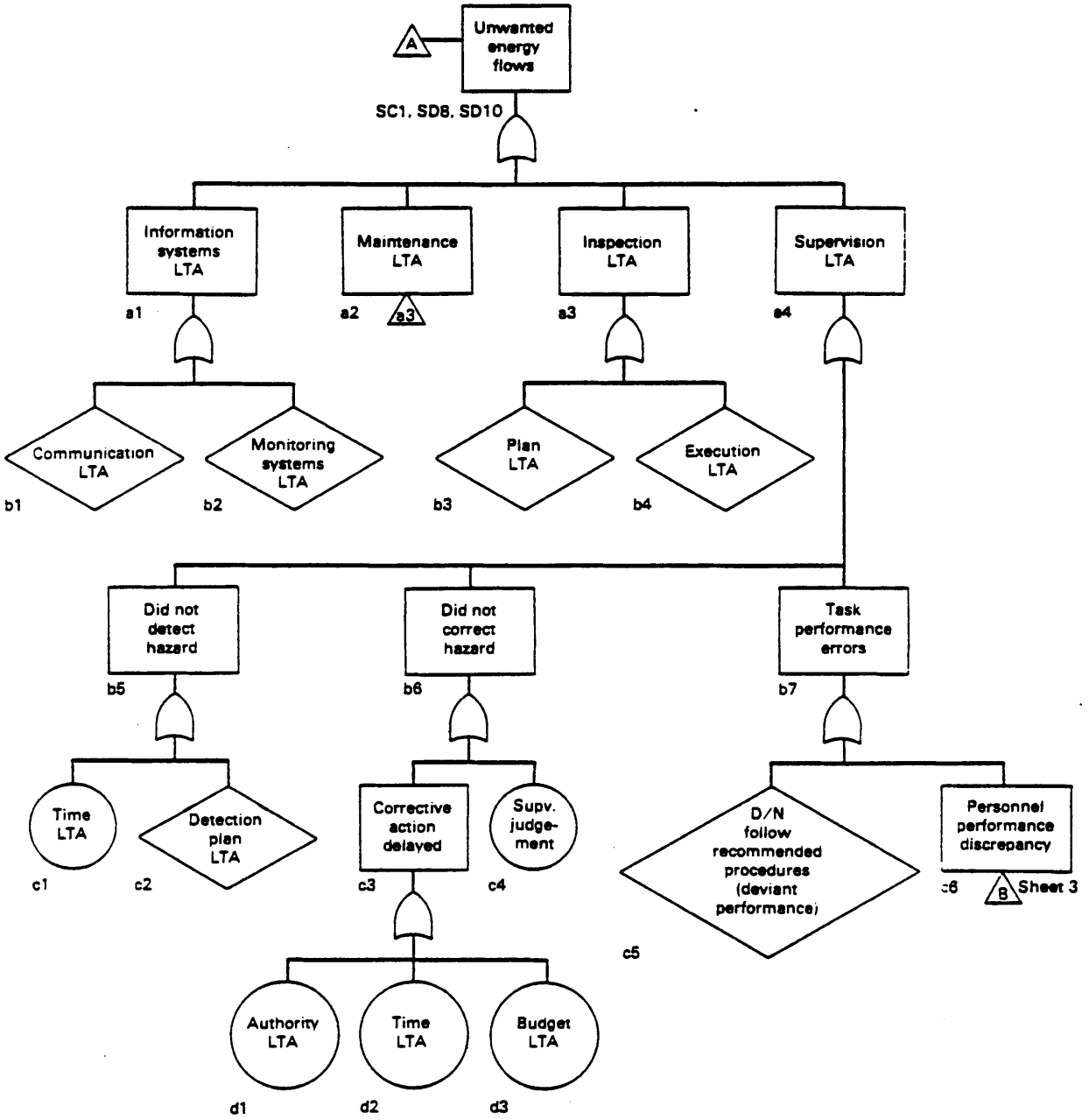


FIGURE 10. - Example branch from the MORT diagram for the example problem

The result of the above process is a MORT-type analytical tree specifically for the postulated accident. The analyst's next step is to record the logic associated with the potential accident sequence and the reasoning behind the selection of the less than adequate safety elements included in the MORT diagram. This is not required but is recommended for the analyst to preserve details of the evaluation for future use. A structured format indexed to proper locations on the MORT diagram like that shown in Table 21 is useful.

Results of the MORT analysis indicate the most important oversights that could lead to this accident relates to maintenance and inspection procedures. An inspection plan exists that appears adequate to prevent this accident. However, supervisors should ensure that personnel performing these tasks do so in a rigorous and thorough manner. Supervisors should also see that maintenance-related activities are performed effectively and promptly. It is recognized that the decision to change a hoist rope is a management responsibility but supervisors must see that management is notified that a rope is worn or damaged. The authority to repair or replace hoist safety systems could be given to supervisors to assure prompt correction of hazards.

Some other safety program features that application of MORT analysis to the example problem identified are as follows. Training of supervisors and inspection personnel in the area of hoisting component degradation should be adequate so they can spot failures. It is important to adhere to requirements for a test run of the hoist prior to each shift in case inspection or maintenance personnel are not well-trained or motivated. Management and supervisors must ensure that checklists are filled out prior to each shift indicating the status of hoisting components and hoist safety features. These procedures would take approximately fifteen minutes.

Design personnel who have the task of calculating rope stress and specifying the proper ropes for use should be well-trained with a thorough knowledge of the task. In addition, these calculations and specifications should be reviewed thoroughly by competent personnel. Designs of safety systems or the hoisting equipment should incorporate the technology, as much as possible, to ensure reliability and availability. It is the responsibility of management to supply information on the latest technology to designers and to incorporate it in final designs. Supervisors should be aware of design and operating personnel discrepancies, such as personal conflicts, lack of motivation, or disregard of recommended procedures. As mentioned earlier, the most effective accident prevention and control measure is to design the system for minimum hazard, as has been done for this system.

This example has illustrated the MORT analysis procedure and has provided an example for the reader to follow when actually performing the analysis. It has also shown the kind of results to expect from application of this technique. The complete analysis of the postulated accident can not be shown due to its length and level of detail.

TABLE 21. - MORT logic for muck bucket falls to bottom of shaft while hoisting personnel: example sheet

SA1. Accident:

The bucket falls to the bottom of the shaft while hoisting personnel.

SB1. Incident:

Brake failure causes the bucket to overrun the top limit, strike the headrame, and snap the rope.

SB2. Barriers LTA:

Two barriers are provided to prevent the bucket from falling after striking the headframe. Both must fail in order for the bucket to fall.

a1. The bucket will not fall unless the rope snaps. The rope is designed with a safety factor.

a2. In case the rope snaps, a safety catch is provided to prevent the bucket from falling.

SB3. Persons in Energy Channel:

Persons are inside the muck bucket when they are being hoisted.
NOTE: A similar accident would be one where the persons in the energy channel are underneath the muck bucket on a galloway deck or on the shaft floor under the muck bucket wells.

a1. Nonfunctional personnel may be in bucket, e.g., authorized visitors, trespassers, etc.

b1. Control of access to the bucket by non-functional persons may be LTA.

b2. Control of access may be impractical.

a2. Persons in bucket may be functional (operators).

b1. Control of access to bucket by functional personnel may be LTA.

b2. Control of access may be impractical.

SC1. Consequent Unwanted Energy Flow:

MGH - bucket falls down shaft.

Computer Adaptability

Evaluation of the computer adaptability of MORT analysis indicates that it is both feasible and desirable. Since MORT has been reduced to a large, comprehensive diagram, the feasibility of adapting it to the computer is virtually ensured. It is desirable to adapt the MORT technique to the computer for the purposes of reducing the amount of paperwork involved and for assisting the analyst to conduct the assessment in a structured format, thus reducing the possibility of error or omission. The size of the computer program required to adapt MORT analysis to a user-interactive computer is relatively large because the technique integrates over 1500 safety program elements and safety concepts into the large MORT diagram. This results in a significantly larger labor requirement to install the program initially and to perform the first stage of the analysis.

The conceptual computerized MORT safety analysis program is envisioned to be a 2-stage approach as shown in Figure 11. Stage 1 is a computerized guide to the analysis procedure, including checklists and other specialized forms commonly used in MORT analysis. The computer program could be made user-interactive so the computer would ask questions that the user must answer. With the aid of computer graphics, portions of the MORT diagram could be displayed on the screen to offer the analyst a broad view of the location of specific information. In other words, the conceptual computer program would be able to ask a question for the analyst to answer regarding some element of the MORT diagram while displaying the immediate branch of the tree surrounding the element.

Stage 1 of the conceptual computer program is the actual performance and recording of the analysis. The structure and framework of the standard MORT diagram would be programmed into the computer software. As discussed above, the computer could display the top portion of the MORT diagram and begin asking the suggested questions contained in the event boxes, just as in the paper-type study. Prior to this, the analyst must have chosen the potential accident sequence to be analyzed and given some consideration to the hazardous energy flows and barriers. The checklists shown in Tables 18 and 19 could be programmed into the computer software and displayed when needed to refresh the analyst's memory. The analysis procedure begins with the computer asking questions regarding the top event of the MORT diagram, then continues down the specific control factors branch of the tree, and then analyzes the management system factors branch. The standard rules and symbols of analytical tree construction would be used, although only the event statements of the MORT diagram need be shown on the displayed tree branch. The answers to the questions asked by the event statements would be typed into the computer memory and displayed on the screen. It may take a special, large screen to display this much information, although it is believed it can be done. A drawing of the conceptual display is shown in Figure 12. Important conclusions from the analysis may be input to a special memory file that may be printed out and utilized as a checklist for future safety inspections. This checklist may contain the hazardous elements and contributory causes to potential accidents.

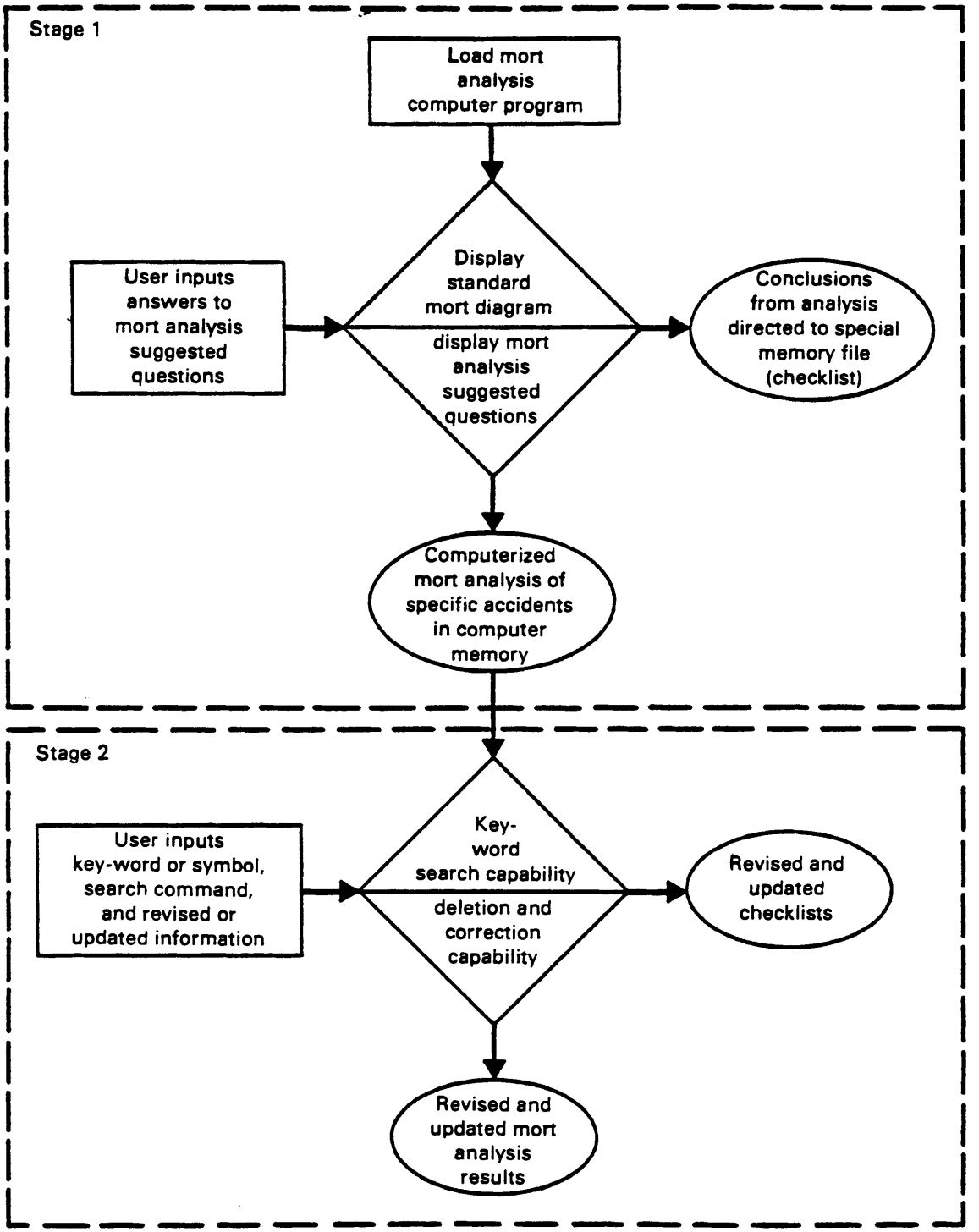


FIGURE 11. - Conceptual flow scheme for a computerized MORT analysis

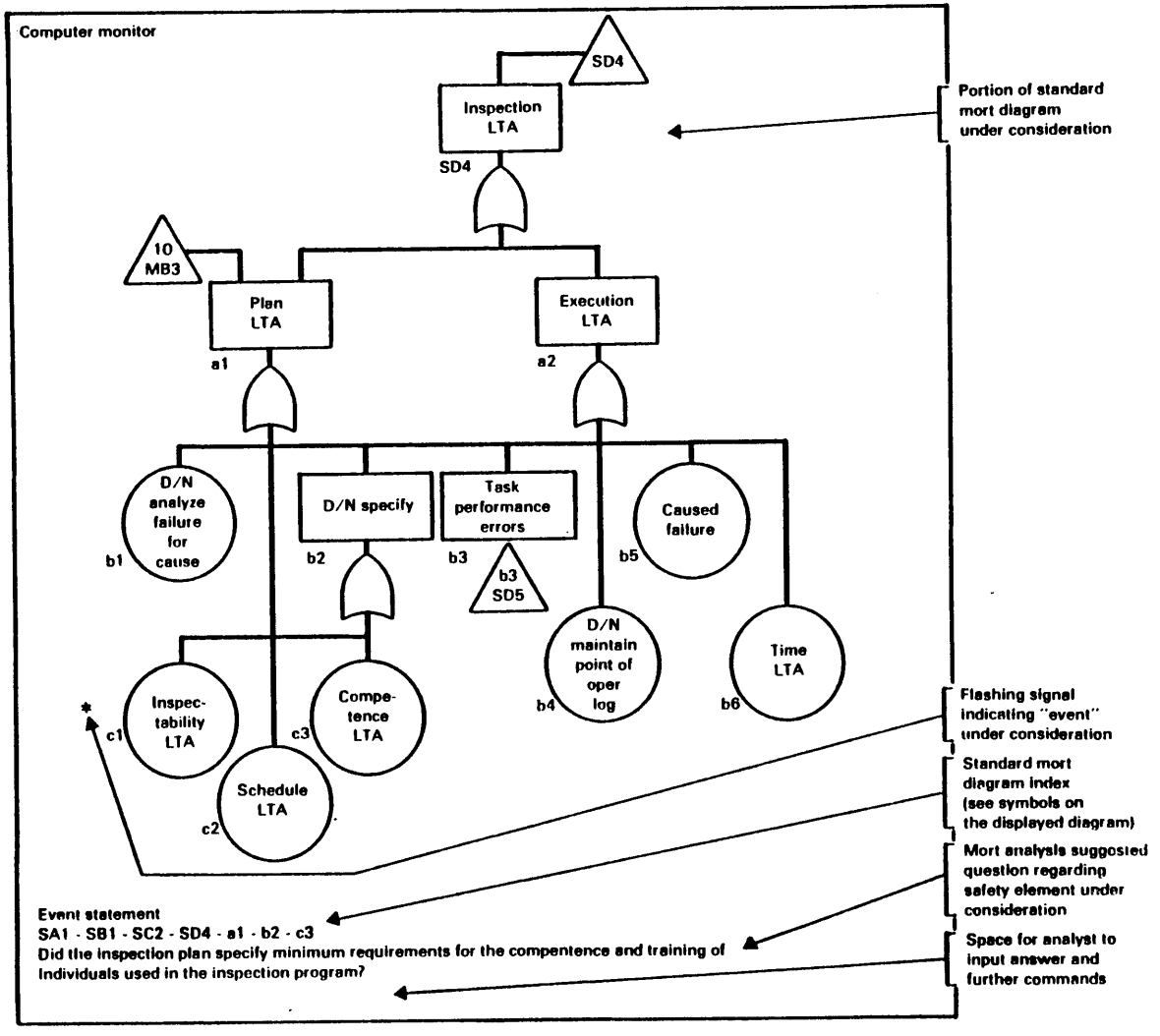


FIGURE 12. - Conceptual computer display for the MORT analysis procedure

Stage II of the conceptual computer program is necessary because MORT analysis and mining systems are both dynamic processes. The conceptual computer program is capable of deleting out-dated information and inserting modified or revised information regarding any safety program element the analyst wishes. It is envisioned that the program is provided with key-word search capabilities and indices to allow the analyst to rapidly search and display specific entries contained in the computer memory. The word processing capabilities of current computer systems enables the analyst to delete and insert information as needed. Using these capabilities, the MORT accident analyses could be revised in relation to the constantly changing mining system and the potentially new hazardous situations created by these changes.

Estimated Costs of Implementation

This section presents the bases, assumptions and estimated costs for implementation of a MORT-type safety program at a mine. Two estimated costs are developed: 1) the estimated costs for implementing a conventional paper-type MORT analysis safety program and 2) estimated costs for a computerized MORT safety program. The estimated costs developed in this section can be used by mine operators to weigh the costs of utilizing the MORT approach versus its benefits which have been discussed throughout this section.

The estimated costs of a MORT-type paper study were developed based on the assumption that the analysis is performed by the mine safety staff. Thus the costs are dominated by the costs for training these people and the labor costs for the training and for performing and updating the analysis. It is estimated that approximatley 1 month is required for MORT analysis training for each individual involved in the analysis. This month includes attendance at a one-week short course on MORT analysis and three weeks to review the analysis procedure and work some example problems. With this detailed training, the MORT analyst should be capable of completing the analysis of a potential accident sequence relatively quickly. Therefore, it is estimated that 1.0 man-years of staff labor is required to complete the initial MORT analysis of a large mining system. Assuming the safety staff labor rates and overheads discussed in the final report for this study, labor costs total $45,000 to $65,000 for performance of the initial analysis. The total cost of implementation also includes 1 month's labor costs for training 3 safety people in the MORT technique, including 2 safety foremen and their supervisor. These estimated costs are about $8,000 to $10,000. The estimated costs for three persons to attend the MORT analysis short course is about $9,000 to $12,000 including attendance fees, airline travel to the short-course location and the three persons' salaries, lodging and living expenses for one week. The total estimated cost of implementing a MORT-type safety program at a mine are thus $62,000 to $87,000. Since MORT is a dynamic process that must be updated and revised periodically, it is estimated that 3 to 4 man-months/year is required for this activity. Therefore, the estimated annual operating costs of the MORT safety program are about $10,000 to $15,000/yr. Note that these costs do not include the costs for an initial analysis (such as a Preliminary Hazards Analysis) to identify potential accident sequences. Only the costs associated with performing a MORT analysis are included in the above estimate.

The estimated costs for implementing a computerized MORT analysis includes the capital costs and installation of the computer system and software in addition to staff labor costs. Costs for an adequate computer system are based on a survey of currently available micro-computer systems and are estimated to be about $5,000, including delivery, installation and supplies. Annual computer maintenance costs are estimated to be 10% of the initial capital cost per year, or $500/yr. Also included in the estimated costs for a computerized safety program are costs for the safety staff to attend short courses on MORT training and computer training (including registration fees, travel, and living expenses). These costs are developed in the companion to this document and the assumptions will not be repeated here. It should be indicated that the one-month MORT training period and staff labor required to learn the paper-type analysis technique has been increased to 3 to 4 man-months to allow for the computer program to be loaded onto the computer system and the analysis to be initiated. Also, note that the estimated costs do not contain the costs for developing the computer software. These costs are difficult to estimate and it is not known if they will be paid by government or the mining industry. Therefore, the reader should recognize that software development costs are in addition to the estimated costs for implementing the computerized MORT-type safety program. The fixed and operating costs are summarized below:

FIXED COSTS

Computer system purchase and installation	$ 5,000
Short course attendance and expenses	$ 9,000-12,000
Analyst's burdened labor charges	
Initiate analysis	$10,000-15,000
Perform analysis	$45,000-65,000
TOTAL	$69,000-97,000

ANNUAL OPERATING COSTS

Computer system maintenance	$ 500/yr
Analyst's burdened labor charges	$10,000-15,000/yr
TOTAL	$10,500-15,500/yr

Since the MORT safety assessment program would be performed as a replacement to current mine safety official duties, the costs shown above are not additional costs. The actual additional costs above the costs for the current mine safety programs are lower.

HUMAN-RELIABILITY ANALYSIS

The most difficult component of a complex industrial system to characterize and evaluate is the human element. Accident statistics in industries where operations are predominantly some form of material handling, such as the mining industry, indicate that a large percentage of accidents are either caused initially by humans or human error in some way contributed to accident propagation. Human error is an important aspect of both normal and emergency situations. For this reason, human error (or conversely, human reliability) should be considered in a detailed systems safety analysis of a mining system.

Human-reliability analysis (HRA) is the study of human performance within a complex man-machine operating system. HRA can be used to develop qualitative information regarding the causes and effects of human error in specific situations. HRA can also be used to develop numerical human failure rate data that is normally used by fault tree analysts to estimate the probability of system failure. The quantitative portion of HRA is at this time not recommended for technology transfer to the mining industry due to the complex mathematics involved and minimal utility of the quantitative results at this time. It is believed that the qualitative portion of HRA can yield significant results for the mining industry by helping to identify the causes of their most frequent accidents, i.e., those caused by human error. With the information resulting from this analysis, mine safety officials and management will be able to identify design changes, procedural improvements, and specific areas of training that can help reduce hazards at mines.

Analysis Procedure

The procedure for performing the qualitative portion of an HRA is described in this section. First, a brief discussion of the limitations of such an analysis is presented. Then the analysis procedure is outlined and the major tasks are described. The reader should be aware that a detailed discussion of all aspects of the HRA fill entire textbooks. For a greater understanding of the methods presented in this sub-section, the reader is urged to study a recent publication, the Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278 (Swain and Guttman 1982). As the title suggests, this handbook emphasizes nuclear power plant operations but the general concepts are applicable to the mining industry.

Human performance is variable and thus, difficult to predict. Any given person frequently shows variability from day to day and from one moment to the next. Human behavior is also difficult to predict because humans perform more different functions in more different environments than any other component of a system. Furthermore, humans interface with many different elements (including other humans), accept a wide variety of inputs, and provide a wide variety of outputs. For these reasons, one of the limitations of HRA is that it cannot identify and eliminate all human errors. However, it is possible to evaluate the reliability of a human involved in a task for which he is adequately trained and suggest changes that might improve that reliability.

Human errors can be classified into two categories: situation-caused errors (SCEs) and human-caused errors (HCEs). SCEs are errors that are caused primarily by factors related to the design of the work situation. For example, less than adequate equipment designs, management practices, and operating procedures are SCEs. HCEs are errors with primary causes related to some human characteristic, such as sabotage or intentional errors. It has long been recognized that most errors in a well-defined work situation are due to SCEs and relatively few are due to HCEs. Therefore, the techniques described in this section are intended to enable the reader to identify and examine the effects of SCEs.

The analysis procedure for performing the qualitative HRA is summarized in Figure 13. The procedure consists of 6 tasks or steps. Each step is described separately in the following paragraphs.

STEP 1 - Describe the System Goals and Functions

The purpose of this step is to see where people fit into the system goals and functions. The analyst looks for what people are supposed to do to accomplish various functions and for points of interaction between the system and the people. These points are often defined as the interfaces between equipment and personnel; e.g., manual valves, switches for motor-operated equipment, displays to be read, and signals or cues to respond to. A useful technique for helping the analyst to identify interfaces is called a "link analysis". This technique is used to indicate the operational relationships between two elements of a system, whether they are two persons or a person and a piece of equipment. Link analysis is concerned with their positions, arrangements, and frequency of interchange. Once all links are identified, this step in the HRA is complete. However, the link analysis technique itself can be extended to gain further information for the task analysis procedure (see step 4 and 5) and on suggesting changes to the system (see step 6).

Link analysis is normally performed on centralized control operations and may not be as useful to the mining industry where most of the operations are performed manually. However, this technique is useful for defining the procedures used to perform a specific task, their proper order of performance, and cues to the operator related to which step in the task should be performed next. For example, consider the cutting operation at a coal mine. This operation is assumed to be performed using a rubber-tired vehicle that cuts the rock face with a cutting bar similar to a large chainsaw. A typical cutting cycle consists of several steps, including a methane check, a step to unlock the cutting bar, a step for connecting water hoses, and several steps for the actual cutting process. Link analysis consists of the following steps:

(1) Describe the task procedure in the proper operating sequence

(2) Estimate the time requirements of each step in the procedure

(3) Draw a simple illustration of the operation and indicate the movements of personnel that are required to perform the task. Record the locations where the tasks are performed and show by arrows the paths the operators must take.

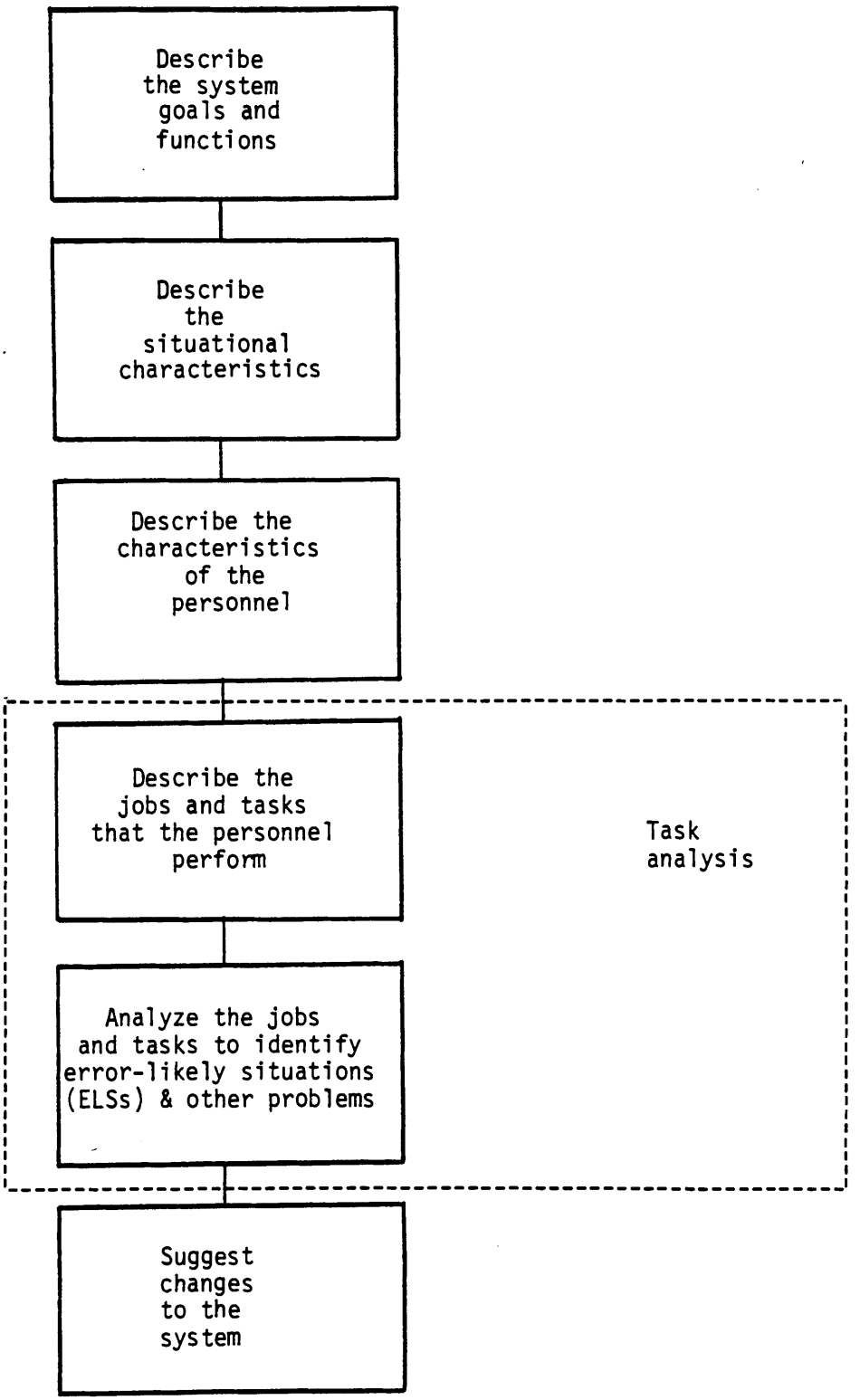


FIGURE 13. - Summary analysis procedure for the qualitative portion of a human-reliability analysis

With the task movements indicated on the diagram drawn in the last step, the analyst can identify such items as steps for which too little time is allowed for movement between stations, specific locations where the operator frequently returns, and cues which inform the operator when a task or step in a task should be initiated or completed.

Sources of information for this step include schematics, flow diagrams, block diagrams, design requirements, written procedures, and personal interviews with system planners and personnel with experience in the operation of similar systems. Visits to an existing or similar plant are also good sources of information. An extremely useful source of information is for the analyst to actually perform the tasks himself to get a very good understanding of the actual and potential problems in each task.

STEP 2 - Describe the Situational Characteristics

Many factors affect (or shape) human performance in a complex man-machine system. Some of these factors are external to the person in the system and some are internal. Such factors include the general work environment (especially equipment design and written and oral work procedures), the individual's skills, motivations, and expectations, and psychological and physiological stresses. These factors are termed "performance shaping factors" (PSFs). PSFs determine whether human performance will be highly reliable, highly unreliable or some level in between. A checklist of PSFs that can be used when performing this step is shown in Table 22. This checklist can be used by the analyst to identify the factors that could potentially cause a human to commit a performance error or omit a task or step. The analyst is to examine the system goals and functions obtained from Step 1 and identify the PSFs that could adversely affect the actions taken by operators.

As can be seen from Table 22, PSFs can be divided into three general categories: (1) those outside the individual, the external PSFs, (2) those that are a part of the individual himself, the internal PSFs, and (3) stresses and stressors. In general, external PSFs are those that define the work situations at the mine. External PSFs fall into three general categories. The first category is called "Situational Characteristics". Situational characteristics include PSFs that are often plant-wide or that cover many different jobs and tasks at the mine. For example, many deep underground mines are very warm and humid. These are two measures of the quality of the working environment which is a PSF that covers many jobs and tasks at the mine. "Task and Equipment Characteristics," include PSFs that are restricted or limited to some given job or even to a task within a job. This can be illustrated by the many tasks at mines that are performed by workers who specialize in a specific job, such as loading and firing blasting rounds or operating the hoisting equipment. "Job and Task Instructions," are those PSFs connected with instructional and training activities. This is essentially a sub-group of task characteristics, but are singled out because they represent an area that is a cost-effective method of improving human reliability.

The second general category of PSFs, internal PSFs, are the certain skills, abilities, attitudes and other human attributes a person comes to the

TABLE 22. - Checklist of factors that shape human performance

PERFORMANCE SHAPING FACTORS

EXTERNAL

Situational Characteristics

Architectural Features
Quality of Environment:
  Temperature, Humidity, Air Quality
  Noise and Vibration
  Degree of General Cleanliness
Work Hours/Work Breaks
Availability/Adequacy of Special Equipment, Tools, and Supplies
Manning Parameters
Organizational Structure (e.g., Authority, Responsibility, Communication Channels)
Actions by Supervisors, Coworkers, Union Representatives, and Regulatory Personnel
Rewards, Recognition, Benefits

Job and Task Instructions

Procedures Required (Written or not Written)
Written or Oral Communications
Cautions and Warnings
Work Methods
Plant Policies (Shop Practices)

Task and Equipment Characteristics

Perceptual Requirements
Motor Requirements (Speed, Strength, Precision)
Control-Display Relationships
Anticipatory Requirements
Interpretation
Decision-Making
Complexity (Information Load)
Narrowness of Task
Frequency and Repetitiveness
Task Criticality
Long-and Short-Term Memory
Calculational Requirements
Feedback (Knowledge of Results)
Continuity (Discrete vs Continuous)
Team Structure
Man-Machine Interface Factors:
  Design of Prime Equipment, Test Equipment, Manufacturing Equipment, Job Aids, Tools, Fixtures

STRESSORS

Psychological Stressors

Suddenness of Onset
Duration of Stress
Task Speed
Task Load
High Jeopardy Risk
Threats (Of Failure, Loss of Job)
Monotonous, Degrading, or Meaningless Work
Long, Uneventful Vigilance Periods
Conflicts of Motives about Job Performance
Reinforcement Absent or Negative
Sensory Deprivation
Distractions (Noise, Glare, Movement, Flicker, Color)
Inconsistent Cueing

Physiological Stressors

Duration of Stress
Fatigue
Pain or Discomfort
Hunger or Thirst
Temperature Extremes
Radiation
G-Force Extremes
Atmospheric Pressure Extremes
Oxygen Insufficiency
Vibration
Movement Constriction
Lack of Physical Exercise

INTERNAL

Organismic Factors

Previous Training/Experience
State of Current Practice or Skill
Personality and Intelligence Variables
Motivation and Attitudes
Knowledge of Required Performance Standards
Physical Condition
Attitudes Based on Influence Of Family and Other Outside Persons or Agencies
Group Identifications

job with. Internal PSFs determine the potential level to which an individual can be developed. Attitudes based on both outside and inside influences are especially important in mining because things are constantly moving about and changing. In this type of operation, one brief moment of uncertainty or inattention can cause someone to be struck by a moving ore car or by a backlashing scaling bar when the rock gives way.

The third class of PSFs are called stressors. In a well-designed man-machine system, the demands placed on workers to perform their tasks are consistent with the worker's capabilities, limitations, and needs. Any time that the requirements of a task impose too many demands on a worker, performance will suffer. This is one cause of stress. Stress can be psychological (mental) or physiological (physical). Stress can arise when there is a mismatch between the external and internal PSFs. For example, assume a mine under analysis uses blasting to loosen ore from the rock face. Blasting is normally restricted to two times each day, at the end of the day and evening shifts. This means that work is often hurried towards the end of the shift to prepare for blasting or the charge cannot be set until the end of the next shift. Many minor injuries, such as pinched fingers, crushed toes, etc., occur because of this psychological stressor - excessive task speed. In this example, the internal PSFs that motivate workers to complete a blast at the end of their shift (such as competition between shifts, bonus pay or incentive contracts) overshadow the external PSFs (such as warnings and cautions).

A detailed explanation of each PSF shown on Table 22 cannot be presented in this user's manual due to its length. Fortunately, most of the PSFs are self-explanatory statements. For a detailed discussion of each PSF, the reader is urged to study the primary reference for this section (Swain and Guttman 1982). To summarize the procedure, the analyst evaluates the PSFs in relation to the system goals and functions that were identified in Step 1. Then, the analyst records PSFs that could have an impact on the performance of humans and equipment individually and as they interact together to cause accidents. This step is particularly useful for identifying areas in which relatively minor changes can significantly reduce hazards.

STEP 3 - Describe the Characteristics of the Personnel

In this step, the analyst identifies the skills, experience, training, and motivation of personnel who operate and maintain the plant systems. This is done so the analyst can understand the capabilities and limitations of plant personnel. These aspects are then compared with the demands the systems place upon the personnel. Mismatches between capabilities/limitations and demands require modifications to the man-machine interfaces.

Two important aspects of this step are as follows. First, it is important to evaluate people's past experiences with other systems in order to avoid transfer of bad habits to the new system. Second, for safety-related systems it is especially important to evaluate provisions for response to low probability events, such as a failure of the ventilation system at a mine. Without this practice, the readiness to handle such events will decrease.

It is useful for the analyst to break the mining system down into major functional blocks and identify the tasks personnel are required to perform to fulfill each function. The analyst should identify and describe the characteristics of the personnel involved and compare them with the task demands determined in Step 2. Mismatches between the personnel characteristics and the task demands should be recorded and referred to in later stages of HRA. The analyst can consider these mismatches and, if possible, recommend measures to correct them by providing special training, reassigning personnel, or redefining the system goals.

STEP 4 - Describe the Jobs and Tasks that the Personnel Perform

Steps 4 and 5 together constitute a task analysis, which is defined as "... an analytical process for determining the specific behaviors required of the human components in a man-machine system" (Swain and Guttman 1982). The individual tasks, or steps in the task, form the basis of the human reliability model that is used to estimate numerical human error rates. This aspect of a task analysis is not discussed in this section.

Task analysis can be divided into two parts, description and analysis. Step 4 of the HRA is the descriptive part. In this step, the analyst breaks down the operating procedure into tasks or smaller units of behavior and enters this and other necessary information into a table. In most cases, the necessary information consists of such items as the piece of equipment on which an action is performed, the actions required of the worker, the limits of his performance, the locations of the controls and displays, and explanatory notes. With the system goals and functions from Step 1 and the situational characteristics from Step 2, the analyst can describe the demands that each job places on personnel. The purpose of this step is to describe the tasks and PSFs in detail to ensure that the analytical part of the task analysis (Step 5) is provided with sufficient information. In other words, this step is used to integrate the information from Steps 1, 2, and 3 into a logical format. There are many different formats for task analysis. The format is unimportant to the analysis. However, it is important to describe and analyze each task as necessary to identify error-likely and accident-prone situations. A recommended task analysis format that includes both a descriptive part and an analytical part is shown in Table 23.

The first five columns in Table 23 are the descriptive part of the example format. The analyst considers the job or task under analysis and assigns numbers to indicate the sequence of performance. Under the column labeled "Instrument or control," the analyst indicates each item that displays information to the operator, such as bells, lights, gauges, meters, and strip-chart recorders. The controls include such items as switches, keys on a computer console, connectors, and tools. The column labeled "Activity" is used for action verbs that describe the kinds of human actions related to the items in the second column. The action verbs used should help identify the kind of display or control used. For example, if a toggle switch is used, the words "Flip up," or "Flip down" can be used to describe the action. The analyst should indicate the position to which a switch is set or other measure of response adequacy. Under the column labeled "Cue for initiation or completion

TABLE 23. - Recommended task analysis format for performing an HRA

Job: ____ Task: ____ TASK BEHAVIORS (Description) Page ___ of ___ Pages TASK COMPONENTS											
Subtask: ____ Conditions: ____ Task Analyst: ____											
Task or Step	Instrument* or Control**	Activity	Cue for initiation or completion of activity (immediate or delayed)	Remarks	Task or Step	Scanning, perceptual, anticipatory requirements	Recall req's (LT = long-term ST = short-term # = initiating cue absent or poor)	Interpreting req's	Manipulative Problems	Likely human errors (or other problem areas)

*Anything that displays information.
**Anything that is manipulated.

of activity," the analyst indicates the cue that tells the operator when to begin a step and the cue that indicates the step has been completed successfully. Errors can result if the design of equipment and procedures do not provide good cues. Misleading or incomplete cues can result in the omission of some step in a procedure. Column 5, "Remarks," is used for relevant information that is not covered in Columns 1 through 4. This completes the task description phase that is designed to provide the necessary information for the analytical phase (Step 5) where error-likely and accident-prone situations are identified and examined.

A useful aid to the task description process is link analysis (see Step 1). This tool aids in the design and layout of control rooms and control consoles by depicting the pathways among different parts of a system as operators and other plant personnel move about checking and manipulating gauges, dials, etc., and communicating. This type of analysis can suggest improvements in the design of control centers and operating procedures to make the actions required of operators more convenient and thus, improve human performance. Link analysis can be applied to task procedures where a specific sequence of steps is required.

STEP 5 - Analyze the Jobs and Tasks to Identify Error-likely Situations (ELSs) and other Problems

This step is the analytical part of a task analysis. Each human action is analyzed to determine error-likely situations (ELSs) arising from equipment design features, methods of use, methods of training, and the skill levels of people in the system. ELSs involve errors that are likely to occur because the demands placed on humans exceed their capabilities and limitations. For example, if a toggle switch is used where the up position is "OFF," errors are likely because in this country we expect the opposite arrangement. A special case of error-likeliness that is often encountered is called an "Accident-Prone Situation" (APS). A familiar example of an APS is a slippery floor.

There are no well-defined rules for making the determinations of ELSs. The validity and effectiveness of the task analysis depends upon the ability of the analyst to put himself in the place of the operator so the actual and potential problems in each task can be identified and understood. For this reason, mine safety officials are the ideal candidates for performing a task analysis. However, even the best task analyst cannot hope to identify all possible human responses, predict all errors of omission or commission, or predict all extraneous actions by personnel. Still, it is possible in a thorough task analysis, given sufficient time, to identify most of the important tasks to be performed at a mine and most of the ways errors may be committed.

The "analytical" part of the task analysis format shown in Table 23 indicates the kinds of factors the analyst must consider in identifying an ELS. The listed factors are under four broad headings that are self-explanatory: (1) scanning, perceptual, anticipatory requirements, (2) recall requirements (long-term or short-term memory), and initiating cue (present, absent or poor), (3) interpreting requirements, and (4) manipulative problems.

Normally, entries are made in the analytical half of the form only when the analyst identifies an ELS. In reference to the factors in the columns, ELSs exist when the operator's capabilities are exceeded by the system demands for recalling, interpreting, decision-making, or manipulating processes. These errors can be errors of commission or omission, extraneous acts, or sequential or time errors.

The analyst makes entries in the analytical part of the form only when an ELS is identified. The analysis is done for each task or step in a task to determine the PSFs that seem likely to result in errors. In other words, ELSs are situations in which the performance shaping factors in a task are not compatible with the capabilities and limitations of the intended performer of the task. Task performance errors can also result when there are conflicts between external and internal PSFs. This type of information leads to the identification of the causes of ELSs and will indicate if human reliability can be improved by changing any PSF. This leads up to the final step in performing the qualitative portion of an HRA.

For further assistance in identifying ELSs, the reader is referred to several publications. According to Swain and Guttman (1982), the most concise document is MIL-STD-1427B, Military Standard, Human Engineering Design Criteria for Military Systems, Equipment and Facilities (U.S. Department of Defense 1974). Two other useful publications include ERDA-76-45-2, SSDC-2, Human Factors in Design (Nertney and Bullock 1976) and a textbook Human Factors in Engineering and Design (McCormick 1975). These documents present large amounts of information on the best ways to design human interfaces. Although these documents are useful, the best way to identify ELSs is for the analyst to perform the tasks himself supplemented by observing and interviewing operators who perform the tasks. To ensure that sufficient information is obtained by the analyst, the checklist shown in Table 24 can be used. This checklist is extremely useful for identifying the information that should be placed in the analytical half of the task analysis format.

STEP 6 - Suggest Changes to the System

This is the final step in the qualitative assessment stage of an HRA. In this step, the analyst reviews the information obtained in Steps 1 through 5 and suggests measures that could eliminate or mitigate specific ELSs. The three documents on human factors listed in Step 5 are excellent sources of information for suggesting these measures. Using the results of the task analysis as a guide, suitable design changes to system components can be developed that could reduce the likelihood of human errors, increase the likelihood that an error will be detected or corrected, or it may provide for the system to tolerate the error. The design changes may address any of the performance shaping factors associated with the potential error.

Advantages and Disadvantages

A major advantage of performing an HRA on a mining system is that the contributions of human error to system failure can be examined. Human error is a potential reason for an accident to occur in the first place, and also

TABLE 24. - A checklist for evaluating task error-likeliness

1. The cue or sign that tells the operator to begin each task and each activity in a task is simple and unambiguous:

   a. No inconsistencies, gaps, or misleading information that could result in errors of judgment.

   b. No competing activities that could interfere with perceiving the cue or with responding in a timely manner.

2. The cue or sign points to the correct task or activity only.

3. The task or activity is easy to do.

   a. No special problems in the scanning, anticipatory, or other perceptual requirements; in long-term or short-term memory requirements; in interpreting and decision-making requirements; or in manipulative requirements.

   b. No special problems with competing activities or past experience.

4. The completion cue or sign for the task or activity is simple and unambiguous.

   a. No misleading feedback to the operator.

   b. No special problems with competing activities.

5. The completion cue or sign for one activity in a task cannot be misinterpreted as signaling the completion of the entire task.

contributes to less than adequate recovery from accidents. The analysis procedure discussed in this section is particularly suitable for identifying the causes of human errors, whether they are characteristics of the plant and hardware or of the human himself. The results of the analysis suggests areas that can reduce the likelihood of human errors by such measures as focusing operator training sessions on identified hazards, providing input to safe operating procedures, and postulating appropriate design changes. This stage of the HRA requires little system safety analysis expertise beyond a detailed knowledge of the system, control configurations, and operating procedures.

The primary disadvantage of an HRA is that an adequate and effective analysis is relatively time-consuming. The technique also requires significant subjective judgement by the analyst which introduces uncertainty. Also, the technique requires more than a detailed knowledge of how the system functions. It requires the analyst to know how to operate equipment and components, how to monitor plant variables, and what changes in plant variables mean. This, however, was considered an advantage in the evaluation of safety methods performed for this study because the people who believe they should perform these methods, the mine safety officials, are already knowledgeable regarding this information.

Example of Analysis Procedure

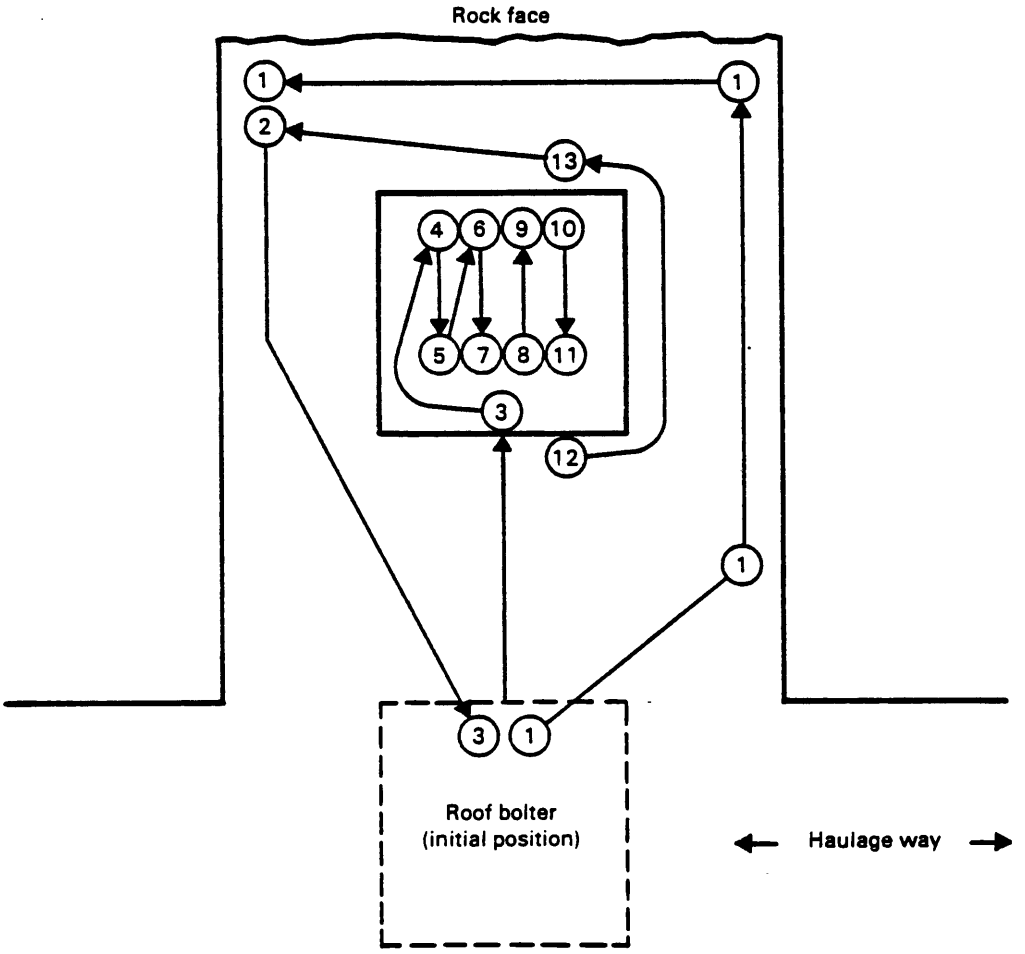
The example chosen for illustration of the HRA procedure is a roof bolting operation at an underground coal mine. The reader should recognize that HRA is applicable to all aspects of the mining operation. Only the analysis of the roof-bolting operation is presented because a complete HRA of a mining system is too lengthy to present in this manual. Roof-bolting is one of the most hazardous of all underground mining operations. The roof bolter is a rubber-tired vehicle used to drill holes and insert and tighten expansion-shell-anchor bolts into the roof, thus supporting the roof either through beam-strengthening (clamping thin layers into a thick layer) or hanging the weaker strata to a competent bed. Normally, drilling is accomplished with a rotary action using auger-type bits with tungsten carbide inserts. Dust resulting from drilling is collected through the bit and the hollow drill rod.

The first step of the HRA of the roof-bolting task is to describe the operation. A partial description is provided above. It is also recommended to perform link analysis on the operating procedure because this operation consists of several steps performed in a specific sequence. The first step of the link analysis is to describe the task procedure in the proper operating sequence and estimate the time requirements for each step in the procedure. This is done below.

(1) Check general roof conditions and check roof bolt spacings: 1.0-2.0 minutes
(2) Methane check: 0.5-1.0 minutes
(3) Maneuver to first drill hole, extend jacks: 0.2-0.4 minutes
(4) Place drill steel: 0.1-0.2 minutes
(5) Drill hole: 0.2-0.5 minutes/foot drill rate
(6) Add extension to drill steel (or change steel): 0.1-0.2 minutes
(7) Place steel aside: 0.05-0.1 minutes
(8) Lower drill boom, retract drill rods: 0.05-0.1 minutes
(9) Insert bolt and tighten: 0.20-0.50 minutes (without planks or straps)
(10) Place wrench aside: 0.05-0.1 minutes
(11) Retract stablizing jacks: 0.1-0.2 minutes
(12) Empty dust bin: 0.5-1 minute
(13) Mark off hole locations: 0.5-1 minute
(14) Repeat operations 2 through 12 for subsequent roof bolting.

Roof quality plays an important role in determining cycle times since the length of hole, hole spacing, drilling rate, and the necessity for planks, straps, or blocks as part of the roof support are governed by roof conditions.

Once the procedure has been described and time requirements have been estimated, the next step in link analysis is to draw a diagram showing where the operating steps occur. Arrows are drawn between these locations indicating the movements of the operator. A link analysis flow diagram for the roof bolting operation is shown in Figure 14. It can be seen that there is considerable mounting and dismounting of the roof bolting machine by the operator to perform some of the steps. This is one potential hazard,



Note: The legend for the numbered task symbols is shown in the text

FIGURE 14. - Link analysis flow diagram for the roof bolting operation

particularly in moist, humid, and slippery conditions. Another potential hazard is to omit the methane check or to perform it out of sequence, thus possibly allowing the methane concentration to build to explosive levels without being noticed by operators. Similarly, the steps for setting and retracting the stabilizing jacks may be omitted or delayed which could cause damage to the machine while drilling or when it is moved to a new location. Personnel may also be injured if the drill bit slips out of the drill hole because the jacks are not in place. A further potential sequencing problem could occur if the operator fails to check the hole spacings before drilling. Regulations require a maximum spacing of roof bolts (5 ft x 5 ft or less) and if this spacing is not met, the likelihood of roof collapse is increased in

addition to the civil penalties and fines that the mining company would be subject to if the proper spacing is not maintained. This essentially completes Step 1 of the HRA procedure as it applies to the roof bolting operation.

Step 2 of the analysis procedure is to describe the situational characteristics associated with the roof-bolting task. To do this, the analyst consults the checklist of performance shaping factors (see Table 22) and identifies those PSFs that could potentially affect the actions taken by operators. The analyst follows the task operating procedure and identifies the PSFs associated with each step in the task. For example, in Step 2 of the roof-bolting task procedure, the operator is required to check methane levels in the cut, prior to starting the drilling machine motor. It is possible that the operator might omit this step and start the motor in a high methane atmosphere and cause an explosion. The analyst identifies the potential causes of the operator forgetting or deliberately omitting the methane check. Some of the PSFs associated with this task error are shown in Table 25, supplemented by a brief explanation of why they were selected. Other PSFs are associated with this task step but are not shown due to the length of the explanation required. Table 25 is presented for illustration purposes only.

TABLE 25. - Examples of performance shaping factors that could cause a roof bolting machine operator to omit the methane check

TASK STEP - Methane Check Prior to Starting Machine

Potential PSFs

- Quality of environment - Uncomfortable temperature and humidity, potentially slippery conditions. This could cause the operator to deliberately omit the methane check because he must dismount the machine to do so.
- Availability/Adequacy of methane detectors - Operator may feel his perception of the methane levels is better than a potentially inaccurate or unreliable methane detection device.
- Job and task instructions - Inadequate procedures, warnings, and plant policies could affect this step.
- Interpretation - Possibly the operator performs the methane check and misinterprets the results.
- Frequency and repetitiveness - The operator may feel that since he has checked methane levels prior to drilling a previous hole a second check is not needed.
- Man-machine interface factors - Design of the methane detector may be inadequate which could lead to interpretation errors.

Once the PSFs associated with each step of the roof bolting task have been identified, the analyst continues to Step 3 of the analysis and describes the characteristics of the machine operators and the personnel who maintain the machines. The analyst should examine the characteristics of the personnel involved in order to determine if the demands placed on the operators by the task exceed the capabilities and limitations of the personnel. For example, methane checks are repetitive and frequent task steps. Examination of the machine operator characteristics may indicate that a particular operator has little or no patience for performing repetitive checks which may not yield any different results than previous checks. This is a common characteristic of humans and in this case it would only take one omitted methane check to seriously injure that operator. The analyst continues to compare the personnel characteristics with the PSFs to determine this type of information for each task and each step in the tasks.

Steps 4 and 5 of the HRA procedure together constitute a task analysis. Results of the task analysis are often combined on one table, as shown previously in Table 23. Step 4 consists of the descriptive portion of the task analysis and Step 5 is the analytical part. The objective of these two steps together is to identify error-likely situations and their potential causes. A completed task analyis for human error while checking methane levels prior to starting a roof bolting machine is shown in Table 26 for the reader to follow throughout the following illustration of the task analysis procedure.

As can be seen in Table 26, the step in the roof bolting task for the methane check is broken down into four smaller units of behavior, labeled 2A, 2B, 2C, and 2D. The procedures for these sub-tasks are described in column 3 of the table. Activity 2A is for the operator to dismount the roof bolting machine, acquire the methane detector, and advance to the rock face. There is no cue or sign for the operator to begin this activity. This is recorded in column 4. In column 5, the analyst places remarks concerning the performance shaping factors associated with the activity. The identified PSFs for sub-task 2A include the quality of the environment (often hot, humid, slippery, and dark conditions), perceptual requirements (the operator should know when not to expose himself to a loose roof), task speed (treacherous footing), and fatigue (over-tired operators are more likely to omit part of a task or commit an operating error). In addition, this column is used for recording personnel characteristics that may have an impact on task performance. Note that one operator is identified as one who lacks patience and takes unnecessary chances for the sake of increased speed at his tasks. Other examples of items of this nature include personal problems, medical conditions (such as back injuries, asthma, alcoholism, etc.), personal capabilities (such as physical strength, in-shape, out-of-shape, etc.) and mental capabilities (disciplined, expertise in some specific area, reasoning ability, etc.). This completes the descriptive part of the task analysis.

Next, the analyst begins the analytical portion of task analysis. The objective of this part of the analysis is to identify situations where human error is likely and their potential causes. Error-likely situations may arise

TABLE 26. - Example of a complete task analysis form

TASK: Roof Bolting — TASK BEHAVIORS — Page ____ of ____ Pages

Subtask: _____ Conditions: Wet, Humid, Slippery — Task Analyst: _____

Task or Step (1)	Instrument or Control (2)	Activity (3)	Cue for initiation or completion of activity (immediate or delayed) (4)	Remarks (5)	Task or Step (6)	Scanning, perceptual or anticipatory requirements (7)	Recall Requirements (LT = long-term ST = short-term # - initiating cue absent or poor) (8)	Interpreting Requirements (9)	Manipulative Problems (10)	Likely human errors (or other problem areas) (11)
(2) Methane check	Methane sensor and display gauge (fully self-contained)	2A. Operator dismounts roof bolting march	Completion of task Step 1 - Inspection of Roof and hole location markings	Muddy floor conditions, operator may elect to neglect Methane check altogether, excessive task speed, availability and adequacy of detectors, Operator A works too fast occassionally; error-prone	2A.	Repetitive task, cues for initiation of task are not obvious	NONE	NONE	NONE	Methane check not performed, either deliberate or otherwise
		2B. Check for mechanical zero, battery voltage	NONE	This step often neglected; operator rushed, poor conditions, poorly designed	2A.	Repetitive task	ST, although no initiating cue except for operator memory	Gauge reads methane %age in air directly; need good lighting	Gloves must be removed to manipulate switches, etc.	Inaccurate methane level reading; could cause explosion if reading is low or unnecessary shutdown if reading is high

Continued . . .

TABLE 26. - (continued)

Task or Step (1)	Instrument or Control (2)	Activity (3)	Cue for initiation or completion of activity (immediate or delayed) (4)	Remarks (5)	Task or Step (6)	Scanning, perceptual or anticipatory requirements (7)	Recall Requirements (LT = long-term ST = short-term # = initiating cue absent or poor) (8)	Interpreting Requirements (9)	Manipulative Problems (10)	Likely human errors (or other problem areas) (11)
		and electrical zero on detector		switches and gauges				and clear gauge face. Task speed may cause omission		
		2C. Energize detector	INITIATION: All checks in 2A are satisfactory	Simple operating procedure	2B.	NONE	ST	NONE	Gloves must be removed, ON switch sticks in humid conditions	NONE LIKELY
		2D. Read Methane level off gauge	Detector has red light which indicates the Methane level is ready to be read	Simple gauge, reads Methane level directly	2C.	Ready light is easily seen	LT, must remember from training sessions, although used every day	Operator reads gauge and compares with standards; hindered by poor conditions, task speed, distractions (noise)	NONE	Operator reads level before detector is ready, may misread level due to distractions

from equipment design features, methods of use, methods of training, and the skill levels of people in the system. The kinds of factors the analyst is looking for in each human action are grouped into four broad categories, as shown in columns 7, 8, 9, and 10 of Table 26. Column 7 is for scanning, perceptual, and anticipatory requirements. The analyst examines the number and kinds of gauges, dials, labels on switches, warning signs, and other items that convey information about the process to the operator. With this information the analyst can identify situations where the operator may omit a step or fail to detect a hardware failure, alarm, or other cue for the operator to begin a task. Recall requirements for the tasks are recorded in column 8. Recall requirements can be categorized into short-term memory and long-term memory requirements. The analyst examines the thinking processes that operators must use to perform their tasks and identifies whether the task procedure is one that is considered by the operator frequently (possibly daily or weekly) or infrequently. Emergency evacuation procedures are an example of a long-term memory item. Emergency procedures are not frequently considered by workers. Obviously it is not economical to practice emergency evacuation procedures at a mine on a relatively frequent basis. Therefore, other methods for training workers to escape from an emergency situation must be utilized in addition to infrequent practice evacuations. Such measures as emergency, battery-powered lighting and posted, well-lit escape routes are often used at mines and other operating systems. Interpreting requirements are recorded in column 9. For this column, the analyst examines the workers' responses to the cues for him to begin or complete a task. Often workers are required to analyze a situation and react accordingly, gathering information from indicators, alarms, gauges, and his environment. As can be seen from the example in Table 26, environmental variables can play an an important role in interpreting requirements at mines where conditions are often wet and slippery. Excessive task speed is also a likely cause of interpretive errors. Manipulative problems are recorded in column 10. These are problems regarding the physical performance of the task. In the example problem, potential manipulative problems related to the wearing of gloves are identified. These items are most often related to the design of the control mechanisms, plant hardware, and work stations. A further example might be a toggle switch in which the up position means OFF and the down position means ON, exactly the opposite of what is expected in this country. This completes the identification of factors that could cause error-likely situations. The reader should recognize that this process is repeated for every task and operation at the mine requiring human interaction.

Error-likely situations are identified and recorded in column 11 of the task analysis form. The identification of ELSs is facilitated by the use of a checklist of questions that the analyst asks himself to answer. This checklist was shown previously in Table 24. The analyst begins at the top of the list and evaluates each question in regard to the performance of the tasks under analysis. For example, an ELS was identified in Task 2B, the check-out of the methane detector required before its actual use. The analyst inspected the checklist and identified items that were inconsistent with the statements contained therein. The specific statement that the actual situation conflicts with is Item 3a of Table 24, "No special problems in scanning, anticipatory or other perceptual requirements; in interpreting and decision-making requirements;

or in manipulative requirements." More specifically, the actual situation in the mine has many distractions, normally poor environmental conditions (muddy; could result in warning signs and equipment operating stamps being rendered unreadable), and there is often significant economic incentive for workers to perform their tasks as quickly as possible. Any of these situations can result in a task performance error which in this case is an error of omission of a step in a task. The analyst continues evaluating each task described in columns 1 to 5 of the task analysis table, consulting the checklist for each task step, until he has examined every task and step in a task for ELSs. This completes the discussion of the example of the task analysis procedure. The results can be used to prepare a checklist of ELSs for the safety official to use in planning a hazard reduction program, communicating the results to management, and identifying areas for safety improvements.

The analyst's next step is to use the information obtained thus far to postualte measures that could eliminate or mitigate specific ELSs. In the stated example, one of the identified ELSs is where a worker reads an inaccurate methane level due to an improperly functioning detector (Activity 2B). The effects of such a reading can potentially cause an explosion and multiple deaths if the detector gauge reads a lower methane concentration than is actually present or can cause an unnecessary shutdown of operations if the actual methane level is lower than the detector is indicating. The potential causes of this ELS are a lack of cues for initiation and performance of the detector check-out test sequence, the fact that this procedure is repeated many times every day, excessive task speed, and potentially poor environmental conditions. In consideration of this information, possible measures for mitigating this ELS include: (1) focusing worker training on the need for proper testing procedures for methane detectors, and (2) permanently attaching a sign in a conspicuous location on each methane detector that indicates the testing and operating procedures. Little can be done to eliminate the excessive task speed, repetitiveness, and poor environmental conditions, beyond informing miners of the hazards. However, if a particular worker refuses to follow procedures or continues to work excessively fast after repeated warnings, he could be removed from responsibility for this task and thereby eliminate his contribution to the ELS. The analyst continues down the task analysis table and suggests possible measures to eliminate or correct potential ELSs inherent in each task and step of mining operations. This completes the discussion of the example problem.

Computer Adaptability

Much of the HRA procedure follows a structured and iterative format. Task analysis, which is the heart of the qualitative portions of HRA, follows such a format. It is believed that task analysis could be adapted to a user-interactive computer program for this reason. Also, the checklist of performance shaping factors (see Table 22) and the checklist for evaluating task error-likeliness (see Table 24) can be input to a computer memory and recalled when the analyst desires. There is no better way of gathering human reliability information than to perform the tasks under analysis personally. Thus, procedures such as link analysis and the task of gathering and recording system description information may best be performed externally to the

computer. Furthermore, the computer has the capability to display only about one page of information at a time. It is desirable in the first three steps of the analysis to be able to quickly review several pages of information without losing the train-of-thought. This is facilitated by having the information on separate pages that can be seen simultaneously by the analyst. Thus, at least initially, it is recommended that only portions of the HRA procedure described in this section be adapted to the computer.

A conceptual user-interactive HRA computer program was developed as part of this study. As discussed above, a good deal of work is required before the analyst can sit down and initiate the computerized analysis. Link analysis is believed to be not readily adaptable to the computer, due to the drawing required, although graphics capabilities of current computer systems are improving. The analyst may wish to record the significant results from the link analysis in the computer memory to be recalled later in the analysis. For example, link analysis is particularly useful for identifying sequential errors (omitting or performing steps in a task in the wrong sequence). If the analyst identifies a likely situation where a sequential error could occur, this situation can be described and input to the computer memory with appropriate references to the link analysis flow diagram where the situation is described. When the analyst is performing the task analysis, the sequential errors in the computer memory are available as the analyst desires.

The conceptual HRA computer program is a two-stage approach. A flow chart for this conceptual program is shown in Figure 15. Stage 1 is essentially a user-interactive aid that facilitates performance of the task analysis (see Steps 4 and 5 of the HRA procedure). The computer program is envisioned to contain a large set of questions corresponding to the columns of the task analysis format shown in Table 23. The computer will display these questions in the same logical format shown in the table. The analyst will then type the answers to the stated questions into the computer processor. The computer then stores the information in appropriate locations in its memory. In essence, the computer program serves as a guide to the analysis procedure and as a permanent record of the task analysis results. The computer can be programmed to print out the results in a format that might be useful to mine safety officials as a checklist of potential causes of human errors. This checklist is envisioned to contain the error-likely situations at the mine and the potential performance shaping factors and human characteristics that could produce ELSs. This checklist is useful for identifying changes to the mining system that can reduce the likelihood and consequences of human errors. It can also be used to convey results of the analysis to mine management.

A further feature of the conceptual HRA computer program is the possibility of inputting several checklists to the computer memory. These checklists facilitate performance of the HRA by reducing the large checklists and statements on the checklists to a computer-useable form. In other words, the statements on the checklists will be indexed to allow the analyst to simply input an index number to the computer memory rather than the entire statement. The computer program will be able to remember which statement goes with each index and when displaying or printing results would search for the appropriate index and output the statement associated with that index. This

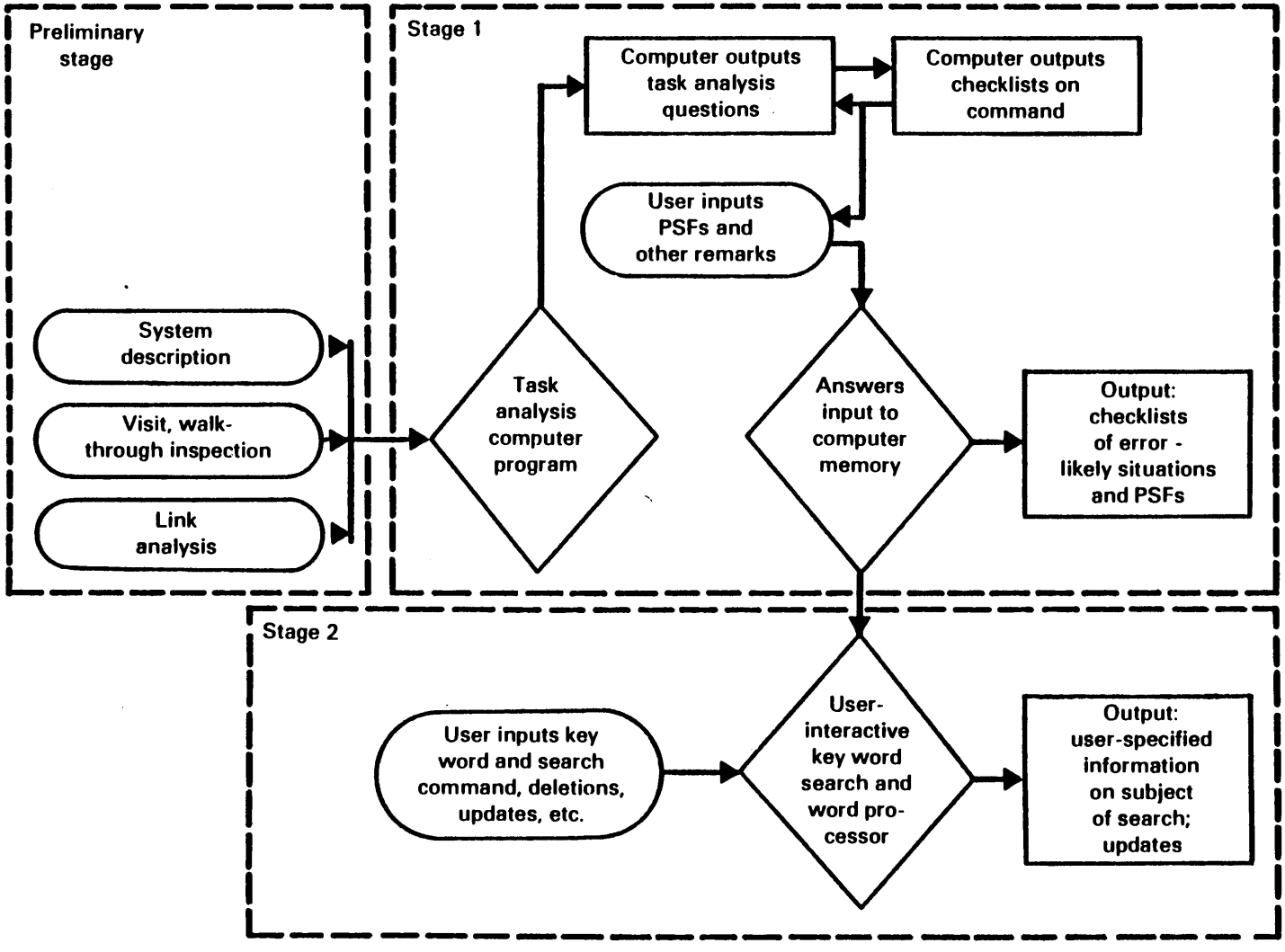


FIGURE 15. - Conceptual flow chart for a computerized HRA

scheme could be applied to the checklist of performance shaping factors (used in Steps 2, 4, and 5), and the checklist for evaluating task error-likeliness (used in Step 5). The latter checklist could be programmed directly into the computer software and used as a guide for performing the analytical part of the task analysis. The user-interactive computer software can be programmed to display these statements to prompt a response from the analyst. The analyst inputs the appropriate index for the PSFs associated with the task that could potentially contribute to an error-likely situation, and the computer stores this information in memory. The analyst can also add remarks or other findings as narrative statements where appropriate, such as when an adverse personal characteristic of a specific worker is identified. This completes the discussion of Stage 1 of the conceptual computer program.

Stage 2 of the conceptual HRA computer program is envisioned to contain key-word search and word processing capabilities. Since mines are constantly changing and expanding, the initial HRA performed on a mine is likely to become outdated in a short period of time. In addition, mining equipment is revised periodically by manufacturers to incorporate state-of-the-art features that are not present on older models. Therefore, the conceptual HRA computer program is envisioned to include capabilities that can update, revise, and modify the initial analysis when and where it is appropriate. To illustrate this, assume that an initial HRA determined that use of flame safety lamps to detect methane levels contributes to many error-likely situations. The safety official and mine management evaluated this situation and decided to purchase state-of-the-art methane detectors to reduce the likelihood of human error in this situation. To update the computerized HRA, the analyst simply locates tasks and task steps in which methane detectors are used by utilizing the key-word search capabilities of the computer. He then uses the word processing capabilities of the computer to delete the old information and type in the updated information. The reader should recognize that this process is significantly more efficient than if the analyst were to search the large amount of paperwork that can result from a paper-type HRA study.

Estimated Costs of Implementation

Two cost estimates are developed and presented in this section; 1) costs for implementing a paper-type HRA study and 2) costs for a computerized HRA study. The costs for implementing an HRA paper-study are dominated by the costs of labor. It is estimated that a detailed qualitative HRA of a mining system would require about 2.0 man-years of safety staff labor. Assuming the safety staff is paid $15.00/hr., and including overheads, benefits, taxes, and uncertainty (unit cost estimates are developed in the final report for this study and the bases and assumptions will not be repeated here), total labor costs are estimated to be in the range of $90,000 to $120,000. The annual costs for updating and revising the analysis is estimated to require about 3 to 4 man-months/yr. The total annual costs for this activity are estimated to be about $10,000 to $15,000/yr.

The estimated costs for implementing a computerized HRA safety program includes capital and installation costs for the computer hardware in addition to the staff labor costs. Capital and installation costs for an adquate

computer system are estimated to be about $5,000, including delivery and supplies (see final report for a survey of available microcomputer systems). Annual maintenance costs are assumed to be 10% per year of the initial purchase price. Also included in the costs for implementing this computer program are the costs for the safety staff to attend week-long short courses on computer training and safety analysis training. These costs were developed in the final report prepared for this study and will not be repeated here. The total fixed and operating costs are summarized below:

FIXED COSTS

Computer system purchase and installation	$ 5,000
Short course attendance and expenses	$ 9,000-12,000
Analyst's fully burdened labor costs	
Initiate program	$ 10,000-15,000
Perform analysis	$ 90,000-120,00
TOTAL	$114,000-152,000

OPERATING COSTS (after first year)

Computer system maintenance and supplies	$ 500/yr
Analyst's fully burdened labor costs	$ 10,000-15,000/yr
TOTAL	$ 10,500-15,500/yr

The reader should recognize that the above estimated costs do not contain the costs for development of the computer software. It is difficult to estimate these costs accurately. Further, it is not known whether these costs will be borne by the government or the mining industry. Therefore, software development costs are in addition to the estimated costs for implementing the HRA safety program shown above. It should also be noted that since safety staff labor charges are included in the above estimates and since the HRA safety program would replace some of the safety staff's current duties, the actual additional costs for implementing the HRA program are lower.

REFERENCES

1. Cybulskis, P., et al. 1981. Review of Systems Interaction Methodologies, NUREG/CR-1896, Battelle Columbus Laboratories, Columbus, Ohio.

2. Hammer, W. 1972. Handbook of System and Product Safety. Prentice-Hall, Inc. Englewood Cliffs, New Jersey.

3. Johnson, W.G. 1973. The Management Oversight and Risk Tree - MORT, SAN 821-2, U.S. Atomic Energy Commission, Washington, D.C.

4. Jordan, W.E. 1972. "Failure Modes, Effects, and Criticality Analyses" in Proceedings of Annual Reliability and Maintainability Symposium, San Francisco 1972, Institute of Electrical and Electronic Engineers, New York, New York.

5. Knox, N.W. and Eicher, R.W. 1976. MORT User's Manual, ERDA-76-45-4, SSDC-4, Aerojet Nuclear Co., Idaho Falls, Idaho.

6. Lambert, H.E. 1975. Fault Trees for Decision-Making in Systems Analysis, UCRL-51829, Lawrence Livermore Laboratory, Livermore, California.

7. McCormick, E.J. 1975. Human Factors in Engineering and Design, 4th ed., McGraw-Hill Co., New York, New York.

8. Nertney, R.J. and Bullock, M.G. 1976. Human Factors in Design, ERDA-76-45-2, SSDC-2, Aerojet Nuclear Company, Idaho Falls, Idaho.

9. Swain, A.D., and Guttman, H.E. 1982. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, Sandia National Laboratories, Albuquerque, New Mexico.

10. U.S. Department of Defense 1974 Military Standard, Human Engineering Design Criteria for Military Systems, Equipment, and Facilities, MIL-STD-1472B, Washington, D.C.