DOE--76-45/4-Rev.3

DE93 007061

MORT User's Manual

For Use With the Management Oversight and Risk Tree Analytical Logic Diagram

Norm W. Knox
Robert W. Eicher

Published February 1992

System Safety Development Center

Idaho National Engineering Laboratory
EG&G Idaho, Inc.
Idaho Falls, Idaho 83415

Prepared for the
U.S. Department of Energy
Deputy Assistant Secretary for Safety and Quality Assurance

DISCLAIMER

ABSTRACT

This report contains the User's Manual for MORT (Management Oversight and Risk Tree), a logic diagram in the form of a "work sheet" that illustrates a long series of interrelated questions. MORT is a comprehensive analytical procedure that provides a disciplined method for determining the causes and contributing factors of major accidents. Alternatively, it serves as a tool to evaluate the quality of an existing system. While similar in many respects to fault tree analysis, MORT is more generalized and presents over 1,500 specific elements of an ideal "universal" management program for optimizing environment, safety and health, and other programs.

This User's Manual is intended to be used with the MORT diagram dated February 1992.

ACKNOWLEDGMENTS

We gratefully acknowledge the many helpful suggestions we received from our colleagues of the System Safety Development Center during the preparation of this manual.

The source document for this "condensation" was the MORT text, "MORT-The Management Oversight and Risk Tree" (SAN 821-2), authored by W. G. (Bill) Johnson.

INTRODUCTION TO REVISION 3

Revision 3 is designed primarily to add conceptual material developed by S. B. Haber and D. P. Thurmond in "A Preliminary Identification of the Human Performance Issues Within the Department of Energy," Task 1 Report prepared for the U.S. Department of Energy (1989) and applied in "Human Performance Appraisal" in June 1990. Concurrently, other minor revisions to the User's Manual were performed.

MORT text cross-references to W. G. Johnson's 1980 "MORT Safety Assurance System" are not being done at this time since this text is under revision. The User's Manual will be cross-referenced to the revised "MORT Safety Assurance Systems" when these revisions are complete.

CONTENTS

FIGURES

PART I

A. PURPOSE

This document was prepared for a two-fold purpose:

1. Primarily, it is intended to be a practical working tool. It is designed to help the novice Management Oversight and Risk Tree (MORT) practitioner achieve quicker, deeper insight and understanding of the MORT safety program concepts by: (a) providing a brief explanation of the related rationale supporting the word statement given in a specific event "box" of the MORT logic diagram and (b) listing page references to detailed explanations of the original MORT text, "MORT — The Management Oversight and Risk Tree," published in 1973 as ERDA publication SAN 821-2.*

2. Additionally, it is intended to serve as an information document directed to system safety professionals, program managers, and higher level management with responsibility for accident investigation or program evaluation. It seeks to explain simply the MORT "programmatic" concepts and "analytical" methodology, and to inform those people that MORT is available for immediate use: (a) in investigating the elements of management oversight and risk relative to an accident that has happened; or (b) in the evaluation of an existing program to determine the likelihood that a significant accident is about to happen.

While this document is generally applicable to any issue of the MORT logic diagram, it is keyed or indexed specifically to the MORT logic diagram revision dated April 1986.

B. BACKGROUND

Prior to 1970, the Energy Research and Development Administration (ERDA) had no system safety program as such. During that time, ERDA (the predecessor to the Department of Energy [DOE]) Division of Safety, Standards, and Compliance (SSC), funded a study prepared by W. G. (Bill) Johnson, who had recently retired as General Manager of the National Safety Council.

The argument for the study and the planned objectives, paraphrasing the words of the original proposal, was as follows:

> "...Emerging concepts of systems analysis, accident causation, human factors, error reduction, and measurement of safety performance strongly suggest the practicality of developing a higher order of control over hazards (than now exists)."
>
> "The formulation of an ideal system appears to be a valuable precondition for knowing what information to seek after an accident and what aspects of performance (of the accident-related safety system) to seek to measure."

*The original text has since been revised and published as "MORT Safety Assurance Systems," W. G. Johnson, Marcel Dekker (1980).

Johnson advanced the idea that application of controls and resources made by managements of occupational safety programs could be categorized into five levels:

1. Less than minimal compliance with regulations and codes.

2. Minimal compliance with regulations and codes.

3. Application of manuals and standards.

4. Advanced safety programs exemplified by those currently found in leading industrial companies and in DOE.

5. An as-yet-nonexistent, superlative safety program synthesized by combining the "system safety" concepts pioneered by the military and aerospace industry with the best occupational safety practices and factoring in the newer concepts of the behavioral, organizational, and analytical sciences.

In Johnson's view, there were sufficient data to suggest that progression from one one level of safety program to the next better level might result in an order of magnitude reduction in the annual rate of disastrous accidents experienced by a specific enterprise. Accordingly, the goal set for the conceptualized fifth level system, to be developed by the ERDA study, was an order of magnitude improvement in the already exemplary ERDA safety record.

The study was titled "Development of Systems Criteria for Accident Reporting and Analysis and for the Measurement of Safety Performance."

In 1971 the first generation MORT text was published and the study moved to the next logical phase of pilot use at an actual ERDA contract activity. The Idaho National Engineering Laboratory (INEL), then known as the National Reactor Testing Station, was chosen primarily because the prime operating contractor, Aerojet Nuclear Company (ANC), then known as the Idaho Nuclear Corporation, had a well-established safety program and additionally was developing and using "system safety" techniques patterned after methodologies pioneered by National Space and Aeronautics Administeation (NASA) and Department of Defense (DOD).

The first generation MORT text introduced four key innovative features basic to the MORT program:

1. An analytical "logic tree" or diagram from which MORT derives its name, "Management Oversight and Risk Tree." This diagram arranges safety program elements in an orderly, coherent, and logical manner.

2. Schematic representation of a dynamic idealized or "universal" safety system model by using Fault Tree Analysis methodology.

3. Methodology for analyzing a specific safety program through a process of evaluating the adequacy of implementation of the individual safety system elements.

4. A collection of philosophical statements and general advice relative to the application of the MORT system safety concepts and listed criteria by which to make an assessment of the affectivity of their application.

A major MORT premise is that the MORT safety system is congruous (i.e., harmonious) with a goal-oriented, high performance, complex management system.

Working under the direction of a Steering Committee composed of senior ANC line and staff managers, a MORT development team was formed consisting of Johnson and three ANC employees, Dr. Robert Nertney, Jack Clark, and Jack Ford. During the next two years, MORT concepts were subjected to trial use under actual operational conditions. Additional systems concepts were developed and tested.

In 1973, the second generation MORT text was published. It included additional safety systems developed and refined by ANC and the Idaho Field Office of the ERDA, and incorporated the result of an intensive effort of collecting and organizing the best safety elements from different programs throughout the world.

It should be emphasized that MORT does not represent new and untried methodology. MORT does represent the synthesis of those best safety program elements and concepts with the state-of-the-art techniques of safety program analysis and evaluation.

Careful review of the results of numerous studies conducted over nearly four years, coupled with the ANC trial application results, led ERDA-SSC to embark upon a full-scale orientation and training program of ERDA and ERDA contractor personnel throughout all of the ERDA. In August 1974, the System Safety Development Center (SSDC) was established at Aerojet under the joint sponsorship of ERDA-SSC and ANC. In October 1976, EG&G Idaho was awarded the prime operating contract at the INEL, including the management role of the SSDC.

Staffing and responsibility for the MORT orientation and training program was assigned to the SSDC. The formal implementation plan adopted consisted of four points:

1. MORT Five-Day Training Seminars
2. MORT Management Briefings
3. Mini-MORT Seminars
4. Safety Program Improvement Projects (SPIPs).

To date, many seminars have been conducted, both at the INEL and at other DOE facility locations. The continued activities of the SSDC are presently projected to a 10 year program of further MORT development. This includes presentation of MORT orientation and training seminars for DOE, DOE contractors, and NRC with seminar locations spotted throughout the U.S. In addition, several MORT-based workshops have been developed. These workshops are also being held throughout the country to certify "trained investigators" as prescribed by DOE Orders as well as other training.

C. INTRODUCTION

The MORT principle has two meanings:

1. A total safety program concept (viewed as a specialized management subsystem) focused upon programmatic control of industrial safety hazards, and

2. The actual logic diagram which displays the structured set of interrelated safety program elements and concepts comprising the ideal management program model called MORT. This universal logic diagram becomes a master "work sheet" for use in analyzing a specific accident or alternatively for use in the evaluation and appraisal of an existing safety program for accident/incident potential.

As an ideal management program, MORT was designed to include the following:

1. Prevent management oversights, errors, and omissions.

2. Result in identification, assessment, and referral of residual risks to proper management levels for appropriate action.

3. Optimize allocation of resources available to the program and to individual hazard control effort.

The many state-of-the-art safety system concepts and safety program elements synthesized to produce "programmatic MORT" are presented in considerable detail in the second generation MORT text. Integrated into the MORT program model are the best features of exemplary safety programs found in the U.S., i.e., management implementation, hazard analysis, human factors analysis, work processes, monitoring, information systems, and organization systems and services.

Innovative concepts, such as the sequential role of unwanted energy flow, barriers to energy transfer, error, change, and risk, are systematically related along with the most current concepts of the behavioral, organizational, and analytical sciences.

Translated to "analytical MORT" (the MORT logic diagram), these features of "programmatic MORT" accumulate to over 1,500 "basic events" (i.e., causative problems or preventive measures related to an ideal safety system). These, in turn, underlie nearly 100 different generic problems identified in successively broader areas of management and accident prevention. Incorporated into the above listed concepts are some 50-70 "new ideas." (The actual number is highly subjective, depending upon a person's background and experience.) The way in which the MORT concept (programmatic MORT) is schematically represented by a logic diagram (analytical MORT) is shown in Figure I.

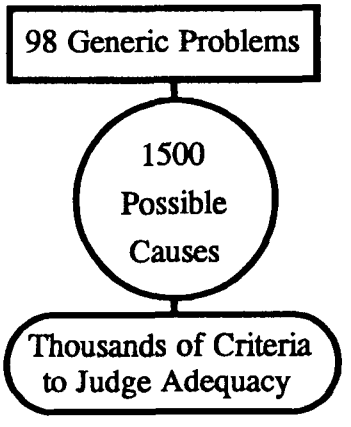
MORT is simply a diagram which arranges safety program elements in an orderly and logical manner. It presents a schematic representation of a dynamic, idealized (universal) safety system model using Fault Tree Analysis methodology.

MORT structures the largely unstructured safety literature and current best safety practices into three levels of relationships:

a. Generic Events (Problems)

b. Basic Events (Causes)

c. Criteria (Judgment rationale from the MORT text)

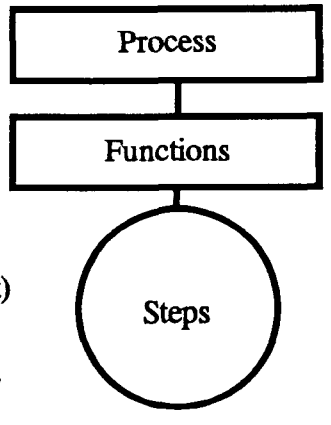


MORT makes explicit:

a. The functions necessary to complete a process.

b. The steps to fulfill a function.

c. Judgment criteria (from the MORT text) by which to judge when a step is well done or is "less than adequate" (LTA).



It provides relatively simple decision points in an accident analysis or safety system evaluation and enables an analyst or evaluator to detect omissions, oversights, or defects.

Figure 1. Schematic of the MORT Process

Fundamental to a successful accident investigation or safety program evaluation is the assignment by higher management of technically qualified, competent, safety-motivated personnel to participate in the investigation. Even so, experience, to date, indicate that a well qualified person (but novice MORT practitioner), armed with only the MORT text and the MORT "work sheet" with its collection of symbols and terse statements, will likely find the initial encounter with the MORT proposition somewhat overwhelming.

This User's Manual was prepared to help the MORT practitioner develop a quick familiarity with the MORT process.

In the remaining sections of Part I, the reader is introduced to the basic concepts of system analysis and the role of change. Fault Tree Analysis (FTA), from which the more generalized MORT analytical procedure is derived, is briefly discussed in the Appendix.

In Part II the actual User's Manual plan is presented. The structured relationship of each generic causative problem or preventive measure to the idealized safety system is explained and fitted into the event indexing scheme adopted for the MORT diagram. As each major branch and its principal subbranches are listed, occasionally commentary relative to the safety program concept or best practice safety program element involved is made. With this additional insight, more probing questions can now be asked by the MORT analyst.

The analyst, with enhanced understanding, is able to make a better judgment whether the specific safety program element being examined is "adequate" or "less than adequate" (LTA). The analyst, as previously mentioned, is encouraged to use the MORT diagram as a master "work sheet," marking the individual program elements. Suggestions for working with the MORT analysis are made.

The cross-reference tabulation to the index code used on the MORT diagram is presented in "indexed" fashion for easy location. Page number references back to the MORT text are provided in the parentheses that follow the indexed event tabulation.

Once completed, the MORT analytical "work sheet" provides an all-important visibility to the accident investigation process or to the safety program evaluation. The analyst is able to review his findings, present them meaningfully to others, alter or revise the analysis as additional facts warrant, and conveniently document the total effect for later use.

In summary, the objective of the User's Manual (Part II in particular) is to provide the MORT practitioner with quick-look additional insight to the "programmatic MORT" concepts behind the statement in the MORT diagram event symbol. With this insight, it is hoped that facility in the use of the MORT diagram as an analytical work sheet to analyze a specific accident or safety program will be more quickly obtained.

D. SYSTEM SAFETY ANALYSIS VERSUS THE SAFETY SYSTEM PROGRAM

The MORT logic diagram as previously stated is an idealized safety system model based upon the fault tree method of system safety analysis. To understand what is meant by system safety analysis, we must first understand what is meant by system. Many words can be (and have been) written to explain the concept. We will simply state it is an orderly arrangement of

interrelated components that act and interact to perform some task or function in a particular environment and within a particular time period. We must include people, who are the prime intelligence factor that initiates the system and communication (i.e., information flow), which is the prime factor that makes the system function.

A system is a dynamic entity that changes with time. In a "perfect" system, all components function in a manner that contributes to or complements the task achievement. In an imperfect system, some "fault" exists. A fault then is any factor not complimentary to the task achievement. (System effectiveness is a measure of the degree to which the end goal is accomplished without unplanned deviations from the planned course of tasks or functions.)

System analysis is a directed process for the orderly acquisition and review of specific information pertinent to a given system. Its purpose is to provide the basis for informed management decision.

The goal of a safety system or program is to produce a safe system; i.e., a system in which the likelihood of occurrence of all identifiable hazardous events is maintained at an acceptable level. A safety system or program is a formal approach to eliminate or control hazardous events through engineering, design, education, management policy, and supervisory control of conditions (environment) and practices. MORT system safety analysis is one method that can be used to evaluate the success of a safety program.

E. THE ROLES OF CHANGE ANALYSIS AND THE ENERGY BARRIER CONCEPT

Within the MORT system, an incident is defined as Barrier-Control inadequacy or a failure without consequence. An accident is defined as unwanted flow of energy or environmental condition that results in adverse consequences.

MORT suggests that an accident is usually multifactorial in nature. It occurs because of lack of adequate barriers and/or controls upon the unwanted energy transfer associated with the incident. It is usually preceded by initiating sequences of planning errors and operational errors that produce failures to adjust to changes in human factors or environmental factors. The failure to adjust satisfactorily leads directly to unsafe conditions and unsafe acts that arise out of the risk associated with that activity. The unsafe conditions and unsafe acts, in turn, provoke the flow of unwanted energy.

MORT was designed to use as an investigative tool that focus' upon the many factors contributing to an incident/accident. It accomplishes this by means of a meticulous trace of the unwanted energy sources, along with consideration of the adequacy of the barriers provided. As the analysis proceeds, MORT is ready to alert to any system changes, both planned and unplanned. When change is detected, MORT strongly suggests the need for detailed change analysis.

The practice of change analysis gives the analyst the ability to determine whether (1) changes are needed in a stable operational system, or (2) a changing operational system requires safety-related counterchanges.

In the first instance, many examples can be found of systems where the commonly used indicators and guidelines (accidents/injuries per man-hour, etc.) give indication of an acceptable safety program; however, the application of quite simple risk projection techniques reveals a high probability of a severe consequence accident.

In the second instance, the need for safety counterchanges is related to the simple fact that any real-life operational system is constantly experiencing changes in personnel, procedure systems, and equipment. Again, many examples can be found in accident investigation literature of such changes leading directly to accidents and incidents.

Implicit in consideration of change and its potential consequence is the concept of defined risk acceptance at the appropriate management level (without assumption of undefined risk because of oversights and omissions). Application of elementary principles of good business management point to the need for formal change analysis and control methods. These management practices will better define the risk, focus on needed safety counterchanges, and lead to an informed decision by the cognizant management level on whether or not to accept new change-related risks.

MORT is, therefore, designed to investigate accidents and incidents and to evaluate safety programs for potential accident/incident situations. Two of the many basic MORT concepts are the analysis of change and the evaluation of the adequacy of energy barriers relative to persons or objects in the energy channel.

PART II

A. GENERAL FEATURES OF THE MORT EVENT TREE

Figure 2 summarizes the logical arrangement adopted for depicting the generic events that comprise the TREE Top of the MORT diagram.

The construction layout of the MORT tree depicts three main "branches" ordered with Specific and Management (S/M), Oversights and Omissions on the left and Assumed Risks (R) on the right. The MORT technique requires events in the Assumed Risk branch to be events transferred there from the Oversights and Omissions branch. R factors are defined as only those risks that have been analyzed and accepted by the proper level of management; unanalyzed or unknown risks are not considered to be Assumed Risks.

Development of the two main branches comprising Oversights and Omissions is ordered with Specific Control Factors (S) on the left and the more general Management System Factors (M) on the right.

M factors are shown separate from the process that produced the specific adverse event for two reasons:

(1) Depiction of the existing management systems will suggest related background aspects of the specific accident that should be closely examined, and

(2) The specific event may, in turn, suggest certain aspects of the management systems that may be LTA.

In general, the further development of the S branch is keyed to time as well as process. Left to right is earlier to later and bottom to top of the tree shows causal sequence progress from basic detailed causes to generic causes. Specific rules of construction for extending the MORT diagram tree are given in the Appendix.

The key to understanding "programmatic" MORT is a close element-by-element examination of the MORT diagram. The diagram branches, in large part, are self-explanatory. Each element of the diagram branch presents a relatively simple question. One starts at the diagram top with the actual losses resulting from an accident or the potential loss if the diagram is being used to evaluate an existing safety program. Each of the three main factors (branches) is considered in turn. Detailed consideration of the S branch is accomplished by reasoning backward in time through several sequences of contributing factors. The analysis ends when the question posed by the circled statement is answered yes/no.

Obviously, some factors (branches) will be more relevant than others. On the other hand, the user should know there is some planned redundancy in the MORT diagram. A higher degree of hazard protection is attained when a hazard may be identified and connected at two or more places. It is better to ask the right question twice than to fail to ask it at all.

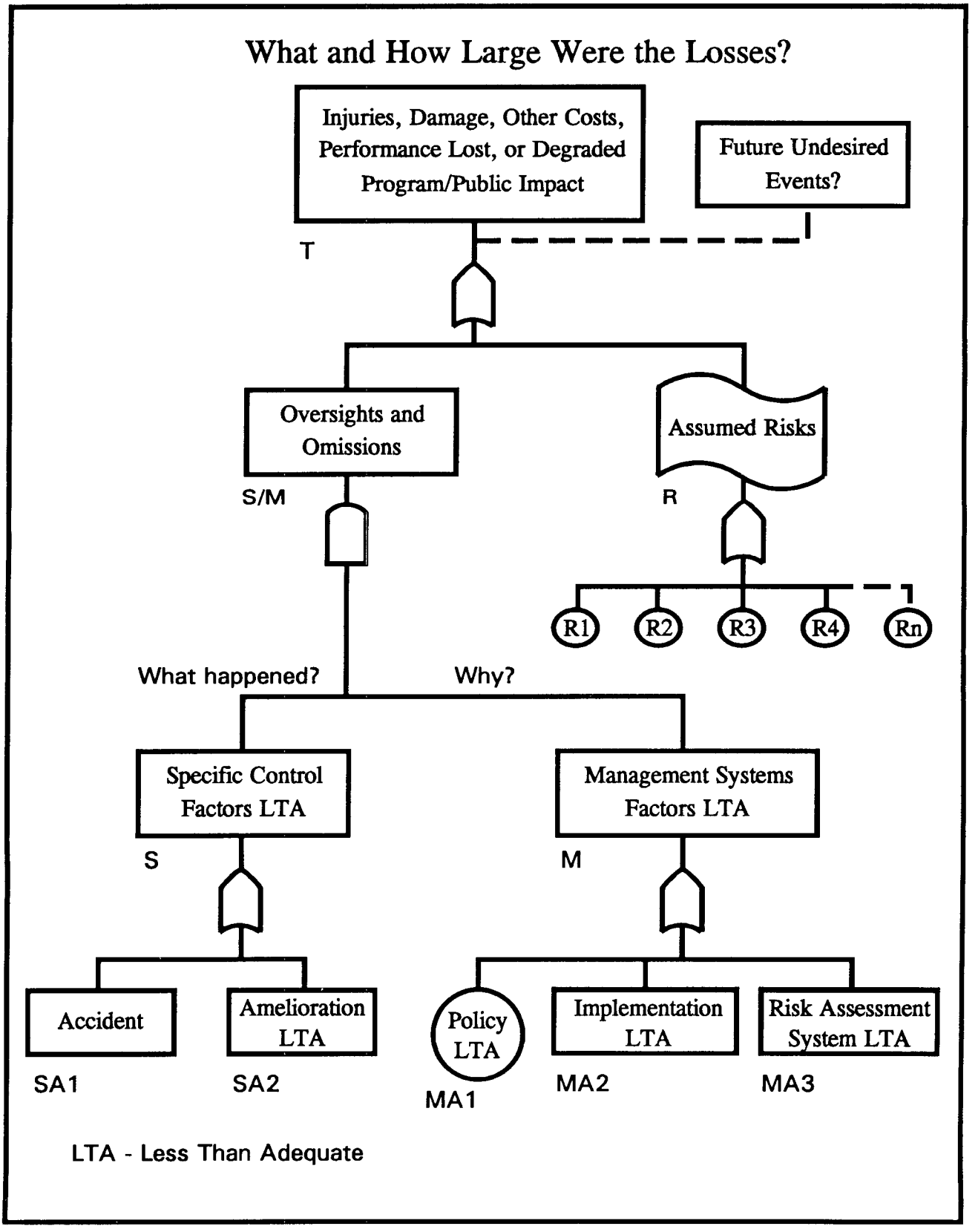


Figure 2. MORT Top Events

B. WORKING WITH THE MORT ANALYSIS

Repeated practice and experience with the MORT diagram are necessary before good dexterity and skill in its application are acquired. The novice should test the method on an actual accident. While many subsections of the MORT diagram may not apply to a specific accident, the analyst probing the accident for its probable cause(s) will be surprised at the number of beneficial subsections (branches) that are (as indicated by the name of the method) overlooked by management.

It is best to assume that all the boxes are colored blue. Let the color blue require of you more information before judgment can be made. This is where the questioning begins. If the questioning reveals that certain elements on the diagram indicates a deficiency, the element should be colored red. Those elements that appear adequate as indicated by your investigative technique are colored green. Those elements where adequate information is not available to make the above two judgments should remain (colored) blue. Those elements that truly do not apply to your search are crossed ("x'd") off with a black pen. Your investigation is complete when you have completed this process.

From experience with the MORT diagram, the following four suggestions can be given:

1. The MORT analytic diagram works best if it is used as a working paper. Pertinent facts about an accident or problem may be noted in margins at appropriate places. Informality is a key - the diagram will take care of the discipline. MORT is a screening guide and a working tool, not the finished report. Writing the report is a separate process. MORT is structured to facilitate analysis. It helps avoid personal hobbies, bias, or the tunnel vision that commonly results from pet theories of accident causation.

2. Commonly, the first reading of an accident report prepared by persons not using MORT leaves the impression that the documentation of what happened is complete. But on second reading, if one uses the MORT diagram as a supplementary aid, the gaps in information about what happened are readily revealed. Questions about why it could have happened begin to emerge.

3. A slower, more disciplined trip through the diagram is then in order. It is usually necessary to trace unwanted energy flow meticulously on a separate sheet, and then examine the nature of possible barriers step-by-step. If a situation emerges that is not covered in any of the MORT elements, the analyst can draw in an additional section using the construction methods and symbols described in the Appendix.

4. The distinction between S factors and M factors should be kept in mind at all times. The specific event associated with the actual incident/accident sequence of the Specific Control Factors branch will often have its counterpart in the general Management System Factors branch. The analyst must focus his thinking upon the accident process when evaluating the S branch. When evaluating the M branch, he must expand his thinking to the "global" or total management system concept.

C. PLAN OF THE USER'S MANUAL

The judgment used by the analyst to determine whether a specific event of a MORT diagram is "satisfactory" or "LTA" is partly subjective. The decision depends upon the selection, application, and evaluation of related criteria. An important function of MORT is to greatly reduce subjective judgments, personal bias, etc.

The MORT text (SAN 821-2) collected, organized, and commented upon the best concepts and practices found in the largely unstructured current safety literature. In total, therefore, the MORT text contains the state-of-the-art criteria applicable for judging when an event is adequate or LTA.

The obvious problem for the MORT practitioner is how to quickly relate the applicable criteria to the specific event being considered. The MORT text is an invaluable reference document, but it is not the handy, quick-look, supportive reference source needed by the inexperienced MORT practitioner.

In the pages which follow, this User's Manual seeks to summarize, index, and cross reference to the MORT text the concepts and criteria applicable to each event of the MORT diagram.

An event-by-event review is made, using an indexed tabulation format keyed to the event identification scheme of the MORT diagram. Basic event statements are usually converted to questions, as this is the form the analyst must use as he asks himself whether the particular event is adequate or LTA. The style and tense adopted for the Specific Control Factors branch are based upon the assumption a specific accident has occurred, with consequent injury or property damage. The style and tense used for the Management System Factors branch are based upon use of the MORT diagram for appraisal of an existing safety system. The questions are phrased in a positive manner so that if the answer is "LTA," the evaluated event is judged a "fault."

Four format issues used are provided as follows:

1. Statement of the MORT Indexed Event

   Each event listed on the MORT diagram is reviewed whether it be a "generic" event or a "basic" event. The event statement is positioned on the page in accordance with its indexed position in the MORT indexing scheme. The statement is usually paraphrased as a question. Incomplete sentence structure is sometimes used for brevity (particularly at the basic event level).

2. Additional Questions

   In some instances, additional questions relative to the event are posed to the reader. The purpose is twofold: (a) to probe how effectively the event fits the accident or safety system being analyzed and (b) to help the user determine whether sufficient information is available to answer the question implied by the event statement, or whether more detailed information is needed before judgment can be made.

3. Commentary

Additional explanation or caution based upon MORT seminar teaching experience is made where appropriate. The nature of the commentary depends upon the specific event (i.e., whether an upper tier generic type event or a lower tier basic event).

In general, the amount of commentary has been limited to that required for the MORT practitioner to grasp the thought associated with the event statement.

4. MORT Text Cross-Reference

Should the user want a more detailed explanation of the safety program concept and criteria, a MORT text page number(s) is often provided in parentheses following the commentary of the indexed event statement. Where more than one page number is given, the first number listed is the principal MORT text reference. If an additional tree is available for more rigorous analysis, as in Independent Review, the reference is shown as Tree, page 5 of Exhibit 8 in the MORT text.

QUESTIONS FOR THE MORT ANALYST

The following questions may be used in conjunction with the MORT diagram. The reader is reminded that the Specific Control Factors (S) branch questions presume an accident, whereas the General Management Factors (M) branch questions are phrased from the assumption of a safety system evaluation. Whatever is the actual case, the user should have no great difficulty in making the mental adjustment.

T. Fundamental Questions (the Top event)

What happened?
Why?
What were the losses? (Specify the number and type of injuries, the amount of property damage, production downtime, product degradation, reduction in employee morale, program impact, negative publicity, or any other type of loss.)
[The construction layout shows an alternative top event connected to the diagram by a dashed line. This unique method is employed to show the duality of MORT application. When using MORT as an appraisal tool, the analyst views the Top event statement as future potential losses that may result from an Assumed Risk or from an Oversight/Omission existent in the safety system evaluated.]

S/M. Oversights and Omissions

[The tree structure depicts two fundamental causes of the adverse consequences listed by the Top event: (1) Management Oversights and Omissions, or (2) Assumed Risks. All contributing factors in the accident sequence are seen as Specific Oversights and Omissions until such time as they are transferred to Assumed Risks. Further discussion of Assumed Risks is provided under its appropriate heading. Input to the Oversights and Omissions event is through an AND logic symbol, because MORT experience, to date, shows the S and M branches to be mutually inclusive.]

S. Specific Control Factors

What were the specific control factors of the management system that were overlooked or omitted? [Detailed understanding of the incident/accident sequence leads naturally to: (1) consideration of the Management System Factors, and (2) judgment whether the fault (failure potential) was an Assumed Risk.]

SA1. Accident

Describe what happened.
[MORT conceives the accident occurred when an unwanted energy flow or environmental condition that results in adverse consequences reaches persons and/or objects. MORT combines this concept and others into a functional accident definition as follows: An unwanted transfer of energy or environmental condition because of lack or inadequate barriers and/or controls, producing injury to persons and/or damage to property or the process.]

SA2. Amelioration LTA

Once an accident has occurred, was there adequate amelioration on the part of all concerned parties?

[Amelioration can only be considered and evaluated after an accident, thus the "Accident Occurrence" constraint on the gate leading to lower branch elements. The intent of amelioration is to limit the consequences of what has immediately occurred and to reduce the sensitivity of those consequences whenever possible. When evaluating Amelioration from an overall management system standpoint, consider the following: (1) Are all of the amelioration functions preplanned (as opposed to the possibility of having them occur fortuitously at the time of a particular accident)? (2) Does the plan adequately scope the types and severity of accidents which it intends to cover? (3) Are adequate resources allocated to properly execute the plan? and (4) Is management aware of any residual risk beyond the scope of the plan?]

a1. Prevention of Second Accident LTA:
Was prevention of a Second Accident or further losses adequate? Through the efforts of individuals at the accident scene and those who arrived later, were steps taken to prevent a second accident caused directly or indirectly as a consequence of the first?

b1. Plan LTA:
If properly executed, was the plan adequate to accomplish the intended function? Was the plan provided to those who needed it?

b2. Execution LTA:
Was the plan executed as was intended?

c1. Practice LTA:
Was there sufficient practice of various plan assignments? Was the practice realistic?

c2. Personnel and/or Equipment Changes:
Was there personnel or equipment changes that caused the execution of the plan to be LTA? Were trained personnel free of any recent physical or mental changes? Was the equipment familiar to the users and free of defects or modifications?

d1. D/N Counterchange:
Had appropriate counterchanges been considered and introduced where applicable for changes in personnel or equipment?

c3. Task Performance Errors:
Was the plan executed properly through successful completion of all steps?
[Note the transfer in of other lower tier events from SD5-b3.]

a2. Emergency Action (Fire Fighting, Etc.) LTA:
Was the emergency response prompt and adequate?
Which emergency response teams were required? Were they notified and did they respond?
[Include local facility fire brigade, health physics team, fire department, bomb squad, and other specialty teams. Be sure to consider delays or problems in both notification and response.]
[Note other lower tier events included by transfer from a1.]

a3. Rescue LTA:
Were trapped or immobilized victims satisfactorily removed to a safe area? Before entering a hazardous area, did rescuers consider the risk of injury to themselves versus the ability to lessen the severity of injuries to victims? Include the evacuation of employees or the public from potentially hazardous areas.
[Note other lower tier events included by transfer from a1.]

a4. Medical Services LTA:
Was adequate medical service available?

b3. First Aid LTA:
Was adequate first aid immediately available at the scene? Was it used properly to prevent immediate injuries from becoming more severe?

b4. Transport LTA:
Was mobile service available to transport medical personnel and equipment to the accident scene and/or to transport injured to medical facilities? Was transport executed properly?

c4. Plan:
Was there a medical service plan? Was it distributed to appropriate personnel?
[Consider such things as: (1) how to make a notification, (2) training of medical personnel and drivers and when they are available, and (3) who and what equipment will respond.]

c5. Notice:
Was notification made in an adequate time and manner? Were employees instructed on how to notify medical services? [Consider whether notification process was easy to do, especially during the stress of an emergency.]

c6. Personnel and Equipment:
Did the personnel use the equipment correctly? Did the equipment function properly? Did the medical and transport personnel have all the equipment necessary to properly perform the jobs expected of them? Where the personnel adequately trained relative to the postulated needs?
[Consider whether equipment could be operated easily during the stress of an emergency.]

c7. Distance:
Was there a significant distance between medical services and area to which service responded?
[If the distance is great, response time is increased.] [Note the event is flagged with R1 assumed risks. Top management must assume distance/time response risk.]

b5. Medical Treatment LTA:
Was there adequate medical treatment enroute and at the medical facilities?

a5. Rehabilitation LTA:
Was rehabilitation of persons and objects made after the accident?

b6. Persons:
If the injury was disabling, could its overall disabling effect have been reduced and/or the individual made more functional? If such rehabilitating activity was possible, was it done?

b7. Objects:
Was damaged equipment, buildings, or other property expeditiously repaired, salvaged, or replaced?

a6. Relations LTA:
Was there a management plan outlining the protocol to be followed and steps to be taken subsequent to a significant accident? Was the accident news disseminated to all concerned parties in a proper and timely manner?

b8. Employee:
Did the relatives of the injured employee first hear about the accident from a responsible, tactful individual within the organization? Were the other employees in the organization notified firsthand about the accident with some assurance that significant corrective action would be taken?

b9. Officials:
Were the facts about the accident given accurately and in a timely manner to the proper officials of: (1) the organization, (2) the customer, (3) the local municipality, (4) the state, and (5) other governmental agencies as appropriate?

b10. Public and

b11. Media:
Were the news media (and thereby the public) given the accident facts and assurance that significant corrective actions were being taken? Was a specific point of contact within the organization provided as the source of additional information?

SB1. Potentially Harmful Energy Flow or Environmental Condition

What was the energy flow or environmental condition that resulted in the accident. [SB1 denotes an energy flow or environmental condition which could result in harm if barriers and controls are inadequate and a vulnerable person or object is exposed.]

a1. Nonfunctional:

Was the energy flow or environmental condition causing the harm a functional part of or product of the system?

b1. Was there adequate control of nonfunctional energy flows and environmental conditions?

b2. Was such control practicable?

[Note that the event is flagged with R4 assumed risk symbol. Proper management level must assume responsibility for this decision.]

a2. Functional:

Consider the lower tier elements below this only if the harmful energy flow or environmental condition was a functional part of or a product of the system. Given a failure of the barrier system, the following questions should be considered:

b3. Were the administrative controls adequate to prevent the harmful energy flows or environmental conditions from reaching vulnerable persons or objects?

SB2
SB3

b4. Diversion LTA:

c1. Was there adequate diversion of harmful energy flows or environmental conditions?

c2. Was diversion impractical?

[Note that this event is flagged with R5 assumed risk symbol. An appropriate management level should assume risk responsibility for this decision.]

SB2. Barriers and Controls LTA (Incident)

Were adequate barriers and controls in place to prevent vulnerable persons and objects from being exposed to harmful energy flows and/or environmental conditions?

Note: The constraint placed on SB2 is intended as a device to prevent oversight. It is designed primarily to draw attention to barriers and control related to harmful energy flows or environmental conditions and those controls designed to control movement of target persons or objects.

Both types of barriers should be considered but rigorous and proper classification is not necessary to the analytical processes, provided that all barriers are considered.

Were the barriers and controls designed to prevent harmful energy flows or environmental conditions from reaching vulnerable people and objects LTA? [Refer to SC1 and SC2 for further development.]

Were barriers and controls designed to prevent vulnerable people and objects from encountering harmful energy flows and environmental conditions LTA? [Refer to SC1 and SC2 for further development.]

SB3. Vulnerable People or Objects

Note: The constraint "value" in place here. An accident is defined in terms of loss of something of "value."

What vulnerable people and/or objects of value were exposed to the harmful energy flow or environmental condition?

a1. Nonfunctional:

Was the person or object performing a functional role in operation of the system?

b1. Was there adequate control of nonfunctional persons and objects?

b2. Was such control practicable?

[Note that the event is flagged with R4 assumed risk symbol. Proper management level must assume risk responsibility for this decision.]

a2. Functional:

Consider the lower tier elements below this only if the person or object was performing a functional role in operation of the system. Given a failure of the barrier system consider the following:

Note: The constraint in place here. An accident can only occur if the barriers were LTA.

b3. Were the administrative controls adequate to prevent persons or objects from being exposed to the harmful energy flow or environmental condition?

b4. Evasive Action LTA:

c1. Was there adequate evasive action for vulnerable persons or objects?

c2. Was evasion impractical?

[Note that this event is flagged with R5 assumed risk symbol. An appropriate management level should assume risk responsibility for this decision.]

SB4. Events and Energy Flows Leading to Accident-Incident

What were the events and energy flows leading to conversion of hazards to actual accident-incidents. (Analyze as appropriate to the accident events.) [Refer to SC3 and SC4 for further development relating to precurser events and energy flows.]

Note: Energy-barrier analysis (1) and events and causal factor analysis (2) should be used as appropriate to the situation.

SC1. Control LTA

Were there inadequacies in the control system that was established to prevent vulnerable people and objects from interacting with harmful energy flows or environmental conditions? [Analyze the specific nature of these failures in terms of SD1 through SD6.]

SC2. Barriers LTA

Were there failures of barrier systems provided to prevent interactions between vulnerable people and objects and harmful energy flows or environmental conditions?

Were there adequate barriers? What were the specific barriers? [The 12 barriers listed on page 33 of the MORT text and their order of listing should be reviewed carefully. MORT treats the first five listed barriers as a function of concept and design. The four "intermediate" barriers (i.e., source-target) are listed by MORT as specific inputs to this Barriers event. The final three "target" barriers are treated elsewhere on the MORT diagram. The example of grinding wheel safety practices, Figures 2-3 on page 35 of the MORT text, is particularly helpful in illustrating the barrier concept.]

Note: The following breakdown (a1, a2, a3, a4) is intended as a device to prevent oversight. All barrier types should be considered.

Rigorous and proper classification in terms of a1, a2, a3, a4 is not necessary to the analytical process provided that all barriers are considered. A supplementary barrier analysis form available from SSDC may be used in recording this information.

a1. Were there barriers on the energy source?

[Note other lower tier events included by transfer from a3.]

a2. Were there barriers between the energy source and the injured person/damaged equipment?

[Note other lower tier events included by transfer from a3.]

a3. Were there barriers on persons and/or objects?

[Note all lower tier development under this event also transfers to a1., a2., and a4.]

b1. None Possible:

[Note use of the Diamond event symbol, indicating termination of fault sequence because of the lack of solution. Note also the event is flagged with R2 assumed risk symbol. Appropriate management must assume risk for design where no barriers were possible.]

b2. Barrier Failed:

Did the barrier function as intended?

b3. D/N Use:

Were barriers used?

c1. D/N Provide:

Were barriers provided where possible?

SC3
SC4
SD1

[Note the event is flagged with R3 assumed risk symbol. An appropriate level of management must assume risk for failure to provide barriers, e.g., failure to provide safety glasses.]

c2. Task Performance Errors:

Were the provided barriers used properly? (e.g., Were available safety glasses improperly used?)

[Note that all the lower tier development under event SD5-b3 transfers to this event also.]

a4. Were there "barriers" of time or space which separated the energy and the person or object?

[The term "barrier" has the connotation of physical intervention; however, the barrier may be a "paper barrier." Separation by time or space in particular may be accomplished by written procedure or some other type of administrative control.]

[Note other lower tier events included by transfer from a3.]

SC3. Barriers and Controls LTA

Were barriers and controls on energy transfers and other events leading to conversion of a hazard to an actual accident less than adequate? [Refer to SC4 for description of these events and to SB2 for further development relating to barriers and controls on preceding events.]

SC4. Events and Energy Flows

What were the precursor events and energy flows that resulted in conversion of a hazard to an actual accident? [Refer to SB1 for further development relating to these preceding events.]

Note: Energy-barrier analysis (1) and events and causal factor analysis (2) should be used as appropriate in the SC3 and SC4 subjects.

SD1. Technical Information Systems LTA

Was the technical information system adequate (with respect to the unwanted energy flow)? (349)

[Complex work flow processes must be supported by complete technical information systems. It is axiomatic that complex systems will depart from plans and procedures to some degree. Therefore, information systems need to detect deviations, determine rates and trends, initiate corrections, and, in general, assure that goals are attained. MORT conceives a technical information system as consisting of "research" persons, "program" persons, and "action" persons obtaining, handling, and providing technical information relevant to the work flow process in a "communication" network.]

a1. Technical Information LTA:
Was there adequate technical information relevant to the work flow process?
[Often relevant information exists but is not available to the "action" persons associated with the process. Possible reasons are investigated by the following series of questions.]

b1. Knowledge LTA:
Was knowledge of the work flow process adequate? [The question is investigated by subdividing into known and unknown precedent.]

c1. Based upon known precedent (i.e., for the prevention of the unwanted energy flow):

d1. Was application of knowledge obtainable from codes and manuals adequate? (260)

d2. Was the list of experts (to contact for knowledge) adequate?

d3. Was any existing but unwritten precedent relevant to the work flow process (i.e., part of the supervisor's regular practice) known to the "action" person?

d4. Were there studies directed to the solution of known work flow process problems? Was the effort being spent in the search for their solution reasonable and adequate? (265)

c2. If there was no known precedent:

d5. Were there investigation and analysis (i.e., risk analysis) of prior similar accidents/incidents or the work flow process accident potential? Was the investigation adequate? (95)

d6. Was there research directed to the obtaining of knowledge about the work flow process? Was the research effort reasonable and adequate? (97)

b2. Communication LTA:
Was the exchange or transmittal of knowledge adequate (relative to the potential unwanted energy transfer)?

c3. Was the internal communication adequate? (391)

d7. Was the definition of the internal communication network adequate?

d8. Was operation of the internal network adequate?

c4. Was the external communication adequate? (411)
[The query relates to the interface between the in-house (internal) information system and national information systems, such as the National Safety Council, NASA, NSIC, and others.]

d9. Was the definition of the external communication network adequate?

d10. Was the operation of the external communication network adequate? Was the method of searching, retrieving, and processing relevant information adequate?

a2. Monitoring Systems LTA:
Was the monitoring system adequate? Were the principal elements of a good monitoring system present? (351)
[Highly complex work flow processes require a high order of excellence of the monitoring subsystem of the technical information system. The management Risk Assessment system must be closed-loop to maintain the process "in control." Triggers for fast action fixes and data for achieving long-range hazard reduction goals are generated by the Monitoring System and transmitted by the Technical Information System to the Hazard Analysis Process (HAP) portion of the Risk Assessment System.]

b3. Was the safety observation plan (employed by work flow process supervision) adequate?

b4. Was there a planned independent searchout effort for high potential hazards by a safety professional? Was the safety inspection searchout effort adequate?

b5. Was incident/accident information, relative to prior incidents/accidents in similar processes, recorded and reviewed?

b6. Was there a planned Reported Significant Observation (RSO) system? Was it operative? (116, 361) MORT uses this term for a special safety study rather than the better known "critical incident" for semantic reasons. ("Critical" and "criticality" have very different and specific meaning in the nuclear energy field.) The RSO concept relates to the study of near-miss incidents observed and reported by line supervision and work level personnel.]

b7. Error Sampling System LTA:
Was there an error sampling plan? Was it operating adequately? (357)
[Error sampling is a specific management plan whereby staff personnel systematically sample for operating errors, using prepared checklists and definitions.]

b8. Were the routine field safety work site inspections made? Were they adequate?

b9. Was the audit of "upstream" work flow processes conducted in an adequate manner? (114)

[MORT separates the general work flow process into: (1) worksite operations; and (2) upstream work flow processes such as design, construction, selection and training, etc. Each segment must be examined relative to the three basic work ingredients - hardware, procedures, and people.]

b10. Was the general health monitoring of work flow process personnel adequate? (373)

a3. Data Collection and Analysis LTA:
Were the data collection and analysis procedures adequate? Were there analyses (i.e., measurement techniques) made of the data? Did the analyses provide the proper risk assessment information to the decision maker responsible for the risk assumption? (415, 372)

b11. Was there a priority problem list? Had it been updated to be a current list? (375) [Management should, at all times, know what its most significant assumed risks are thought to be. Any delay in corrective action for budget reasons becomes an assumed risk for the present.]

b12. Were the available status and predictive statistics adequate? (415)

b13. Was the diagnostic statistics analysis adequate?

b14. Was the risk projection analysis adequate?

b15. Was the "War Room" status display of current problems, analyses, and results adequate? (439, 97)

a4. HAP Triggers (Fix Control Initiators) LTA:
Were triggers (stimuli) for the initiation of the Hazard Analysis Process (HAP) adequate? Were they utilized to obtain early safety anticipation and review in planned or unplanned changes? (233) [MORT postulates HAP triggers as part of the HAP portion of the Risk Assessment System, but originating from the Monitoring Subsystem of the Technical Information System.]

b16. One-On-One Fixes LTA:
Was the information from the technical information system adequate to trigger the HAP preventive action plan for individual problems? (397)

b17. Priority Problem Fixes LTA:
Was the information from the technical information system adequate to provide a continuous trigger to the HAP Priority Problem Lists? (234)

b18. Planned Change Controls LTA:
Were HAP triggers from planned changes in the work process adequately recognized? Were they used? (233)

b19. Unplanned Change Controls LTA:
Were HAP triggers from unplanned changes in the work process adequately recognized? Were they used? (233)

b2O. New Information Use LTA:
Were HAP triggers from research, new standards, etc., detected and used? (234)

a5. Independent Audit and Appraisal LTA:
Was there a recent appraisal of the total safety system (or audits of parts thereof)? Were the audits and appraisals conducted in a truly independent manner? Was the appraisal plan adequate? (371, 399)

SD2. Facility Functional Operability LTA

In accident/incident analysis, the accident is considered to be prima facie evidence that the system was not operationally ready. MORT, therefore, deals with "operational problems" by evaluating operational readiness in terms of readiness of the three major system elements: "plant/hardware," "procedures/management controls," and "personnel." In MORT analysis, the "operational problems" are analyzed in terms of these three elements in two steps: (1) Operational readiness trees are used to better define and localize the functional inadequacies; and (2) Conventional MORT analyses are used to define causal factor chains associated with the inadequacies (including definition of root causes).

Was the facility and process operationally ready? Were the necessary supplementary operations supportive to the main process ready? (293) [This branch probes the status of "upstream processes" (design, training, etc.) which supports the ingredients of the work process (hardware, procedures, and people). The ingredients used at the worksite are obtained from two major upstream subprocesses: (1) the original design, construction, test, and qualification plus documents defining operating limits and performance specification, and (2) modification projects to the facility. All "upstream processes," including the Hazard Analysis Process, are susceptible to constructive analysis as "work processes" in themselves. Each upstream process can be analyzed as to hardware, procedures, and personnel.]

a1. Verification of Occupancy-Use Readiness LTA:
Was verification of the facility and/or work process adequate? [Two publications of the System Safety Development Center, SSDC-1, "Occupancy-Use Readiness Manual," September 1975, and SSDC-39, "Process Operational Readiness and Operational Readiness Follow-On," February 1987, provide detailed criteria for this major functional branch.]

b1. Was the conduct of an operational readiness review specified?

b2. Were the criteria used for determining the facility or process readiness adequate?

b3. Was the required procedure for determining occupancy-use readiness followed?

b4. Were the personnel who made the decision on occupancy-use readiness adequately skilled and experienced?

b5. Was the follow up of action items from occupancy-use readiness review adequate? Were all outstanding action items resolved prior to startup of the work flow process?

a2. Organizational and Functional Relations LTA:
Was there adequate technical support furnished to the work flow process, particularly at the worksite? Were the organizational versus functional relationships adequate to assure the required level of operability?
[Highly complex processes need close field liaison by scientific and engineering personnel.]

a3. Interface Between Operations and Maintenance and Testing Activities LTA:
Was the interface between operations personnel and testing and maintenance personnel adequate? Were administrative procedures well-planned to preclude misunderstanding of operational status due to a breakdown of communication?

a4. General Design Process LTA:
Was the actual physical arrangement or configuration identical with that required by latest drawings, specifications, and procedures? Were the configuration and documentation of modification to the facility or process adequately controlled? Was the general design process adequate to assure functional operability?

SD3. Maintenance LTA (Basic logic same as SD4, Inspection LTA)

SD4. Inspection LTA

Was there adequate maintenance (or inspection) of equipment, processes, utilities, operations, etc?

a1. Plan LTA:
Was the plan scope broad enough to include all the areas that should be maintained (or inspected)? Was management aware of those areas not included in the plan?

b1. D/N Analyze Failure for Cause:
Did the plan require that any failed item be analyzed for cause of failure? Were the analysis results required to be acted upon by an appropriate individual or group?

(Note: Items b1 and b2 of this section were interchanged in the Maintenance branch.)

b2. D/N Specify:
Were maintainability (inspectability) requirements specified by the design or procurement documents? If not, are they provided adequately by operations plans? (311)

c1. Maintainability (Inspectability) LTA:
Did the plan address methods for minimizing problems with equipment, processes, utilities, operations, etc. when they are undergoing maintenance (or being inspected)?

c2. Schedule LTA:
Was there a schedule? Did the plan schedule maintenance (inspections) frequently enough to prevent or detect (as appropriate) undesired changes? Was the schedule readily available to the maintenance (inspection) personnel? Was the schedule coordinated with operations to minimize conflicts? (313)

c3. Competence LTA:
Did the plan specify minimum requirements for the competence and training of individuals used in the program?

a2. Execution LTA:
Was there adequate execution of the maintenance (or inspection) plan?

b3. Task Performance Errors:
Were the individual tasks (as set forth by the plan) performed properly? [Note other lower tier events included by transfer SD5-b3.]

b4. D/N Maintain "Point-of-Operation" Log:
Was there a log of maintenance (inspections) kept at the point-of-operation on the piece of equipment, process, etc.? (311) [This is distinct from other logs that may be kept in a control room, back at the main office, or in someone's desk or file. Familiar examples include the periodic inspection tags found on fire extinguishers and in elevators.]

b5. Caused Failure:
Was maintenance (inspection) of the work flow process performed without the maintenance (inspection) activity itself causing a failure or degradation of the process?

b6. Time LTA:
Was the time specified in the plan's schedule sufficient to adequately perform the task at each station? Was the time budgeted for personnel adequate to fulfill the schedule? Was the time actually provided?

SD5. Supervision LTA

Was the worksite supervision adequate? Were the necessary supportive services adequate? (297)
[MORT identifies the first line supervisor as a "key man" in worksite safety, as he unquestionably is. However, if the supervisor is to adequately fulfill his responsibilities, he must have competent and useful advice and support from several kinds of supportive services. The adequacy of site supervision is, therefore, examined by MORT in this broader context. In particular, MORT tries to assess management's role in support and service to the supervisor. The emphasis throughout is to discuss what in the management system failed - not who.]

a1. Help and Training LTA:
Were the help and assistance given to supervisors adequate to enable them to fulfill their roles? Was the feedback of information to the supervisor adequate? Was it furnished in a form usable by the supervisor? What training had the supervisor been given in general supervision? What training had the supervisor been given in safety? Has the supervisor training program been evaluated? (300)

a2. Time LTA:
Did the supervisor have sufficient time to thoroughly examine the job?

a3. Supervisor Transfer Plan LTA:
Were there any gaps or overlaps in the supervisory assignments related to the event? If the supervisor was recently transferred to the job, was there protocol for orderly transfer of safety information from the old to the new supervisor? (303)

a4. D/N Detect/Correct Hazards:
Were the supervisor's efforts adequate in detection and correction of hazards?
[Knowledge of hazards is often available from the work force. The supervisor must be receptive and accessible and must display vigor in acting on suggestions, if he is to gain access to that knowledge.]

b1. D/N Detect Hazards:
When did the supervisor last make an inspection of the area? Was any unsafe condition present in this accident/incident also present at the time of inspection? Was the condition detected? (303)
[Note that if the condition was detected but not corrected, the analysis shifts to D/N Correct Hazards.]

c1. Knowledge (Checklists) LTA:
Was a checklist specific to the process available? Was it used? Was the supervisor considered generally competent to assess safety aspects of his area of work?

c2. Detection Plan LTA:
Was there an overall detection plan for uncovering hazardous conditions?

d1. Logs/Schematics LTA:
Was the point-of-operation posting of warnings, emergency procedures, etc., provided for in a general detection plan? Were maintenance and inspection logs at the point of operation adequate? Were work schematics adequate? Were equipment change tags used? (304)

d2. Supervisor Monitor Plan LTA:
What guidance was given to the supervisor relative to inspecting and monitoring status of the process ingredients (i.e., equipment, procedures, and personnel)? Did he use the guidance? Was he given guidance on detection of individual personnel problems, such as alcoholism, drug use, personal problems?

d3. D/N Review Changes:
Was guidance given on review methods and change detection? Were the changes involved known to the supervisor? What counterchanges were made for the known changes?

d4. D/N Relate to Prior Errors:
If there were any known prior errors afflicting the process, was the supervisor told they might correlate with safety errors? Had he made an effort to correlate them? Was he aware of other signs or warnings that the process was moving out of control?

c3. Time:
Did the supervisor have adequate time to detect the hazards?

b2. D/N Correct Hazards:
Was an effort made to correct the detected hazard? (305)
[Some facts about noncorrection of hazards were dealt with under nondetection. There are some basic factors of noncorrection still to be examined.]

c4. Interdepartment Coordination LTA:
If the accident/incident involved two or more departments, was there sufficient and unambiguous coordination of interdepartment activities?
[Interdepartment coordination is a key responsibility of the first line supervisor. It should not be left to work level personnel.]

c5. Delayed:
Was the decision to delay correction of the hazard assumed by the supervisor on behalf of management? Was the level of risk one the supervisor had authority to assume? Was there precedent for the supervisor assuming this level of risk (as then understood by him)?
[Note a decision to delay correction of the hazard may or may not transfer to the Assumed Risk branch. It was an assumed risk only if it was a specific named event, analyzed, calculated where possible, evaluated, and subsequently accepted by the supervisor who was properly exercising management-delegated, decision-making authority.]

d5. Was the decision to delay hazard correction made on the basis of limited authority to stop the process?

d6. Was the decision made because of budget considerations?

d7. Was the decision made because of time considerations?

c6. Program Housekeeping LTA:
Was the housekeeping of the ongoing program adequate? Was the storage plan for unused equipment adequate?
[The true role of housekeeping in the accident experience is usually unclear.]

c7. Supervisory Judgment:
Was the judgment exercised by the supervisor to not correct the detected hazard adequate considering the level of risk involved? If there were previously established supervisor authority limitations, were the supervisor's actions generally in accord with those limitations? [Evaluation of the performance of a supervisor in a given situation is, of course, retrospective and must be fairly considered. If the authority limitations of the supervisor have been defined (as they should be), then the adequacy of his performance is more easily measured.]

a5. Performance Errors:
Was the work activity at the worksite free of performance errors by work level personnel? (331)
[The MORT analysis separates performance errors into task, nontask, and emergency shutoff errors. Worksite activity can be viewed as usually proceeding in a normal manner to attainment of performance goals. If the ongoing activity enters a nonnormal phase requiring work process shutoff, it is described as an emergency, and is analyzed in the light of the additional stress associated with emergency action. The analysis proceeds more easily with these considerations. It should be pointed out that the kinds of questions raised by MORT are directed at systemic and procedural problems. The experience, to date, shows there are few "unsafe acts" in the sense of blameful work level employee failures. Assignment of "unsafe act" responsibility to a work level employee should not be made unless or until the preventive steps of: (1) hazard

analysis, (2) management or supervisory detection, and (3) procedures safety review have been shown to be adequate.]

b3. Task Performance Errors:
Was the task-related work activity free of hazards caused by performance error?

c8. Task Assignment LTA:

Was the task assignment properly scoped with steps and objectives clearly defined? Was the task assignment one the supervisor should have made? (332)

c9. Task Safety Analysis (e.g., JSA) Not Performed:
Was any form of task safety analysis performed as part of the work process? (316)
[Effort directed to task Safety Analysis should be scaled to fit the magnitude of the safety hazard posed by the work task. The safety analysis effort applied to work processes having high energy potential or high hazard potential is usually highly formalized. The analysis results are implemented by a written procedure developed by the task supervisor and a small group of his most skilled craftsmen, and will usually be subjected to independent review. An example of this kind of task safety analysis is Job Safety Analysis (JSA), a process used by many large industrial companies. At the other end of the spectrum of Task Safety Analysis is the informal, oral review of task safety measures by the task supervisor, before work level personnel start to work the task. This latter level of safety analysis is applied to tasks having relatively low energy or low hazard potential. It is used most often with tasks related to routine maintenance and repair activity and will usually not have been independently reviewed.

The task safety analysis level of effort actually applied will range somewhere between the extremes described. MORT uses the concept of Pre-Job Analysis by which is meant that nearly every task must be surveyed step-by-step to determine the level of effort of Task Safety Analysis that should be applied to the work task to be performed. The MORT diagram analysis proceeds with the premise a Pre-Job Analysis should <u>always</u> be made for tasks assessed as having significantly high hazard potential.]

d8. High Potential:
Was an analysis performed for a work task involving a high potential for error, injury, damage, or for encountering an unwanted energy flow?

e1. Pre-Job-Analysis Not Required:
Did the operations management require a pre-job-analysis to scale the magnitude of task safety analysis to be performed?

e2. If required, was the pre-job-analysis, as performed, adequate to scale the magnitude of task safety analysis to be performed?

e3. Pre-Job-Analysis Not Made:
Was a pre-job-analysis required but not made?

f1. Was it not made because of lack of authority?

f2. Was it because of budget reasons?

f3. Was it because of schedules?

f4. Was it because of a decision by the line supervisor?

d9. Low Potential:
Was the work task assessed as one involving low potential? Was this a reasonable assessment? Was the decision to <u>not</u> perform a task safety analysis properly delegated to the supervisor?
[Note the event is flagged with R6 assumed risk symbol. If the criteria for risk identification and assessment were properly met, this event transfers to the Assumed Risk branch.]

c10. Pre-Task Briefing LTA:
Was the work force given a pretask briefing (prior to task performance)? Was it adequate? Did the pretask briefing adequately consider the net effect of recent changes, maintenance, new hazards, etc.?

c11. Task Safety Analysis (e.g., JSA) LTA:
Was the task safety analysis adequate? Was the task safety analysis scaled properly for the hazards involved?

d10. Preparation LTA:
Was the preparation (and content) of the task safety analysis adequate?

e4. Selection LTA:
Were the safety hazards associated with the work task adequately identified and selected? (318)

f5. Were the criteria used adequate?

f6. Were the methods used in prioritizing the identified hazards adequate?

e5. Knowledge LTA:
Was the knowledge input to the task safety analysis adequate?

f7. Employee Suggestions and Inputs LTA: Was consideration of employee-developed suggestions and inputs adequate?

g1. JSA Program LTA:
Was a JSA program used to obtain work level employee participation? Was the process of accomplishing the JSA program adequately defined and staffed?

g2. General System LTA:
Was the general management system for collecting and utilizing other employee suggestions and inputs adequate?

g3. RSO Study LTA:
Were "Reported Significant Observation" (RSO) studies used to gather employee inputs? Were these RSO's readily accessed? (116)

g4. D/N Use Suggestion:
Were employee suggestions and inputs (made through JSA, RSO, and other processes) used in the task safety analysis?

f8. Technical Information LTA:
Was the technical information (with respect to the preparation of the task safety analysis) adequate? [Technical information relevant to safety aspects of the work process often exists but is not available to the "action" persons associated with the process. Possible reasons are investigated by a series of lower tier questions. Analysis of these lower tier events is shown under SD1-a1. Note the analysis transfers to this event also.]

e6. Development LTA:
Was the development of the specific task safety analysis by the first line supervisor adequate? If judged to have been inadequate, what were the true underlying causes for the inadequacy? [An honest assessment should be made of what could reasonably be expected of the supervisor, taking into account existing time and budget restrictions placed upon him by higher supervision.]

f9. Time LTA:
Was there time for an adequate development of task safety analysis?

f10. Budget LTA:
Was there sufficient departmental budget?

f11. Scope LTA:
Were the scope and depth of the task safety analysis development sufficient to cover all related hazards?

f12. Professional Skill LTA:
Were the experience and skill of the supervisor and other participants adequate to accomplish the required work task safety analysis?

d11. Safety Analysis Recommended Controls LTA:
Were adequate worksite controls placed on the work process, facility, equipment, and personnel by the task safety analysis?

e7. Organization and Clarity LTA:
Were the organization and clarity of presentation of the task safety analysis recommendations adequate to permit their easy use and understanding?

e8. Programmatic Conflict:
Were the recommended controls free of conflict with the overall project goals and requirements?

e9. Control Testing LTA:
Were recommended controls tested at the worksite for feasibility before being directed for use?

e10. Directive For Use LTA:
Was the management directive for use of the task safety analysis recommended controls adequate? Was it explicit and not subject to possible misunderstanding?

e11. Availability LTA:
Did the management information system make knowledge of the recommended controls available to the worksite personnel?

e12. Adaptability LTA:
Were the recommended safety controls made in a form which allowed them to be adequately adapted to the varying situations?

c12. D/N Use Safety Analysis Recommended Controls:
Were the safety controls recommended by the task safety analysis used?

d12. Use Not Mandatory:
Was use of the recommended safety controls mandatory? [If use of the recommended safety controls was not mandatory, failure to use them is either an Assumed Risk or a management system failure.]

d13. Deviant Performance:
If use of the recommended safety controls was mandatory, were they actually used?
[If use was mandatory, failure to use them is a deviant performance on the part of the line supervisor.]

c13. Task Procedure D/N Agree With Functional Situation:
Did the work task completion procedure, as directed by oral or written instruction, agree with the actual requirements of the work task? [Direction or requirements, as defined by specifications, operating procedures, equipment manuals, etc., may conflict with actual work task requirements.]

c14. Personnel Performance Discrepancy:
Did the individuals assigned to the work task perform their individual task assignments properly? [Possible causes of performance discrepancy should be considered for each individual whose performance was judged to be discrepant.]

d14. Personnel Selection LTA:
Were the methods of personnel selection adequate? (325)

e13. Criteria LTA:
Were the safety-related job requirements adequately defined so as to select an individual with desired characteristics?

e14. Testing LTA:
Did the individual meet the standards established for the task? Had the assigned individual been recently reexamined to the standards established for the task?

d15. Training LTA:
Was the training of personnel adequate? (327)

e15. None:
Was the individual trained for the task he or she performed?

e16. Criteria LTA:
Were the criteria used to establish the training program adequate in scope, depth, and detail?

e17. Methods LTA:
Were the methods used in training adequate to the training requirements? [Consider methods such as realistic simulation, programmed self-instruction, and other special training in addition to basic indoctrination, plant familiarization, etc.]

e18. Professional Skills LTA:
Was the basic professional skill of the trainers adequate to implement the prescribed training program?

e19. Verification LTA:
Was the verification of the person's current trained status adequate? Were retraining and requalification requirements of the task defined and enforced?

d16. Consideration of Deviations LTA:
Was adequate consideration shown by the supervisor for the need to observe deviant personnel performance? (334)
[The analysis shows contributions to Deviations from both Normal Variability and Changes. Normal personnel performance variability is viewed as manageable through appropriate equipment design, good planning, training, and application of human factors. Change is more the characteristics of illness, fatigue, personal problems, etc., which results in individual performance outside the normal range of variability.]

e2O. Normal Variability:
Was the deviation in personnel performance within the range of normal variability?
[The Scroll event symbol is used to show that some degree of variability is normal and expected.]

e21. Changes:
Was the deviation in personnel performance significantly different than the performance standard needed for the task?
[The Scroll event symbol is used to show that some degree of change is normally expected to occur.]

e22. D/N Observe:
Was the deviation (i.e., extreme variability or significant change) observed by the line supervisor?

e23. D/N Correct:
Did the supervisor act to correct the observed personnel performance deviations?

f13. D/N Reinstruct:
Did the supervisor reinstruct the person observed as to the correct performance?

f14. D/N Enforce:
Did the supervisor enforce established correct rules and procedures? Were disciplinary measures taken against personnel who willfully and habitually disregarded rules and procedures?

d17. Employee Motivation LTA:
Were the employee motivation, participation, and acceptance adequate? (337)
[Employee motivation plays a significant role in personnel performance in accomplishment of the work task. Various aspects of employee motivation are analyzed by lower tier events.]

e24. Management Concern, Vigor, and Example LTA:
Was management concern for safety displayed by direct vigorous personal action on the part of top executives? (200)

e25. Schedule Pressure:
Were task schedule pressures (as experienced by the individual) held to an acceptable level?

e26. Performance Is Punishing:
Was the employee fairly treated for performing as supervision desired?
[From the viewpoint of the employee, sometimes there is an undesirable consequence to the person doing a good job.]

e27. Non-Performance Is Rewarding:
Did the employee find the consequence of doing the job incorrectly more favorable than doing the job as directed?
[Obstructive behavior may be more rewarding to the individual than facilitating behavior.]

e28. Job Interest Building LTA:
Does performing the task well <u>really</u> matter to the individual performing it?
[Perhaps the performing individual believes the consequence is the same to him whether he does the task right or some other way. Good performance should be followed at least periodically by an event considered favorable by the individual.]

e29. Group Norms Conflict:
Are the actions and attitudes of the individual's peer groups in harmony with the task requirements and the goals of the larger organization?

f15. Worker Participation LTA:
Was there adequate opportunity for the worker to participate in analysis, training, or monitoring systems (e.g., JSA and RSO studies)?

f16. Innovation Diffusion LTA:
Was there adequate use of management motivational programs to develop desired behavioral change in individuals (i.e., application of innovation diffusion techniques)? [Appendix H of the MORT text.]

e30. Obstacles Prevent Performance:
Were obstacles that might prevent task performance reduced to an acceptable level? [Often a task would get done more efficiently if conditions were changed. If performance discrepancies appear not to be because of lack of skill or motivation, one thing to look for is an obstacle.]

e31. Personal Conflict:
Are individual personal conflicts, which may have a negative relationship to task safety, adequately resolved in the individual? Does the individual have good standards of judgment?

f17. W/Supervisor:
Were employee and supervisor personalities compatible in the work environment?

f18. With Others:
Was the employee's personality compatible with other workers in the work environment?

f19. Deviant:
Were the psychological traits exhibited by the individual judged acceptable when rated against the task safety requirements? Individuals exhibiting abnormally high levels of social maladjustment, emotional instability, and conflict with authority produce more than their share of accidents. The decision to employ an individual in a given task ultimately rests with the line supervisor.
If the organization has maximized its contribution in the areas of management concern, safeguarded

environment, good job safety procedures, good job training, sound human relations, etc., the use of an individual with known deviant performance characteristics in a high potential energy task becomes an assumed risk. [Note the event is flagged with R7 assumed risk symbol. If the criteria for risk identification and assessment were properly met, this event transfers to the assumed risk branch.]

e32. General Motivation Program LTA:
Was there a general motivation program on safety, employed by management, to adequately motivate employees to perform correctly and safely?
[Slogans, posters, leaflets, and contests are a highly visible part of many safety programs. Their true value is difficult to ascertain. These programs do play a supporting role, however and the adequacy of the safety program in these regards should be evaluated.]

b4. Non-Task Performance Errors:
Was the performance of nontask work free of performance errors?
[A "nontask" is one not assigned by a supervisor.]

c15. Peripheral:
Was the work peripheral to the principle task performed error-free?
[Examples are going to or from work on the premises, authorized work break, etc. The activity was not in conflict with the rules.]

c16. Unrelated:
Were all activities unrelated to the authorized work activity performed error-free?
[Examples are going to lunch, recreational programs.]

c17. Prohibited:
Were all performed activities permitted? If not, were the prohibited activities performed error-free?
[Activity in violation of rules, horseplay, etc., is defined as prohibited activity.]

b5. Emergency Shutoff Errors:
If there was an emergency shutdown of some activity from its normal operating mode, was it done error-free?
[Emergency situations usually are a time of rapid change and high stress. The emergency may evolve from a planned task (an in-process work activity) or from a nontask activity. Note the use of the Constraint event symbol requires an off-normal initiating anomaly to have occurred.]

c18. Task Performance Errors:
Was there an emergency shutoff? Was the execution of a planned shutdown sequence accomplished error-free?
[The entire MORT analysis accomplished under SD5-b3 transfers into this event.]

c19. Non-Task Performance Errors:
If there was an emergency situation arising with a nontask activity (i.e., one not assigned by a supervisor), was it free of performance errors?
[See the classification and explanation of nontask performance errors provided under SD5-b4.]

SD6. Higher Supervision Services LTA

Did upper level management provide the type of supportive services and guidance needed at lower organization levels for adequate control of unwanted work process energy flow?

a1. Research and Fact Finding LTA:
Was necessary information, which was not otherwise readily available, sought out through established research and fact finding techniques?

a2. Information Exchange LTA:
Was there an accessible, open line of communications which permitted transmittal of needed information in both directions between upper and lower levels? Was study of a problem a shared responsibility? Were results provided to users?

a3. Standards and Directives LTA:
In cases where the organization and external sources of codes, standards, and regulations did not cover a particular situation, did management develop (or have developed) adequate standards and issue appropriate directives?

a4. Resources LTA:
Did management have the resources derived from standards and directives it needed to perform the supportive services?

b1. Training LTA:
Was there sufficient training to update and improve needed supervisory skills?

b2. Technical Assistance LTA:
Did supervisors have their own technical staff or access to such individuals? Was technical support of the right discipline(s) sufficient for the needs of supervisory programs and review functions?

b3. Program Aids LTA:
Did management have available, for support of its programs, such aids as: useful analytic forms, training materials, reproduction services, audio-visuals, capable speakers, meeting time and rooms, technical information, monographs, etc.?

b4. Measure of Performance LTA:
Were there established methods for measuring performance which permitted the effectiveness of supervisory programs to be evaluated?

b5. Coordination LTA:
Were other management programs and activities coordinated with the groups and individuals who interfaced with the program participants? Did this coordination eliminate conflicts which could have reduced program effectiveness?

a5. Deployment of Resources LTA:
Were the available resources used effectively and to the greatest advantage of supervisory efforts?

a6. Referred Risk Response LTA:
Was management responsive to risks referred from lower levels? Was there an established system for analyzing and acting upon such risks in a timely manner? Was there a fast action cycle to process imminent hazard/high risks?

"Higher Supervision Services" serves as a mechanism to transfer management intent to field activities. In addition to the specific questions dealt with above, a number of questions should also be asked relative to the more general effects of management on employee performance. These include five questions for example:*

- To what degree do such considerations as pay and benefits, working conditions, job security, rewards, and recognition combine to produce adequate worker job satisfaction?
- To what degree do work ethics and practices, concern for safety, concern for quality team orientation combine to produce adequate worker motivation?
- To what degree do loyalty, sense of ownership, pride, respect for radiation, morale, sense of accountability result in adequate work attitudes?
- To what degree do management activities in controlling person-machine interfaces and person-environment interfaces satisfy human factors requirements in an adequate manner?
- To what degree do management activities relating to fitness for duty, testing programs, and discipline result in adequate human reliability?

*Derived from S. B. Haber and D. P. Thurmond, "A Preliminary Identification of the Human Performance Issues Within the Department of Energy," Task 1 Report prepared for the U.S. Department of Energy (1989) and applied in Human Performance Appraisal in June 1990.

M
MA1
MA2

M. Management System Factors LTA

Are all the factors of the management system necessary, sufficient, and organized in such a manner as to assure that the overall program will be "as advertised" to the customer, to the public, to the organization itself, and to other groups as appropriate?
[In the event-by-event review which follows, the questions are phrased in the present tense. Assume the diagram is being used for evaluation of an existing safety system. For accident investigation, rephrase questions to past tense.]

MA1. Policy LTA

Is there a written, up-to-date policy with a broad enough scope to address major problems likely to be encountered? Is it also sufficiently comprehensive to include the major motivations (e.g., humane, cost, efficiency, legal compliance)? Can it be implemented without conflict? (175, 183)

MA2. Implementation LTA

Does the overall program represent the intended fulfillment of the policy statement? If there are problems encountered in carrying out the policy, are these relayed back to the policy makers? Is the implementation a continuous, balanced effort designed to correct systemic failures, and generally preactive rather than reactive? (185)

a1. Methods, Criteria, Analyses LTA:
Are selective methods used for management implementation and for improving human performance? Is there a comprehensive set of criteria used for assessing the short and long-term impact of the methods on safety for the desired results? Does management demand that adequate analyses be performed and alternative countermeasures examined, or are criteria simplistic and therefore LTA? (185)

a2. Line Responsibility LTA:
Is there a clear, written statement of safety responsibility of the line organization, from the top individual through the first line foreman to the individual employee? Is this statement distributed and understood throughout the organization? Is it implemented? (190)

a3. Staff Responsibility LTA:
Are there provisions for assigning and implementing specific safety functions to staff departments (e.g., safety, personnel and training, engineering, maintenance, purchasing, transportation, etc.)?

a4. Information Flow LTA:
Has management specified the types of information it needs and established efficient methods by which such information is to be transmitted up through the organization?

Has management, in turn, supported this process by providing the information needed in lower organization levels? (198)

a5. Directives LTA:
Is safety policy implemented by directives which emphasize methods and functions of hazard review, monitoring, etc., rather than specific rules for kinds of hazards? Are directives published in a style conducive to understanding and without interface gaps? (193)

a6. Management Services LTA:
Has management provided the type of supportive services and guidance needed at the lower organization levels? Is there a formal training program for all management personnel which addresses: (1) general aspects of management and supervision, (2) specific technologies, (3) human relations/communications, and (4) safety? (195) [Note the transfer in of all the lower tier event analysis from SD6.]

As indicated earlier (SD6), Higher Supervision Services is a mechanism by which management intent as described on the "M" portion of the MORT is transferred to specific activities dealt with on the "S" side of the MORT. In addition to explicit analysis of the management functions themselves, one should also ask more general questions relating to management mechanisms for transfer of management intent to the specific organizational activities.*

- To what degree do guidance and direction, management attention, manager presence, promotion of goals and unity, and appropriate recognition of constituencies/customers combine to provide adequate leadership?

- To what degree do strategic/long-range planning, work planning, program coordination and resource allocation lead to adequate overall planning and scheduling?

- To what degree do information collection and processing, upward reporting systems, information dissemination lead to adequate information management?

- To what degree do work processes, work documentation, quality control, authority and use of procedures combine to result in adequate work controls and practices?

- To what degree do problem identification/reporting processes, root cause analysis, corrective action processes, use of lessons learned combine to result in solution of field level problems?

*Derived from S. B. Haber and D. P. Thurmond, "A Preliminary Identification of the Human Performance Issues Within the Department of Energy," Task 1 Report prepared for the U.S. Department of Energy (1989) and applied in Human Performance Appraisal in June 1990.

- To what degree do problem assessment/trending, self appraisal, independent oversight, independent performance evaluation, performance improvement programs combine to provide an adequate performance assessment program?

- To what degree do safety and environment policy and program, safety and environment requirements definition, compliance monitoring and reporting result in transfer of environment and safety considerations to field activities in an adequate manner?

- To what degree do quality policy and program, quality requirements definition, compliance monitoring and reporting result in transfer of quality considerations to specific activities in an adequate manner?

- To what degree do levels of decision making, assignments of responsibility and accountability, and influence of safety concerns result in effective risk based decision making related to specific activities?

a7. Budgets LTA:
Is the budget adequate not only for the safety group but also for related safety program aspects for which other groups in the organization have responsibility? (189)

a8. Delays:
Are safety program elements implemented in a timely manner? Are solutions to safety problems introduced early in the life cycle phases of projects? (189)
[Delays can and should be made known to management. If this is done and delay is a practical need, the delay becomes an assumed risk.]

a9. Accountability LTA:
Is line management held accountable for safety functions under their jurisdiction? If so, are there methods for measuring their performance? (198)

a10. Vigor and Example LTA:
Have top management individuals demonstrated an interest in lower level program activities through personal involvement? Is their concern known, respected, and reflected at all management and employee levels? (200)
[Do people tell stories of a manager's vigor in support of safety? If not, the manager's example may be LTA.]

MA3. Risk Assessment System LTA

Does the risk assessment system provide management with the information it needs to assess residual risk and to take appropriate action, if the residual risk is found unacceptable? Does the system also provide: (1) comparative evaluation of two or more systems; and (2) development and evaluation of methods supporting the hazard analysis process? (205)

MB1
MB2
MB3

MB1. Goals LTA

Are there high goals for policy and implementation criteria as well as specific goals for projects? Are the goals nonconflicting, sufficiently challenging, and consistent with policy and the customer's goals? (206)

MB2. Technical Information System LTA

Is the technical information system adequate to support the needs of the risk assessment system?
[Note other lower tier events included by transfer from SD1. Refer to SD1 section of this outline for write-up.]

MB3. Hazard Analysis Process LTA

Is the Hazard Analysis Process (HAP) properly conceptualized, defined, and executed? (225, 215, 234)

a1. Concepts and Requirements LTA:
Are the concepts and requirements of the HAP adequately defined? (237)

b1. Definition of Goals and Tolerable Risks LTA:
Have goals and tolerable risks been defined for both safety and performance and any conflicts between the two resolved? (237)

c1. Safety Goals and Risks Not Defined:
Do the goals state what degree of safety excellence should be attained and when? Are tolerable direct and indirect safety risks defined and actual risks quantified?

c2. Performance Goals and Risks Not Defined:
Have goals been set for performance efficiency and productivity? Have tolerable risks for lost efficiency and productivity been established and actual risks quantified?
[Such goals complement safety goals by requiring greater assurance of error-free performance.]

b2. Safety Analysis Criteria LTA:
Have the necessary criteria been specified and elements defined to adequately support the safety analysis program?

c3. Plan LTA:
Has a system safety plan been developed that describes "who does what and when" in analysis, study, and development? (238)

c4. Change Analysis LTA:
Has a specific change-based analytic method been established to review form, fit, or function of components and subsystems (including interfaces) upwards in a review process until no change is demonstrated? (59)

c5. Other Analytical Methods LTA:
Are other appropriate analytical skills available in the organization (or from a consultant) and are they used (e.g., Hazard Identification, Failure Modes and Effects, Fault Tree, MORT, Nertney Wheel, Failure Analysis, Human Factors Review, etc.)? (223, 228, 248)

c6. Scaling Mechanism LTA:
Has some reasonably clear-cut mechanism been established for scaling the seriousness/severity of prior events. Is there a mechanism to project past events to a scaled effort to evaluate current processes? (238)

c7. Required Alternatives LTA:
Does management require confrontation between alternative solutions in its bases for choices and decisions? (186, 208)

c8. Safety Precedence Sequence LTA:
Is the preference for safety solutions prioritized as: (1) Design, (2) Safety Devices, (3) Warning Devices, (4) Human Factors Review, (5) Procedures, 6) Personnel, and (7) Acceptance of Residual Risks (after considering the preceding six items)? (98, 225)

b3. Procedures Criteria LTA:
Are engineers and designers made aware of their limitations in writing procedures for operating personnel, for the need for selection and training criteria for operators, and of supervisory problems? (315, Appendix F)

b4. Specification of Safety Requirements LTA:
Have all applicable and appropriate safety requirements been specified, made available, and used? (260)
Consider whether the following documents have been adequately called out to the extent they are applicable:

c9. DOE (customer) requirements developed in-house.

c10. OSHA regulations that are law.

c11. Other Federal and National Codes by agencies other than the customer and OSHA.

c12. State and Local Codes applicable to the geographical area where the work is to be performed.

c13. Internal Standards developed within the organization to cover situations not addressed by outside requirements.

b5. Information Search LTA:
Is an adequate information search required? (262)

c14. Nature of Search LTA:
Does the nature of the search include incident files; codes, standards, and regulations; change and counterchange data; related previous analyses; and other comments and suggestions?

c15. Scope of Search LTA:
Is the search scoped in a manner that would seek information on problems from conceptual design, through construction and use, to final disposal?

b6. Life Cycle Analysis LTA:
Is there an adequate safety analysis which starts with planning and continues through design, purchasing, fabrication, construction, operation, maintenance, and disposal? (263, 225)

c16. Scope LTA:
Does the scope include not only the prime mission equipment, but also checkout and test equipment and procedures, facilities and operations, procedures for operation, selection of personnel, training equipment and procedures, maintenance facilities, equipment and procedures, and support equipment?

c17. Analysis of Environmental Impact LTA:
Is the life cycle analysis scoped to include an analysis of environmental impact which complies with all applicable requirements? (259)

c18. Requirement for Life Cycle Analysis LTA:
Is the requirement for Life Cycle Analyses (LCA) rigid enough to assure that a thorough LCA will be initiated during the planning stage?

c19. Extended Use Factors LTA:
Has sufficient consideration been given to special requirements, new problems, and other factors to be encountered if the facility/operation is extended beyond its original intended life?

a2. Design and Development Plan LTA:
Does the development phase provide for the use of the major safety results of the Concepts and Requirements Phase (MB3-a1)? Is the design a true representation of the developed criteria, definitions, specifications, and requirements? (267)
[Note that barriers and amelioration, analyzed separately in accident investigation, are part of the design process.]

b7. Energy Control Procedures LTA:
Is there an attempt, whether by design or procedure, to control energy to only that which is needed for the operation and to contain its interactions to the intended function?

c20. D/N Substitute Safer Energy:
Does the design use the safest form of energy that will perform the desired function?

c21. D/N Limit Energy:
Is the amount of available energy limited to that which will perform the operation without any unnecessary excess energy?

c22. Automatic Controls LTA:
Are there devices to automatically control the flow of energy and to maintain it in its operating mode? Is use of redundant design adequately employed? (267)

c23. Warnings LTA:
Are there clear, concise warnings for all situations where persons or objects might unintentionally interface with an energy flow? (268)

c24. Manual Controls LTA:
Are there manually-operated controls to maintain the proper energy flow during the normal mode or as a manual override of automatic controls?

c25. Safe Energy Release LTA:
In the event that the energy containment fails through normal flow channels, is there a designed-in route through which the energy can be safely released?

c26. Barriers and Controls LTA:
Are there adequate barriers included as part of the design, plan, or procedure? Do they separate energies and/or protect people and objects? (33, 268)
[Note other lower tier events included by transfer from SB2.]

b8. Human Factors Review LTA:
Has consideration been given in design, plan, and procedures to human characteristics as they compete and interface with machine and environmental characteristics? (273)

c27. Professional Skills LTA:
Is the minimum level of human factors capability, needed for evaluation of an operation, available and will it be used? (275)

c28. D/N Describe Tasks:
For each step of a task, is the operator told: When to act? What to do? When the step is finished? What to do next? (276)

c29. Allocation Man-Machine Tasks LTA:
Has a determination been made (and applied) of tasks that humans excel in versus those tasks at which machines excel?

c3O. D/N Establish Man-Task Requirements:
Does the review determine special characteristics or capabilities required of operators and machines?

d1. D/N Define Users:
Is available knowledge about would-be users defined and incorporated in design?

d2. Use of Stereotypes LTA:
Are checklists of stereotypes (typical, normal, expected behavior) used in design? (e.g., Is a control turned right to move a device to the right?) Are controls coded by size, color, or shape?

d3. Displays LTA:
Are displays used which can be interpreted in short time with high reliability?

d4. Mediation LTA:
Is consideration given to delays and reliability of interpretation/action cycles?

d5. Controls LTA:
Are controls used which can be operated in short times with high reliability?

c31. D/N Predict Errors:
Is there an attempt made to predict all the ways and frequencies with which human errors may occur, and thereby determine corrective action to reduce the overall error rate?

d6. Incorrect Act:
Have all the potential incorrect acts associated with a task been considered and appropriate changes made?

d7. Act Out of Sequence:
Has the consequence of performing steps of a task in the wrong order been considered and has appropriate corrective measures been made?

d8. F/T Act:
Is there an attempt to reduce the likelihood of operators omitting steps or acts which are required by procedure?

d9. Act Not Required:
Are all the steps that are needed to accomplish a task required in the procedures? Are only those steps in the procedure?

d10. Malevolence:
Are deliberate errors and other acts of malevolence anticipated and steps taken to prevent them or reduce their effect?

b9. Maintenance Plan LTA:
Is maintenance of an operation/facility given consideration during the conceptual phase and on through the rest of the life cycle? Is there an adequate maintenance plan? (311)
[Note other lower tier events included by transfer from SD3-a1.]

b10. Inspection Plan LTA:
Is inspection of an operation/facility given consideration during the conceptual phase and on through the rest of the life cycle? Is there an adequate inspection plan? (312)
[Note other lower tier events included by transfer from SD4-a1.]

b11. Arrangement LTA:
Does the design consider problems associated with space, proximity, crowding, convenience, order, freedom from interruption, enclosures, work flow, storage, etc.?

b12. Environment LTA:
Are people and objects free from physical stresses caused by: (1) facility physical conditions, (2) conditions generated by the operation, or (3) interactions of one operation with another?

b13. Operational Specifications LTA:
Are there adequate operational specifications for all phases of the system operation? (269)

c32. Test and Qualification LTA:
Is there a "dry run" or demonstration to prove out all associated hardware and procedures and to check for oversights, adjust for the final arrangement, and provide for some first "hands-on" participation?

c33. Supervision LTA:
Are there guidelines for the amount of supervision required, minimum supervisory capabilities needed, and responsibilities of operating supervisors?

c34. Task Procedures D/N Meet Criteria:
Do the procedures for each task meet selection and training criteria and applicable operating criteria? Are the procedures responsive to supervisory problems that can be addressed in written procedures?
(315, 269, Appendix F)

d11. D/N Fit With Hardware Change:
Are procedures revised, if necessary, to agree with changes in plant or equipment?

d12. Clarity and Adequacy LTA:
Does the writing style of the procedures give consideration to variations in reading skills and intelligence of intended users? Are procedures sufficiently scoped to cover all steps of a task and is enough information given about each step?

d13. D/N Verify Accuracy:
Are procedures rechecked with applicable criteria and tested for correctness under "dry run" operating conditions?

d14. Emergency Provisions LTA:
Do procedures give users clear instructions for all anticipated emergency conditions? Are instructions easy to perform under the stress of an emergency?

d15. Cautions and Warnings LTA:
Are dynamic and static warnings used when appropriate? Are they located at point-of-operation as well as in procedures? Is their meaning unambiguous?

d16. Event Sequence LTA:
Do procedures have steps performed in a sequence: (1) according to criteria; (2) that is safe; and (3) that is sufficient?

d17. Lockouts LTA:
Are lockouts called for where hazardous situations are encountered or created through use of procedures?

d18. Communication Interfaces LTA:
Do the procedures adequately convey their intended message? If procedures call for contact between users and other individuals, are these interfaces clear?

d19. D/N Specify Personnel Environment:
Do procedures specify maximum permissible levels of physical stresses imposed on the users?

c35. Personnel Selection LTA:
Are personnel selected on the basis of the capability (both physical and mental) which is necessary and sufficient to perform the operation? (327)

c36. Personnel Training and Qualification LTA:
Are personnel given all the training they need for the equipment and procedures they will be using? Do they demonstrate through "hands-on" use that they know how to apply the training properly? (327)
[Personnel training and qualification factors are considered in detail under SD5-d15.]

c37. Personnel Motivation LTA:
Do personnel want to perform their assigned work task operations correctly? (337)
[Personnel motivation factors are considered in detail under SD5-d17.]

c38. Monitor Points LTA:
Are there sufficient checkpoints in written procedures during an operation to assure that steps are performed correctly? (351)

b14. Emergency Provisions LTA:
Does the design of plant and equipment provide for safe shutdown and safety of persons and objects during all anticipated emergencies? (306)

b15. Disposal Plan LTA:
Is the design such that disposal problems and hazards are minimized when the facility or operation has served its useful life? (270)

b16. Independent Review Method and Content LTA:
Is provision made for thorough and independent safety review at preestablished points (e.g., milestones) in the life cycle process? Are the risk-reduction trade-offs documented? Is the technical competence of Review Board members properly scaled to the level of technology involved? (283, Tree of Exhibit 8)

b17. Configuration Control LTA:
Is there a formal program to assure adequate configuration control throughout the entire life cycle of the facility? Does the program allow for easy access for review of modified procedures, drawings, and other documentation? (270, Tree of Exhibit 3)

b18. Documentation LTA:
Are all types of documentation complete, up-to-date, and accessible to users? (271)

b19. Fast Action Expedient Cycle LTA:
Is there an existing method to bypass the usual delays in order to get an immediate correction for an imminent hazard or problem of significant consequences?

b20. General Design Process LTA:
Are commonly recognized good engineering practices, including safety, reliability, and quality engineering practices, adequately incorporated into the general design process? (281)

c39. Code Compliance Procedures LTA:
Are there written procedures to assure compliance with applicable engineering and design codes?

c4O. Engineering Studies LTA:
Where codes, standards, regulations, and state-of-the-art knowledge cannot furnish required design data, are engineering studies conducted to obtain the needed information?

c41. Standardization of Parts LTA:
Is there an attempt to use proven existing standardized parts where possible, or to design so as to encourage their use?

c42. Design Description LTA:
Does the design description provide all the information needed by its users in a clear and concise manner?

c43. Acceptance Criteria LTA:
Are acceptance criteria stringent enough to assure operability/maintainability and compliance with original design?

c44. Development and Qualification Testing LTA:
Is there adequate testing during development of a new design to demonstrate that it will serve its intended function? Does qualification testing assure that nonstandard components satisfy the acceptance criteria?

c45. Change Review Procedure LTA:
Does change review cover form, fit, and function on up the part-component-subsystem chain to a point where no change is demonstrated? Are there change dockets on drawings and at points-of-operation?

c46. Reliability and Quality Assurance (R&QA) LTA:
Is there an adequate reliability and quality assurance program integrated into the general design process? (282)
[In some organizations, the reliability and quality assurance functions are very specifically separated; other organizations combine them. Whether combined or separated, R&QA is a strong complement to safety. Close mutual support between safety and R&QA should be evident throughout the general design process.]

MB4. Program Review LTA

Do the Environment, Safety and Quality (ESQ) program reviews assure a planned and measured program, with low cost/high volume services, professional growth, and use of modern methods? (445)

a1. Definition of Ideals and Policy LTA:
Are there adequate ESQ policy statements and are the ideals of the SEQ programs articulated? Do these summarize what management should know (and require) the ESQ process? Do the ideals provide a base that measures the program and projects improvements?

a2. Description and Schematics LTA:
Are program ideals documented in operating manuals and schematics? Are program operating data available and evaluated? Are there outlines, steps, and criteria that substantially describe the ESQ programs?

a3. Monitoring, Audit, and Comparison LTA:
Is there a formal measurement system that compares actual performance with ESQ program ideals and objectives? (446)

a4. ESQ Program Organization LTA:
Are the programs organized with the necessary and adequate elements? (449)

b1. Professional Staff LTA:
Do ESQ personnel rate well by both ESQ and management criteria? Are they effective in both technical and behavioral aspects? Do they have good organizational status and are they educated, experienced, and promotable? (454)

b2. Management Peer Committees LTA:
Are special-purpose and ongoing committees and boards used to improve ESQ understanding and attitudes within scientific and engineering groups? Do these ongoing groups have a positive, action orientation toward real-life problems?

b3. Scope LTA:
Does the ESQ program scope address all forms of hazards, including anticipated hazards associated with advanced technological development and research?

b4. Integration LTA:
Is the staff support for ESQ integrated in one major unit rather than scattered in several places?

b5. Organization for Improvement LTA:
Is the ESQ program organized adequately to achieve the desired pace of ESQ improvement? (119, 209, 457) [Achievement of a breakthrough goal in accident reduction by an ESQ program requires clear goal definition and distinctive organizational effort, particularly by staff personnel.]

a5. Block Function and Work Schematics LTA:
Are charts and drawings of the full array of ESQ-related processes and functions adequate and reviewable?
[This may include provision of ESQ equipment, delivery of other safety reviews to point of need, and other safety-related functions, plus the schematics of various "upstream processes" to be audited or monitored.]

b6. Not Up-To-Date:
Are charts and drawings kept up-to-date?

b7. Incomplete:
Are all items that are needed for review included in the charts and drawings?

b8. Completion Criteria LTA:
Are criteria clear and specific as to what should be included in drawings and when they should be finished and revised?

a6. ESQ Program Services LTA:
Does management provide the supportive services and guidance needed at the lower organizational levels for an adequate ESQ program review?
[Note the transfer in of all lower tier event analysis from SD6.]

R. Assumed Risk

What are the assumed risks? Are they specific, named events? Are they analyzed and, where possible, calculated (quantified)? Was there a specific decision to assume each risk? Was it made by a person who had management delegated authority to assume the risk?
[The specific risk may be: (1) tolerably low (minor) in frequency or consequence, (2) high in consequence but impossible to eliminate, (i.e., hurricane), or (3) simply too expensive to correct when weighed against the risk consequences. The assumed risk events are shown elsewhere on the MORT diagram and flagged with a numbered "R" symbol.]

APPENDIX

MORT DIAGRAM CONSTRUCTION RULES

Introduction

In the MORT seminars, due note has been taken of the tendency of the person not previously familiar with analytical logic diagrams (trees) to be overwhelmed by the apparent complexity of the MORT diagram.

Actually, each element in a MORT diagram is largely self-explanatory and need not be any more complex than the subject being analyzed. The complete diagram should be recognized as a tool to assist the investigator in performing a task rather than a burden or additional workload.

MORT is a "universal tree" developed for an entire safety system discipline. When used as a kind of a "master checklist" to analyze a specific accident or evaluate an existing system, the user will usually see immediately that certain sections are or are not applicable to the particular situation being analyzed. Even in the branches that are used, there will usually be details at the lower levels that will not apply.

On the other hand, the user may find it helpful to further develop some branches of the more complex concepts of the diagram, so as to better isolate and evaluate an important aspect of the situation being analyzed.

The MORT diagram helps, in this case, by visually showing the elements present and serving to call the analyst's attention to any missing elements. Consideration of all significant elements required to evaluate the aspect is thus assured. The principle objective of this Appendix is to list the basic fault tree construction methods and rules used in construction of the MORT diagram, so the novice MORTician can continue the MORT tree branch to a greater level of detail, if needed, by adding on another "lower tier" in an orderly and logically correct manner.

General

The concept of fault tree analysis (FTA) was originated by Bell Telephone Laboratories in 1962 as a technique with which to perform a safety evaluation of the Minutemen Intercontinental Ballistic Missile Launch Control System. At the 1965 Safety Symposium, sponsored by the Boeing Company and the University of Washington, several papers were presented that expounded upon the techniques of FTA and its virtues as a method of system safety analysis. Presentation of these papers marked the first recognition that FTA could be successfully extended from the aerospace safety technology to nuclear reactor reliability, availability, and safety technology and to various other commercial operations.

As previously noted, fault tree construction is the logical development of the TOP event, using the technique of deductive reasoning (e.g., reasoning from the general to the specific) to progressively isolate the contributing factors to the fault event being considered. As the construction proceeds, each fault event is developed until a system component is identified for which a failure is considered primary or basic (i.e., no further breakdown of contributing factors to the failure is necessary for the fault tree construction).

A "fault event" then is the result of the logical interaction of other contributory factors or events. The graphical construction, which shows that fault event and its more basic factors, is termed a "branch" of the fault tree. A schematic representation of a typical fault tree is shown in Figure A-1.

Going from top to bottom on the diagram, events proceed from general to specific. Related events and constituents on one tier are joined by a line before being processed through one of the gates. A vertical line joins a general event at one level or tier, with its more detailed elements at the adjacent tier below. In its strictest form, all events on the same tier (even those not connected by a common line) should all be at the same level of logic or detail. Occasionally, elements on one tier will be listed ladder-style one under the other, because of space limitations. This arrangement should be considered at the same level of logic as if the elements were listed on a single horizontal tier. Examples of good and poor logic are shown in Figure A-2.

Use of Graphic Symbols

Graphic symbols used in fault tree construction are of two general categories: logic symbols and event symbols. For the most part, MORT uses the logic symbols, event symbols, and tree construction techniques that were developed by the Fault Tree Analysis technology.

Two basic logic symbols (logic gates) are used to interconnect the events that contribute to the specified main event (the TOP event). They are adequate for diagraming any fault tree, although several additional specialized logic symbols have been developed to reduce the time and effort required for analysis. The AND-gate provides an output event only if all input events occur simultaneously. The OR-gate provides an output event if one or more of the input events are present. (The OR-gate used is more precisely termed a nonexclusive OR-gate, distinct from an exclusive OR-gate that provides an output if one, and only one, input event is present.) MORT uses only one specialized gate, the CONDITIONAL-gate, shown in Figure A-3.

The three event symbols most frequently used are the RECTANGLE, CIRCLE, and DIAMOND. Additional specialized event symbols have been developed. MORT has developed several that are unique to MORT, such as the RISK symbol and the SCROLL symbol. They are shown in Figures A-3 and A-4.

The RECTANGLE represents a fault event resulting from the combination of contributory fault events acting through a logic gate. The CIRCLE designates a basic system component failure or input fault event independent of all other events. The DIAMOND symbol is used to depict an input fault event that is considered basic to the specific fault tree being constructed, however, the event described is not basic in the sense that laboratory or field failure rate data are available. Rather, the fault tree is simply not developed further either because: (1) the event is of insufficient consequence, or (2) the necessary information to extend the development is not available to the analyst. Events that appear on the tree as circles or diamonds are treated as primary events.

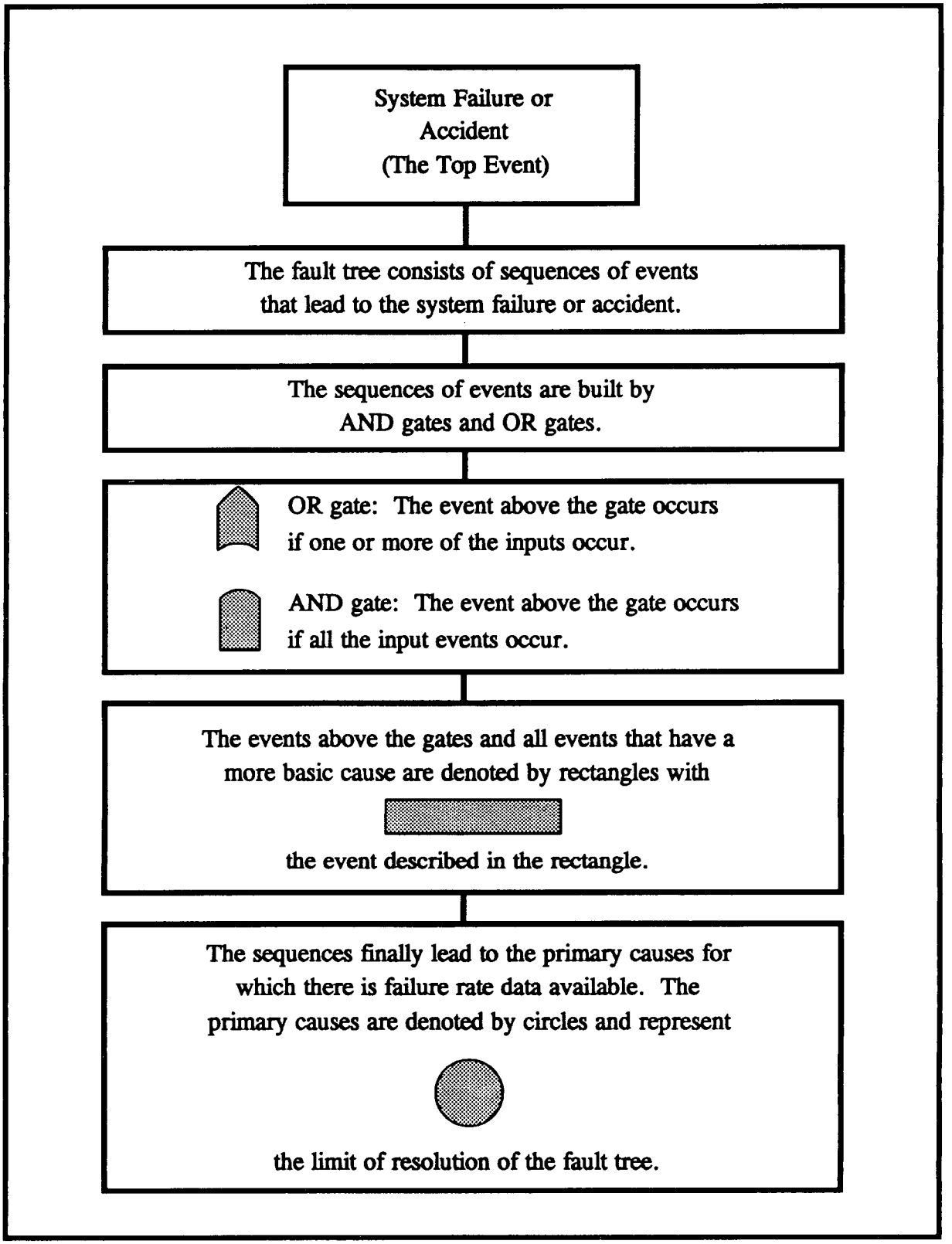
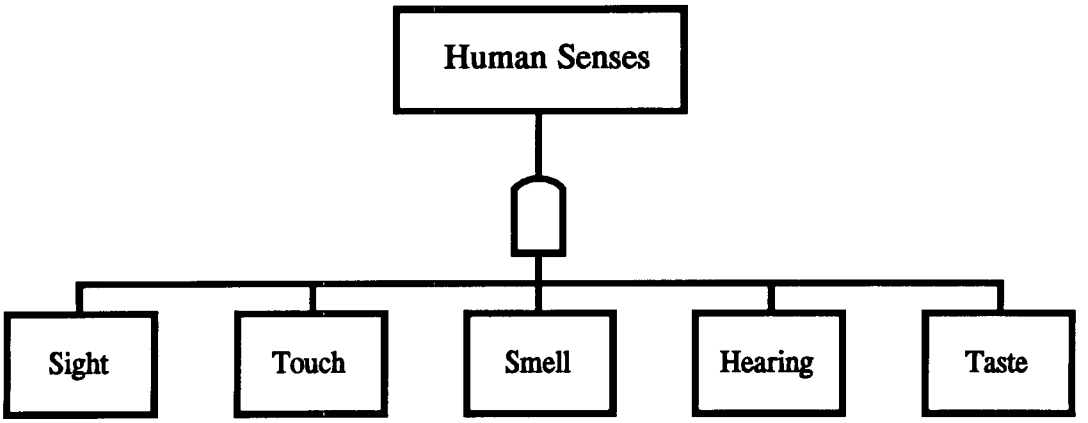
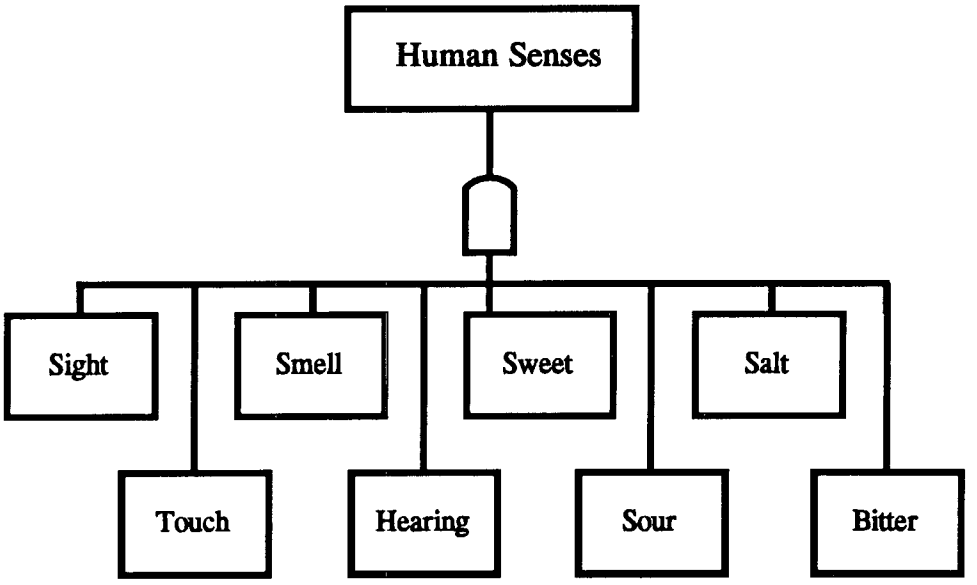


Figure A-1. Schematic of a Fault Tree

The following are examples of good and poor logic relating to the level of detail on one tier.

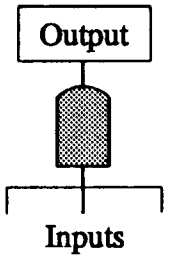


The above example represents good logic because all of the recognized senses are listed, but no extraneous detail is included on the same tier.



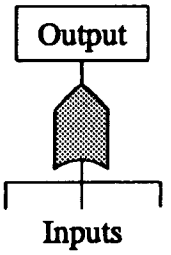
In this second example, poor logic has been used by listing the detailed constituents of taste on the same tier as the other four senses. If this level of detail is desired, the constituents would be better listed on a third tier under the appropriate sense.

Figure A-2. Examples of Good and Poor Logic



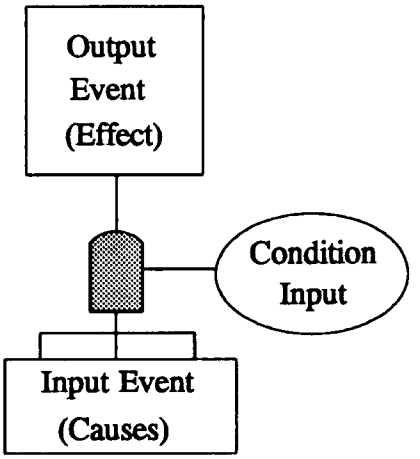
AND-Gate Symbol

Coexistence of all inputs required to produce output.



OR-Gate Symbol (Nonexclusive)

Output will exist if at least one input is present.

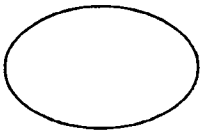


CONDITIONAL AND-Gate Symbol

(Can also be OR)

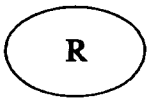
Input produces output provided conditional input is satisfied. Description of condition is written in the oval.

(Sometimes call a CONSTRAINED-Gate or an INHIBIT-Gate.)



CONSTRAINT Symbol

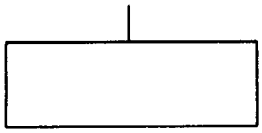
Applies conditions or constraints to basic logic gate or output event. When applied to basic AND-Gate or OR-Gate, creates special conditional gate such as Inhibit, Priority AND, Exclusive OR, etc.



RISK Symbol

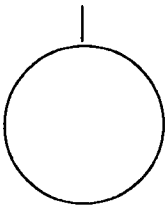
Indicates transfer to "Assumed Risk" branch of tree. Used for problems with no known or practical countermeasure.

Figure A-3. MORT Logic Symbols



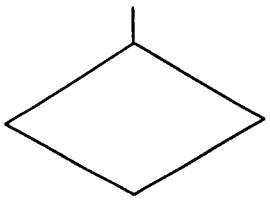
RECTANGLE

An event resulting from the combination of more basic events acting through logic gates.



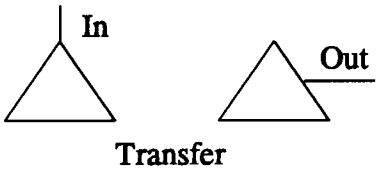
CIRCLE

An event described by a basic component or part failure. The event is independent of other events.



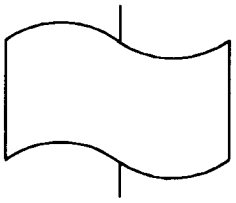
DIAMOND

An event not developed to its cause. Sequence is terminated for lack of information or lack of consequences.



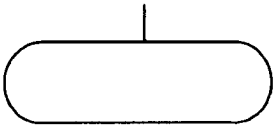
TRIANGLE

A connecting or transfer symbol. All tree construction below the "out" triangle is transferred in at "in" triangle location(s).



SCROLL

An event that is normally expected to occur.



STRETCHED CIRCLE

An event that is satisfactory. Use to show completion of logical analysis.

Figure A-4. MORT Event Symbols

The TRIANGLE shown in Figure A-4 is not a true event symbol, strictly speaking. Two triangles are used to accomplish a transfer of one part of the fault tree construction to another location. A line to the side of the triangle denotes all the tree construction below and including the event transfers out (in addition to its progression up the tree). A line from the triangle apex denotes an event is transferred into the section of the tree as input to the associated logic gate. The transfer-in and transfer-out triangles are uniquely identified to prevent possible confusion between transferred segments. The technique is used to reduce tree construction time and space.

Construction Rules

The methodology of fault tree construction can be succinctly stated in nine specific rules of construction. Their careful application by a fault tree analyst to a specific hardware-oriented system insures the resulting tree (logic diagram) will be orderly, properly time sequenced, logically correct, and suitable for evaluation, using quantitative, probabilistic analytical techniques. While not precisely applicable to the MORT diagram, they should be generally followed if an expanded depth of MORT analysis is needed.

Rule 1: State the fault event as a fault, including the description and timing of a fault condition at some particular time. Include the following:

a. What the fault state of that system or component is.
b. When that system or component is in the fault state.

Test the fault event by asking the follow two questions:

c. Is it a fault?
d. Is the what-and-when portion included in the fault statement?

Rule 2: There are two basic types of fault statements, state-of-system and state-of-component.

To continue the tree, apply these two rules:

a. If the fault statement is a state-of-system statement, use Rule 3.
b. If the fault statement is a state-of-component statement, use Rule 4.

Rule 3: A state-of-system fault may use an AND-, OR-, CONDITIONAL-gate, or no gate at all. To determine which gate to use, the input faults must be the following:

a. Minimum necessary and sufficient fault events.
b. Immediate fault events.

To continue, state the fault events input into the appropriate gate.

Rule 4: A state-of-component fault always uses an OR-gate.

To continue, look for the primary, secondary, and command failure fault events. Then state these three fault events:

a. Primary failure is failure of that component within the design envelope or environment.

b. Secondary failures are failures of that component due to excessive environments exceeding the design environment.

c. Command faults are inadvertent operation of the component because of a failure of a control element. (Note the distinction between fault and failure. An inadvertent command fault is correct system response to the gate input and is not a failure.)

Rule 5: No gate-to-gate relationships.

Rule 6: Expect no miracles; those things that would normally occur as a result of a fault will occur, and only those things. Also, normal system operation may be expected to occur when faults occur.

Rule 7: In an OR-gate, the input does not cause output. If any input exists, the output exists. Fault events under the gate may be restatement of the output events.

Rule 8: An AND-gate defines a causal relationship. If the input events coexist, the output is produced.

Rule 9: A CONDITIONAL-gate describes a causal relationship between one fault and another, but the indicated condition must be present. The fault is the direct and sole cause of the output when that specified condition is present. Inhibit conditions may be faults or situations (which is why AND- and CONDITIONAL-gates differ).

The MORTician expanding upon the MORT diagram does not have the same degree of concern with precise time sequencing as does the fault tree analyst. Lower tier expansion of the "universal" generalized MORT logic diagram is directed to obtaining a qualitative (not quantitative) evaluation of the MORT elements as "adequate" or "less than adequate" (LTA). Nonetheless, the MORTician who follows these nine rules can be sure his MORT event tree expansion is correct.

COMPLETED SSDC PUBLICATIONS

SSDC-1 Occupancy-Use Readiness Manual
SSDC-2 Human Factors in Design
SSDC-3 A Contractor Guide to Advance Preparation for Accident Investigation
SSDC-4 MORT User's Manual
SSDC-5 Reported Significant Observation (RSO) Studies
SSDC-6 Training as Related to Behavioral Change
SSDC-7B DOE Guide to the Classification of Recordable Accidents
SSDC-8 Standardization Guide for Construction and Use of MORT-Type Analytic Trees
SSDC-9 Safety Information System Guide
SSDC-1O Safety Information System Cataloging
SSDC-11 Risk Management Guide
SSDC-12 Safety Considerations in Evaluation of Maintenance Programs
SSDC-13 Management Factors in Accident/Incidents (Including Management Self-Evaluation Checksheets)
SSDC-14 Events and Causal Factors Charting
SSDC-15 Work Process Control Guide
SSDC-16 SPR0 Drilling and Completion Operations
SSDC-17 Applications of MORT to Review of Safety Analyses
SSDC-18 Safety Performance Measurement System
SSDC-19 Job Safety Analysis
SSDC-2O Management Evaluation and Control of Release of Hazardous Materials
SSDC-21 Change Control and Analysis
SSDC-22 Reliability and Fault Tree Analysis Guide
SSDC-23 Safety Appraisal Guide
SSDC-24 Safety Assurance System Summary (SASS) Manual for Appraisal
SSDC-25 Effective Safety Review
SSDC-26 Construction Safety Monographs

- 26.1 Excavation
- 26.2 Scaffolding
- 26.3 Steel Erection
- 26.4 Electrical
- 26.5 Housekeeping
- 26.6 Welding/Cutting
- 26.7 Confined Spaces
- 26.8 Heating of Work Spaces
- 26.9 Use of Explosives
- 26.10 Medical Services
- 26.11 Sanitation
- 26.12 Ladders
- 26.13 Painting/Special Coatings
- 26.14 Fire Protection
- 26.15 Project Layout
- 26.16 Emergency Action Plans
- 26.17 Heavy Equipment
- 26.18 Air Quality

SSDC-27 Accident/Incident Investigation Manual (2nd Edition)
SSDC-28 Glossary of SSDC Terms and Acronyms
SSDC-29 Barrier Analysis
SSDC-3O Human Factors Management
SSDC-31 The Process of Task Analysis
SSDC-32 The Impact of the Human on System Safety Analysis
SSDC-33 The MORT Program and the Safety Performance Measurement System
SSDC-34 Basic Human Factors Considerations
SSDC-35 A Guide for the Evaluation of Displays
SSDC-36 MORT-Based Safety Professional/Program Development and Improvement
SSDC-37 Time/Loss Analysis
SSDC-38 Safety Considerations for Security Programs
SSDC-39 Process Operational Readiness and Operational Readiness Follow-On
SSDC-4O The Assessment of Behavioral Climate
SSDC-41 Investigating and Reporting Accidents Effectively