26
3-3-82

①

I-1727

MASTER

SANDIA REPORT

SAND81-0636 • Unlimited Release • UC-41

Printed December 1981

Guidance for Implementing an Environmental, Safety and Health Assurance Program

Volume 5. A Model Plan for Institutional Accident Investigations

Charles A. Trauth, Jr., Andrew C. Ellingson

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

NOTICE

PORTIONS OF THIS REPORT ARE ILLEGIBLE. It
has been reproduced from the best available
copy to permit the broadest possible avail-
ability.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof or any of their contractors or subcontractors.

Printed in the United States of America
Available from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161

NTIS price codes
Printed copy: \$8.00
Microfiche copy: A01

PAGES 1 to 2
WERE INTENTIONALLY
LEFT BLANK

SAND81-0636
Unlimited Distribution
Printed January 1982

UC-41

SAND--81-0636 Vol. 5

DE82 011685

GUIDANCE FOR IMPLEMENTING
AN ENVIRONMENTAL, SAFETY AND HEALTH
ASSURANCE PROGRAM

Volume 5. A Model Plan for Institutional
Accident Investigations

Charles A. Trauth, Jr.
Andrew C. Ellingson
Special Projects Division, 1418

NOTICE

PORTIONS OF THIS REPORT ARE ILLEGIBLE. It

**has been reproduced from the best available
copy to permit the broadest possible avail-
ability.**

ABSTRACT

This is 1 of 15 documents designed to illustrate how an Environmental, Safety and Health (ES&H) Assurance Program may be implemented. The generic definition of ES&H Assurance Programs is given in a companion document entitled "An Environmental, Safety and Health Assurance Program Standard." The Standard specifies that the ES&H Staff of an institution shall establish policy and practices for accident investigation, and this document provides guidance for establishing an accident investigation program which provides such policy and practices. Unlike most other approaches, the scheme presented here utilizes a self-limiting tree to minimize investigative effort, permits "no-fault" accidents to have occurred, and does not automatically lead to the need for corrective action.

DISCLAIMER

This work was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

Acknowledgments

This work was sponsored by the Department of Energy (DOE), and among those many persons at the DOE who have been supportive and helpful, we would like to especially thank Messrs. Hal Hollister, John O'Connor, Mike Dix (now retired), and Ruben Pritchard for their support, encouragement, and patience. In addition, Mr. L. M. Jercinovic of Sandia National Laboratories is owed many thanks for his valuable technical inputs, discussions, and reviews, which greatly influenced the final form of this document--though, of course, we assume all responsibility for its deficiencies.

CONTENTS

	<u>Page</u>
Introduction	7
Background	11
Management Obligations in ES&H Areas	11
Criteria for Meeting Management Obligations	11
The Role of an Accident Investigation Program in Satisfying These Criteria	14
A Model Institutional Accident Investigation Plan	21
General Accident Investigation Policy	21
Full-Scale Investigations	26
Teams for Full-Scale Accident Investigations	26
Responsibilities of an Investigation Team	26
Phases of a Full-Scale Investigation	29
Restricted-Scale Investigations	62
Personnel Performing Restricted-Scale Accident Investigations	62
Investigator Responsibilities	62
Phases of a Restricted-Scale Investigation	63
Routine Investigations	74
APPENDIX A -- Standard ES&H Audit Checklist for Use in This Institution's Accident Investigation Program	77
APPENDIX B -- Institutional Routine Accident Investigation Form	81
Discussion	82
Notes and References	85

ILLUSTRATIONS

Figure

1	Institutional Structure and Generic Functions in ES&H Assurance Programs	8
2	ES&H Assurance Program Documentation	9
3	Human and Environmental Categories of Concern in ES&H Assurance Programs	12

ILLUSTRATIONS (Continued)

<u>Figure</u>	<u>Page</u>
4 Portions of a Fault Tree Relevant to the Example Accident	17
1* <i>Basic Program Analysis Steps Used in This Institution</i>	31
2 <i>Investigation of Failure To Identify Hazard(s)</i>	33
5 A Partial Generic Administrative ES&H Plan at the Working Level of Line Organization	35
6 The Substeps Involved in Taking Step 2--"Were Approved and Reviewed Controls Exercised over the Appropriate Risk Factors?"	39
3 <i>Investigation of Failure To Establish Controls</i>	40
7 Investigation Sequence for Example Accident Involving a Toxic Waste Pond	43
4 <i>Investigation of Failure To Use Controls</i>	45
5 <i>Generic Inputs into the Decision Whether New or Additional Controls Are Required</i>	47
8 A Partial Generic Fault Tree for a Simple Pressure System	52
9 First Three Steps Using a Fault Tree Logic in an Example Accident Investigation	53
10 Fourth Investigative Step in the Fault Tree	54
11 Possible Fifth Investigative Step in the Fault Tree	55
12 Steps in Fault Tree Approach Illustrating Self-Limiting Character	57
13 Temporal Events and Causal Factors Chart	59
6 <i>The Preliminary Substeps Necessary in Step 2 in a Restricted-Scale Accident Investigation</i>	64
7 <i>Generic Inputs into the Decision Whether New or Additional Controls over Routine Hazards Might Be Needed</i>	64

TABLES

<u>Table</u>	
1 <i>The Three General Types of Accident Investigations Required by This Institution</i>	22
1 An Illustration of a Restricted-Scale Accident Investigation	69

* Italicized figure and table numbers refer to those figures and tables that are part of the self-contained model. Roman numbers run consecutively through the nonmodel portion of this document.

A MODEL PLAN FOR INSTITUTIONAL ACCIDENT INVESTIGATIONS

Introduction

This is 1 of a set of 15 guidance documents designed to illustrate how an Environmental, Safety and Health (ES&H) Assurance Program may be implemented. The generic definition of ES&H Assurance Programs is given in a companion document entitled "An Environmental, Safety and Health Assurance Program Standard,"¹ often referred to as simply the Standard or the Program Standard. As suggested by the title, the Program Standard defines the functions and some of the structure needed within an institution for it to possess an "ES&H Assurance Program." The Standard is, on the other hand, relatively generic, flexible, and nonprescriptive--focusing on the general framework of ES&H Assurance Programs and on *what functions must be performed, not on how* these may be accomplished. This was done intentionally in order to provide maximum flexibility in implementation.

The ES&H Assurance Program Standard requires that an institution possess an independent "ES&H Staff." The remainder of the institution is considered "Line" and "Management" as suggested in Figure 1.* Generic functions of these three organizational components, as required by the Standard, are delineated in Figure 1. The Program Standard is more explicit about the nature of these functions. Specifically, Line organization *plans* are required--and these must reflect the *guidance* from the ES&H Staff, which itself must prescribe activities consistent with the Standard. In addition, the total program, planned by the ES&H Staff and approved by management, must be well defined. Thus,

* Management in this context refers to *upper* (or institutional) management, with the Line organization presumed to have its own managerial hierarchy--designated Line management.

Figure 1. Institutional Structure and Generic Functions in ES&H Assurance Programs

as illustrated in Figure 2, certain documentation must exist within the ES&H Assurance Program.

The intent of this series of guidelines is to provide an *illustration of this documentation*. No suggestion is intended that the program definition given in these guidelines provides a unique or even the most cost-effective means of performing the functions required by the Program Standard. Certainly, it is not intended that they are mandatory requirements stemming from the Program Standard.

We feel, however, an obligation to present one relatively specific program definition that effectively and (we believe) efficiently meets the requirements of the generic Program Standard in order to

Figure 2. ES&H Assurance Program Documentation

- Demonstrate the feasibility of the Standard,
- Provide a specific, well-defined program that can be tested for cost-effectivity, and
- Aid others in structuring programs that are consistent with the Standard.

It was precisely with this in mind that this set of guidance documents was prepared. The set, generically entitled "Guidance for Implementing an Environmental, Safety and Health Assurance Program," consists of the following documents (see also References):

I. Institutional Models and ES&H Staff Program Documents

- Volume 1 A Model Plan for Institutional Environmental, Safety and Health Assurance Programs²
- Volume 2 A Model Plan for Environmental, Safety and Health Staff Audits and Appraisals³
- Volume 3 A Model Plan for Environmental, Safety and Health Staff Review Activities⁴

- Volume 4 A Model Plan for Institutional Emergency Response Programs⁵
- Volume 5 A Model Plan for Institutional Accident Investigations⁶
- Volume 6 Model Documentation for an Environmental, Safety and Health Assurance Information System⁷
- Volume 7 A Model Plan for Institutional Environmental, Safety and Health Assurance Training Programs⁸

II. Model ES&H Staff Guidance Documents

- Volume 8 Model Guidelines for Line Organization Environmental, Safety and Health Committee Operations⁹
- Volume 9 Model Guidelines for Environmental, Safety and Health Analysis Activities¹⁰
- Volume 10 Model Guidelines for Line Organization Environmental, Safety and Health Audits and Appraisals¹¹
- Volume 11 Model Guidelines for Line Organization Environmental, Safety and Health Review Activities¹²
- Volume 12 Model Guidelines for Line Organization Environmental, Safety and Health Inspection and Monitoring Activities¹³
- Volume 13 Model Guidelines for Line Organization Environmental, Safety and Health Meetings¹⁴
- Volume 14 Model Guidelines for Utilizing Quality Assurance Support in Environmental, Safety and Health Assurance Programs¹⁵

III. Model Line ES&H Plans Which Reflect the Above Model Policies and Plans

- Volume 15 A Model Plan for Line Organization Environmental, Safety and Health Assurance Programs¹⁶

Background

Management Obligations in ES&H Areas

Because many hazards associated with today's operations or with new products themselves have the *potential* for impacting large numbers of people--and because many of those *at risk* cannot exercise direct control over that risk--*management* in today's environment *has an obligation to exercise controls that lead to an acceptable perceived level of risk by those at risk.*^{17,18} This may seem a debatable moral statement, but in many cases it has the force of law. In fact,

- When expending federal funds on programs that could have a public or environmental impact, the National Environmental Policy Act¹⁹ and subsequent regulation mandate elaborate procedures for public input designed to ascertain public acceptability.
- Portions of the Occupational Safety and Health Act²⁰ are designed to ascertain acceptability to employees.
- Most ES&H laws and regulations are designed to *express* societally acceptable levels of control and/or permit public input with the same end result.

Among other things, this basic management obligation requires that *management decisions consider*, to an appropriate extent, *ES&H objectives of employees and the public* on a routine and thorough basis. And, in addition, it becomes a management obligation to keep those at risk informed in a credible fashion about protection efforts being undertaken on their behalf.

The ES&H Assurance Program Standard was designed to assist in meeting these obligations of today's management. How it does this is described in more detail in References 17 and 18.

Criteria for Meeting Management Obligations

ES&H programs based on the ES&H Assurance Program Standard are intended to satisfy six basic generic criteria for "success" in ES&H programs. By design, the *intent* of these six basic criteria is to provide a *measure of program performance* that does not rely solely on accidents or incidents; so that one's *positive steps* to provide protection to humans and their environment can be used, in part, to describe one's *success*. These six criteria may be described briefly as follows. (More detail can be found in References 10, 17, and 18.)

I. Identify all significant hazards, specifically or by class.

"Hazards" are defined as *things* which have the *potential* for causing injury to or illness in humans or damage to the environment. The environmental and human categories in which possible impact is of concern are shown in Figure 3. These are discussed in detail in Reference 10. *Unusual* hazards are defined as those hazards not routinely encountered and accepted by the general public, while *routine* hazards are all others, that is, those that *are* routinely encountered and accepted by the general public. Either type of hazard may be *significant*.

Figure 3. Human and Environmental Categories of Concern in ES&H Assurance Programs

II. Define acceptable controls over the significant hazards.

Acceptable controls are developed through an assessment or analysis process (see Reference 10, Volume 9 in this series) which examines the ways (*events*) through which the potential *consequences* (that is, possible types and scope of injury, illness, or damage) of hazards may actually be incurred. Possible controls over the *factors* that affect how these events occur are then identified, and a collection of controls which appears to be cost-effective and acceptable to

persons who might be harmed, or whose environment might be damaged, is then selected.

III. Routinely use the controls as they have been defined.

One of the major contributory factors in accidents or incidents involving significant hazards is the failure to *use* defined controls. "Use," here, is intended to imply implementation, use, and/or maintenance. This is discussed in Reference 21. In order to verify control use, an adequate definition of each control is needed.

IV. Accommodate changing circumstances.

In a way, this is intended to imply only that activities for meeting Criteria I, II, and III are routinely and systematically reviewed and updated, as required. The possibility always exists that new hazards will be introduced into an operation or that factors affecting the nature or scope of, or the likelihood of incurring, consequences from existing hazards will be modified. When such changes do occur, their effect upon the adequacy and reliability of controls must be analyzed and appropriate adjustments made, when necessary.

V. Define an emergency response program consistent with existing hazards and routinely verify its reliability.

There is, of course, no zero risk. In the above framework, acceptable controls carry with them a connotation of *acceptable risk*. One must therefore assume that accidents or incidents will occur--and prepare accordingly. The ES&H Assurance Program Standard requires an emergency response program based on the understanding of the potential consequences that may arise from a hazard and the events (or sequences of events) that may lead to their realization that is gained in the performance of activities which satisfy Criterion II, above.

VI. Provide reliable independent evidence that Criteria I through V are satisfied.

This is the *assurance function* implied in the title of the ES&H Assurance Program Standard. Assurance is accomplished through independent reviews and audits which are efficiently based on information provided by those responsible for an operation or a product.

The primary intent of ES&H Assurance Programs is to provide independent credible *evidence* that Criteria I through V are properly

satisfied. These first five criteria are designed to provide a *systematic* means for the *management of hazards* and may be thought of as defining the objectives of a *control subprogram* of the total ES&H Assurance Program, including both *direct controls* over hazards and *indirect administrative controls*. The latter are designed to provide a management system in which the direct controls are *defined*, and are *routinely used*, and which generates *verifiable evidence* that this is the case.

Assurance is then provided by an overlay subprogram which *verifies* the *adequacy* and *use* of the controls using the verifiable evidence just described. Specifically, *adequacy* is typically verified through document *reviews* (of plans, procedures, etc.), while the *use* of the controls is verified through *audits* and *monitoring actions*. Independent reviews by the institutional ES&H Staff form the basis for credibly reporting on the positive efforts made to protect humans and their environment. In addition, data maintained by the ES&H Staff form a hypothesis about institutional performance that may be efficiently verified by statistical sampling methods by external agencies, as appropriate. The efficiency of performance verification sampling by both the ES&H Staff and external agencies is discussed in Reference 22.

The Role of an Accident Investigation Program in Satisfying These Criteria

Accident investigations can support the achievement of all of the above program criteria, depending upon the circumstances surrounding the accident and the investigation findings. Most serious, or potentially serious, accidents appear to occur as a result of a failure to recognize a hazard(s), a failure to define "adequate" controls, or a failure to actually implement or use the controls--either initially or because of changes that have taken place.²¹ If the hazard is recognized and controls are defined and actually exercised over the factors upon which the likelihood of the occurrence of the accident's failure mode depends, then the accident frequency (in this failure mode) should depend directly upon the reliability of the controls.¹⁰ Under these circumstances, one is faced only with the question of whether the controls are acceptable in view of the occurrence of the accident. Thus, depending upon the situation, an accident investigation will assist in future achievement of Criterion I, II, III, or IV. When failure to prevent or mitigate an accident is found to be due, in part,

to inadequacies in emergency response (viewed as a control program), Criterion V is addressed.

Whether or not program deficiencies are found to exist which led to a failure to recognize hazards, define acceptable controls, use them, or respond to emergencies, the accident investigation also provides an independent measure of program performance--supporting the achievement of Criterion VI.

In ES&H Assurance Programs, the presumption is made that the first five (the control) criteria of the previous section are direct indicators of the generic positive steps that must be taken to achieve an acceptable level of protection. Only with some assumption of this type can one actually manage hazards from a positive perspective. Evidence supporting this assumption is discussed in Reference 17. The more specific program elements associated with ES&H Assurance Programs are designed to yield an ES&H program that satisfies the six criteria, above. Thus, accidents are, in effect, either "acceptable" (at the time of their occurrence) or they occur because of a program deficiency that caused a failure to satisfy the criteria of the previous section. Hence, accident investigations in ES&H Assurance Programs stress examination of program elements in a form structured around the six management system criteria and ES&H plans which detail how they are satisfied (see Reference 16, for example).

A simple accident example may serve to illustrate some of these points. Imagine a pond of liquid waste containing a toxic substance that is part of process effluents from a plant of one kind or another. The intent of the pond is to provide a repository for the toxic substance while the water portion of the effluent stream evaporates. This waste treatment process ultimately leads to a concentrated sludge containing the toxic substance that is then further treated by biological processes irrelevant to this discussion.

As part of the scenario, imagine that the pond was ostensibly designed to control seepage and spills, largely because it is located on a bluff overlooking a river which provides both a source of potable water and irrigation water for the downstream rural population. The accident sequence envisioned in this setting is the subsidence of a portion of the bluff due to an earthquake, a subsequent rupture of the pond, and the spillage of the liquid waste and toxic substance into the

river. The further assumption is made that the operation of the pond is conducted in the context of an ES&H Assurance Program, so that in particular, an ES&H plan exists for this operation.

This scenario has two consequences: it identifies the generic sequence of events that led to the contamination of the river (which is normally determined by the accident investigation--and not always so easily), and it directs the investigation into program areas related to the required contents of the ES&H plan.¹⁰ Thus, investigators may ask as a *first question* whether the hazard¹⁰ (the toxic substance, in this case) was identified. If so, this will be formally done in the ES&H plan. The intent of the pool itself suggests that this was done, but it must be checked because changes in personnel, and so forth, that may take place over a period of time have been known to lead to the loss of recognition of hazards that were recognized at the outset of an operation (see Reference 21 for an example). Assume that the hazard was formally recognized as a part of the ES&H plan. Then, the next series of questions addresses whether acceptable controls were defined. In particular, the *second question* that needs to be asked is whether the potential impact on downstream water supplies was appreciated. Again, reference to the ES&H plan will determine the answer to this question,¹⁰ and for this example, it is assumed that an affirmative answer is obtained.

The *third question* that must be answered is whether the failure mode and the risk factors upon which it depends were known.¹⁰ Thus, in particular, was the event sequence "river contamination," "rupture," and "subsidence" recognized and was "earthquake" identified as a possible factor that would cause subsidence. In asking such a question, the assumption is, of course, that the investigation has determined the event sequence and risk factors involved in the accident, and, as suggested above, this may require considerable investigative effort. Nevertheless, the structure of ES&H Assurance Programs leads the investigation efficiently into the examination of failure modes and the factors upon which the likelihood of their occurrence depends.

In answering the third question, direct reference to the ES&H plan is again appropriate. In the analysis portion of the plan for the operation, one anticipates some logical structure relating undesired events (in this case spillage of the toxic substance into the river) to factors upon which the likelihood of these events depends.¹⁰ Thus, for

example, one might find a fault tree¹⁰ such as that partially shown in Figure 4.

Figure 4. Portions of a Fault Tree Relevant to the Example Accident

In Figure 4, it is imagined that the ES&H analysis abstractly considered the failure mode and risk factor that were involved in the example accident. This, of course, may not always be the case. Thus, in a general way, to answer the third question the investigation must determine whether

- Spillage into the river was considered as a failure event,
- Pond rupture was considered as a failure event that may be involved in spillage,
- Bluff subsidence was identified as an event that might lead to pond rupture, and
- An earthquake was recognized as a factor that might cause bluff subsidence.

If the answer to any of the three questions posed in this narrative is "No," then the program elements that should have supported the accomplishment of the functions necessary for an affirmative answer are

investigated. In this way, not only the basic physical failure mode associated with the accident is sought, but also the basic programmatic elements that may have permitted it to occur are found. How this may be accomplished is illustrated in the next few sections of this document--that it may be accomplished at all is due to the nature of the programmatic framework of ES&H Assurance Programs that links program elements to the satisfaction of the six management system criteria of the previous section.

Not all accidents will be ascribable to program deficiencies. For example, one perfectly reasonable outcome of an investigation of the above example accident might be that subsidence as a result of earthquakes was *not* considered a reasonable mode of failure because all evidence of past geological activity was contraindicative. If all prior evidence indicated that subsidence was, at best, a rare event, an investigative finding that the accident was not reasonably foreseeable would be proper--and even though no controls were instituted, the evidence would indicate that this was an acceptable choice.

To proceed with the example, imagine that Figure 4 is representative of the ES&H analysis of the operation--so that the relevant failure mode and risk factor (earthquake) were known prior to the accident. The *fourth question* is: What controls were instituted to limit the likelihood that an earthquake would cause a release of the toxic substances into the river? Since one cannot prevent, or even control, the frequency and/or intensity of earthquakes, the controls will be in the nature of mitigation actions. Some examples might include

- Design of the pond to withstand subsidence that might be caused by maximum credible 50-year earthquakes,
- The construction of a separate berm near the river to contain spills, should they occur, or
- The construction of a dam across the river so that contaminated water could be collected and decontaminated before release to the downstream public.

The first is intended to prevent the main rupture event itself, while the latter two are intended to mitigate the effects of the rupture of the pond. They may, of course, be used in combination.

To simplify the discussion, assume that the first control, design to withstand subsidence that might be caused by a maximum credible

50-year earthquake, was elected and specified as a part of the ES&H plan. Then one or more of three logical possibilities exists:

- The design was inadequate, in spite of its intent, to withstand the subsidence that might be caused by a maximum credible 50-year earthquake,
- The design was not properly implemented, or
- The intensity of the earthquake that actually occurred exceeded that estimated to be associated with a maximum credible 50-year earthquake.

It is clear that the accident investigation must determine the magnitude of the earthquake in order to begin to accept or reject these possibilities. If the magnitude of the earthquake exceeded that of a maximum credible 50-year earthquake, and if physical and documentary evidence exists that the design was implemented, then a finding that acceptable controls were defined and used is appropriate. The accident, in particular, was not reasonably foreseeable and would be regarded as *acceptable* at the time of its occurrence and *blameless*. If, on the other hand, the intensity of the earthquake was less than that presumably designed for, then either the design itself or its implementation was inadequate. Which of these possibilities existed must be determined by the investigation, and then programmatic reasons for the deficiency must be sought. Program elements exist in ES&H Assurance Programs which address design adequacy and design implementation.

Thus, as alleged, either one has defined and is using acceptable controls, or there are particular program deficiencies involved in the accident. An understanding of the accident and a comparison of this knowledge with performance required in ES&H Assurance Programs permit one to determine which situation obtains, and if the latter, what program faults need to be corrected. This in turn leads to a program that more nearly satisfies the first five of the criteria of the previous section and presents evidence of the corrective action taken in the program to bring it into closer compliance with these criteria (supporting Criterion VI). If, on the other hand, acceptable controls are found to have been defined and used, then a presumption exists that the accident was acceptable (at the time of occurrence) and that it was blameless. The only question that arises in this case is whether the definition of "acceptability" should be changed in view of the occurrence of the accident. As an illustration, suppose that in the above

example the magnitude of the earthquake exceeded best estimates of the maximum credible 50-year earthquake. Then, either

- Past estimates were wrong or
- The earthquake that occurred was a rare event.

If the former, then better estimates must be gotten and appropriate control actions taken--where, in this case, the definition of "acceptable" has changed. If the latter, no new or additional controls may be necessary since the likelihood of a similar event during the remaining lifetime of the operation would be very low--so that the previous controls might still be regarded as "acceptable."

The Environmental, Safety and Health Assurance Program Standard specifies that "The ES&H Staff shall establish policy and practices for the investigation of all incidents involving significant injury or damage or having a potential for significant injury or damage." This policy is reflected in the companion document "A Model Plan for Institutional ES&H Assurance Programs."² How such a generic institutional policy might be translated into a specific, well-defined program for the investigation of accidents that is consistent with both the requirements and the spirit of the Standard is discussed in this document. In a given institutional setting, a document of this sort, but more explicit regarding institutional entities and policies, would form part of the total implementing policy for an ES&H Assurance Program of the institution.² In the next section, a model accident investigation program is given in italics, while comments about it occur in roman type.

A Model Institutional Accident Investigation Plan

It should be pointed out that the following is only a model approach to accident investigation that is consistent with the ES&H Assurance Program Standard¹ and with the other guidance documents for implementing ES&H Assurance Programs. Other approaches to accident investigation policy would certainly be possible, but whatever approach is chosen, it should, to be most cost-effective, have certain characteristics, including

- Flexibility at several levels. Not all accidents require the same investigative effort, and precise policies *a priori* are, at best, difficult to define. Professional ES&H personnel should always have some latitude in determining what efforts are needed and who should undertake them.
- Ease of use. Any approach should be well-structured, take maximum advantage of existing ES&H program efforts and data, be easy to implement against the background of existing program efforts, and be easily learned.
- A structure that naturally leads to the identification of both technical and programmatic oversights that were involved in the accident.

We believe that the approach described has these characteristics.

General Accident Investigation Policy

An accident is defined as any unplanned event that has occurred that caused, or had the potential for causing, injury to or illness in employees or the public, or damage to the environment (including Institutional property). It is the policy of this Institution that all accidents will be investigated, documented, and reported to the ES&H Staff promptly. The scope, intensity, and duration of an accident investigation should depend upon the nature of the hazard(s) involved and the nature of the accident, according to the requirements given in Table 1 as interpreted by the ES&H Staff. Specific policy requirements for the performance of each type of accident investigation shown in Table 1 are given in subsequent sections. Throughout, routine hazards are those routinely encountered and accepted by the general public, while unusual hazards are all others. Guidance for making this determination is given in Institutional policy for the performance of ES&H

Table 1

*The Three General Types of Accident Investigations
Required by This Institution*

<i>Type of Investigation</i>	<i>Investigating Responsibilities</i>	<i>General Criteria for This Type of Investigation</i>	<i>Generic Effort Required (See Remaining Sections for Specifics)</i>
<i>Full Scale</i>	<ul style="list-style-type: none"> Team Appointed by the President with ES&H Staff Review Responsibility 	<ul style="list-style-type: none"> Involving Either an Unusual Hazard with Real or Potential Significant Impact, or a Routine Hazard with a Real Significant Impact, That Extends beyond the Work Site 	<i>Thorough Analyses of the Accident and the Program</i>
	<ul style="list-style-type: none"> Dedicated, Formal Team Appointed by Responsible Department* Management, with ES&H Staff Approval of Investigation Results 	<ul style="list-style-type: none"> Involving an Unusual Hazard with Real or Potential Significant Impact Restricted to the Departmental Work Site 	
<i>Restricted Scale</i>	<ul style="list-style-type: none"> Team or Individual Appointed by Responsible Department Management, with ES&H Staff Approval of Investigation Results 	<ul style="list-style-type: none"> Involving a Routine Hazard with Only Potential Significant Impact Beyond the Work Site and/or with Real Significant Impact Restricted to the Work Site 	<i>Appropriate Program Analysis (Restricted to Departmental Functions) with a Less Formal Accident Analysis Than Required Above</i>
<i>Routine</i>	<ul style="list-style-type: none"> First Line Supervision** 	<ul style="list-style-type: none"> Involving a Routine Hazard with Only Potential Significant Impact Restricted to the Work Site Involving Either an Unusual or Routine Hazard Judged to Have No Potential for Significant Impact 	<i>Completion of Standard Accident Occurrence Form (Appendix B)</i>

*"Department" is used throughout the model of References 2 through 16 to denote the "working level" Line organization in which direct responsibility for hazard control actions is required by the ES&H Assurance Program Standard.

**"Supervision" is intended as a generic term for first-level management, reporting to the "Department" (see Reference 2, for example).

analyses. "Significant," as the term is used in Table 1, implies that the accident caused (Real) or had the potential for causing (Potential) impacts of the form

- Death; or serious injury, or serious illness requiring, or likely to require, hospitalization,
- Loss of more than \$50,000 in facilities, equipment, and/or materials, or
- Any serious irreparable loss or damage to the environment, or any reparable damage to the environment whose cost of repair exceeds \$50,000.

In the event of any accident that is not clearly of a type requiring only a routine investigation, the Emergency Coordinator in the ES&H Staff (Extension HELP) is to be notified immediately by the responsible project leader or manager. The ES&H Staff management will determine the type and scope of the investigation required and by whom it should be performed.

In the case of accidents requiring full- or restricted-scale investigations, the authority of the accident investigation team or individual begins immediately upon appointment. Until then, the site of the accident is to be preserved in as nearly a pristine condition as is permitted by necessary emergency response actions. Emergency response policy is defined in the Institutional Emergency Response Plan, according to which emergency responsibilities are shared by Department personnel, the ES&H Staff, and the emergency response structure. While recognizing that zero risk is an unrealistic goal, it is the policy of Institutional management that all efforts should be made to limit risk to levels acceptable to those at risk. To this end, hazardous conditions that might lead to accidents are to be routinely sought and corrected by each Department in accordance with the ES&H Staff directives that state implementing policy for inspection activities, ES&H analyses, and Departmental assurance activities.

For obvious reasons, different types of accidents should require different investigative responses. However, all accidents should be studied and reported, and both technical and programmatic "basic causes" sought, in order that an institution learn from its own and others' experiences the maximum amount about hazards, their potential impact, failure modes, the reliability of controls, and the efficacy of

programs. On the other hand, such learning is facilitated by a framework in which acceptable, blameless accidents are possible--for there is a tendency to minimize accident reporting when the inevitable outcome of an accident is a penalty. In this respect, ES&H Assurance Programs provide an ideal framework for accident investigation since their very nature permits acceptable, blameless accidents to have occurred, as illustrated in the previous section.

The model above prescribes three possible levels of investigation that are generally consistent with the requirement of the ES&H Assurance Program Standard that ES&H effort should depend upon the seriousness of the potential consequences of the hazards involved. In this model, stress is placed both on "real" seriousness and on the possible perceptions of seriousness that might be held by the public when unusual hazards, not routinely encountered or accepted by the public, are involved. Clearly other approaches exist to defining policy that is consistent with this requirement, and the model presents only one example. Two principles that should be adhered to, however, are

- The involvement of the ES&H Staff in determining the level of effort and
- Consistency with institutional ES&H analysis policies.¹⁰

The investigation of accidents (or incidents, as the term is often used) must be placed in proper perspective with other closely related components of an institutional ES&H Assurance Program--particularly those for emergency response and for hazardous condition investigation. The investigation of hazardous conditions (discussed in both "Model Guidelines for Line Organization ES&H Committee Operations"⁹ and "A Model Plan for Line Organization ES&H Assurance Programs"¹⁶) is primarily a responsibility of the working level Line organization in which the hazardous condition exists, and the ES&H Staff organization provides guidance and may assist or participate. On the other hand, when an accident has occurred, or warnings that an accident may be imminent are received, the Emergency Response Program (discussed in both "A Model Plan for Institutional Emergency Response Programs"⁵ and "A Model Plan for Line Organization ES&H Assurance Programs"¹⁶) provides those immediate actions which are necessary to limit the effect of the accident or prevent its occurrence. This is a function for which emergency response personnel, the ES&H Staff, and the working level Line organization all have defined responsibilities. The accident investigation

functions discussed in this document consist of those actions taken *after* an accident to determine both its technical and programmatic causes and should

- Be appropriately scaled to the seriousness, or potential seriousness, of the accident or its perceived acceptability,
- Be initiated as soon as possible after an accident,
- Evaluate the need for "corrective action," and
- Recommend, as appropriate, how similar accidents might be controlled or mitigated in the future.

In accordance with the requirements of the ES&H Assurance Program Standard, the ES&H Staff organization is responsible for developing both the emergency response program and the accident investigation program, for training those with assigned functions in these programs, and for periodically evaluating these programs.

Full-Scale Investigations

Teams for Full-Scale Accident Investigations

The responsibility for conducting any full-scale accident investigation is assigned to a team of individuals. The management of the ES&H Staff organization is to select team members for each accident that, in its judgment, requires a full-scale investigation team. This is to be done immediately after the occurrence of the accident. The performance of the team is, then, the responsibility of the President of this Institution or the responsible Department manager, as required in Table 1. For full-scale investigations, no team members should come from the responsible Department. At least one of the team members selected must have received training, provided by the ES&H Staff organization, on the methods and techniques of accident investigation based on the policy in this document. Other team members are selected on the basis of the specialties pertinent to the particular accident. One of the team members is designated by the President or the Department Manager, as appropriate, as Chairman and is assigned responsibility for managing the investigation. Team members are expected to devote their time on a priority basis, as required, until the investigation is completed.

The investigation team is given authority to call on applicable Institutional organizations and individuals for priority technical and administrative assistance. The assistance may include the conduct of tests, clerical efforts, photographic work, technical writing, or any other support deemed necessary by the Chairman of the accident investigation team.

Responsibilities of an Investigation Team

Immediate Actions -- *The first action of the accident investigation team is to arrange for the securing of the accident area, to the extent that this has not been done by the emergency response program and is consonant with community needs. This action must be taken to preserve documentation of all necessary evidence for subsequent investigation efforts. Area security may not be removed without the written permission of the Chairman of the investigation team unless otherwise prescribed in emergency response arrangements with external agencies.*

The next action of the investigation team is to photographically record the accident site, especially if there is any possibility that

evidence will be lost due to external forces (such as weather, community activity, and so forth). When the remains of an accident must be removed from public areas, they must be collected and labeled in accordance with their location in site photographs.

The third action of the accident investigation team will be to identify, and obtain statements from, witnesses. All persons who were involved in, or observed, the accident who are able to make statements should be included.

The fourth action of the team is to determine what arrangements for technical and administrative support are required and make arrangements accordingly.

The model policy given in this section stresses the importance of thoroughly and independently examining accidents that were or could have been serious ("significant"). The appointment of an independent, qualified team responsible directly to the President of the institution, or overviewed by the ES&H Staff, with powers to control the preservation of possible evidence (subject to limitations imposed externally) and to call upon experts, as needed, is a first step in obtaining an open, fair investigation. When effects or potential effects of an accident involving an unusual hazard are restricted to a single work site, the investigation is conducted by a team appointed by the responsible working level Line organization management--otherwise an institutional investigation team is required when a full-scale investigation is deemed appropriate.

Although each serious, or potentially serious, accident is different from all others and thus requires different investigation activities, there are important actions which must be taken in any full-scale accident investigation at the earliest possible time in the investigation sequence. Whenever possible, the first step should always be to maintain all equipment and material in its immediate postaccident condition until the investigation team is certain that all conditions are known and recorded. The movement of any item before its position has been documented may destroy an important bit of evidence. As already noted, this area security must begin under the emergency response program, but it must be verified by the investigation team, and the team should have the only authority for releasing it if the accident occurs onsite. Authorities for offsite accidents should be delineated in

emergency response arrangements with appropriate agencies and should address site preservation.

Other actions must be taken as soon as possible after an accident, since area security cannot prevent such changes as those caused by the weather (if the scene is outdoors) or may not be capable of preserving a public site. A photographic record is important for this reason, and picture-taking should be initiated immediately. By the same reasoning, witnesses must be identified and statements from them recorded before a lapse of time can affect their memory of the events involved in the accident.

Next in order of priority is planning for the investigation. The team must make arrangements for such administrative items as filing space, secretarial assistance, and meeting facilities. Also, actions should be initiated on obtaining the assistance of appropriate specialists and on arranging for pertinent physical and material testing, although these actions may continue throughout the investigation as various facets of the accident come to light.

Full-Scale Investigation Planning -- A full-scale investigation (after the immediate actions prescribed above) is to be divided into four phases:

- Data collection,
- Program analysis,
- Physical accident analysis, and
- Reporting.

Because program analysis, data collection, and accident analysis are logically intertwined, these activities should be carried on simultaneously to a large extent as prescribed in Institutional policy given below. A brief plan should be prepared covering these four phases of the investigation. It should be modified, as appropriate, as the investigation proceeds.

Conducting and Reporting a Full-Scale Accident Investigation -- The accident investigation team is responsible for conducting the investigation in accordance with the plan developed. The results are to be presented to the President of this Institution, the Vice-President of the ES&H Staff, and the responsible Department manager in the form of a formal, written accident investigation report. The

policy on each phase of the investigation presented in the next section is to be rigorously adhered to.

Phases of a Full-Scale Investigation

Data Collection -- Data collection consists of gathering physical evidence through observations, inspections, photographs, measurements, material analyses, documents, and statements of witnesses and organization personnel and of gathering programmatic information about the nature of the operation or product involved. During the early stages of the investigation, an emphasis on recording all physical information, even where the relationship of the information to the accident is not clear, is required, as delineated in the previous section. The nature of subsequent data collecting activities is to be determined by the course of the investigation as indicated below.

While studying the next two sections, it should be noted that if the investigation team is trained in the various aspects of the ES&H Assurance Program, particularly in the conduct of ES&H audits^{3,11,22} and the performance of ES&H analyses,¹⁰ the data collection activity can be much more efficient. The structured approach of the ES&H Assurance Program provides a framework for the efficient collection of data and allows for early determination of what is important.

Program Analysis -- Program analysis activities are designed to determine whether ES&H program deficiencies were responsible in whole or in part for the accident. The sequence of program analysis efforts should follow that required in ES&H planning efforts, as described in ES&H Staff policy for the performance of ES&H analyses. As required by that policy, the Departmental plan should first identify significant hazards; then, analyze and specify acceptable controls over those hazards; and finally, present an administrative plan to assure use of the controls that have been developed. The program analysis for accident investigation should follow this same sequence but should limit itself to those hazards involved in the accident and evaluate in detail only where these basic steps are found to be inadequate.

Since one purpose of a full-scale accident investigation is to determine whether there was any program failure that prevented the achievement of an acceptable level of protection, there must be a program analysis which determines whether there were any program inadequacies that contributed to the occurrence of the accident. Better

physical controls (e.g., relief valves) may be needed to limit the frequency of future occurrences, as appropriate, but confidence in the adequacy and use of physical controls is gained through the exercise of program controls in ES&H Assurance Programs (see, for example, Reference 17).

Evaluation of a program is typically accomplished through an audit/appraisal function,^{3,11,22} and a form of audit/appraisal may therefore be used in accident investigations for this purpose. An audit/appraisal conducted in conjunction with a full-scale accident investigation will differ from the more general type of audit/appraisal in two respects:

- It will be limited, as much as possible, to the portions of the ES&H program involved in the accident and
- The program elements to be evaluated at each step in the audit will tend to be dependent upon the results of previous steps.

Program audits, as they are defined in ES&H Assurance Programs (see References 3, 11, and 22) are not difficult or costly because of their well-defined and highly structured nature, and in the context of accident investigations are even easier because they are restricted to program areas relevant to the accident that has occurred. Thus, in both full-scale and restricted-scale investigations (described later), appropriate portions of an institution's program must be audited. As with other audits, audit techniques that are useful in this program analysis portion of the accident investigation include document reviews, observation, and interviews. To promote cost-effectivity, the document reviews are of prime importance, since they deal with the evidence provided by the ES&H Assurance Program itself. Documents providing evidence for the program analysis phase of the investigation may include

- The institutional ES&H Assurance Program Plan,²
- The working level ES&H Assurance Plan^{10,16} (this refers to the plan for the working level organization in which the accident occurred. The plan includes both the administrative plan for the organization and the ES&H analyses for the identified significant hazards),
- The institutional emergency response program,^{4,16}
- Assurance reports, including inspection,¹³ monitoring,¹³ and review reports;^{4,12} internal¹¹ and external³ audit reports; and program evaluation reports;^{2,3} and

- Administrative records, including ES&H meeting records,¹⁴ training records,⁸ records of permits issued, and hazard report forms.^{9,13}

The program analysis is to be conducted in accordance with the steps shown in Figure 1,* below. The first three steps are the keys to the total evaluation based on the program sequence noted above. Each step (after the first) in the scheme of Figure 1 is dependent upon the results of the previous step or steps, so that, for example, Steps 2, and 3 are to be omitted if the results of Step 1 show that the hazard involved in the incident was not identified, since there can be no establishment of controls when there is no recognition that something needs to be controlled. For this reason, the program analysis will involve detailed evaluation in, at most, one of the first three steps shown in Figure 1.

Figure 1. Basic Program Analysis Steps
Used in This Institution

* Figure numbers in the model are italicized and begin with Figure 1 in order to present a "self-contained" presentation. Roman numbers are still consecutive from the beginning of this document.

For the detailed evaluation of program elements, use is to be made of the audit guidance policy documents for both Institutional and Departmental audits issued by the ES&H Staff. Taken together, these documents lead to a generic list of program elements that may have to be audited in the course of a full-scale accident investigation. This list is given in Appendix A of this document. The requirements for full-scale accident investigations given below make use of these elements to define the program areas that are to be investigated. It is intended that audit plans and rating guides from the two ES&H Staff audit guidelines be used in the following evaluations. Policy below is stated in terms of an accident that occurs with a hazard under the control of a Department within this Institution. In the case where control is exercised by the ES&H Staff, precisely the same approach is to be taken--reading "ES&H Staff" for "Department."

As a simple example of this latter situation, an ES&H Staff organization may be responsible for the disposal of toxic wastes. This is in the nature of an institutional control program exercised by the Staff for efficiency, and because it is a "cross-cutting" effort and particular expertise is required, rather than being exercised by each involved working level Line organization. Under these circumstances, an ES&H plan for the waste disposal operations would be prepared by the ES&H Staff. Such a plan would follow the format required of a working level Line organization plan.¹⁰ Thus, in auditing the plan, the use of working level Line organization audit criteria is appropriate, reading (in Appendix A) "ES&H Staff" for "Department." So, for example, one would ask whether the ES&H Staff Waste Disposal Program maintains a hazard list using program element D4 in Appendix A--a program element normally used by working level Line organizations.

Step 1. Step 1 of the basic program analysis shown in Figure 1 is to investigate the identification of the hazard(s) involved in the accident. In this step, it is only the formal identification of the hazard that is important.

To perform Step 1, the documented hazard list in the Departmental ES&H plan must first be reviewed. If the hazard involved in the accident is included in the list, this step of the analysis has then been completed and the investigation will proceed to Step 2. If, on the other hand, the hazard is not on the list, the investigation is to take the direction shown in Figure 2.

Step 1

Figure 2. Investigation of Failure To Identify Hazard(s)

After finding that the hazard was not identified in the Departmental ES&H plan, the next question shown in Figure 2 asks whether the hazard was not recognized because of a change (in design, in personnel, in schedule, etc.). If change was responsible for the nonrecognition, element D27 from Appendix A should be used to evaluate the change control function specified in the Departmental ES&H plan. If the rating on this element is less than "good" according to Institutional audit policy, the plan itself should be evaluated, as discussed under the next question. If the rating is "good" or better, it may be assumed that the Departmental ES&H plan was operating properly but that the change occurred too late for the change control to be effective before the accident occurred. In this case, the investigation will proceed to Step 4 of the basic phases (Figure 1). New controls to be considered in Step 4 should relate to the change control system.

When the failure to identify the hazard was not due to change, the next question is whether the Department had sufficient information on hand to recognize the hazard. If the information was available, the investigation should next look at the Departmental ES&H administrative plan to determine why it was inadequate in providing hazard identification. The plan may be conveniently evaluated through use of the following elements from Appendix A:

Management support elements:	A1, A2, A3, and A4
Organizational elements:	B1, B2, B5, B7, and B8
Program and control elements concerned with functions necessary for hazard identification:	C3, C4, D1, D2, D3, D4, D8, D9, D10, D16, D22
Internal assurance elements:	B6, E1, E2, E3, E4, E5, E6, E7, E8, and E9

In specifying these elements for examination, the assumption is made that they play a role in hazard identification at the working level Line organization. Figure 5 shows how this may occur. This figure is a partial reproduction from the model Line organization administrative plan of Reference 16. With reference to Figure 5, several elements would have to fail in their functions before a hazard would be overlooked. Thus, it is appropriate at this level to examine a collection of program elements. If, on the other hand, the failure occurs in management, organizational, program, or control elements, investigation of assurance functions should focus on why the programmatic failure was not observed by the internal assurance effort as well as the failure of the assurance activities themselves to find the hazard.

CRITERION	RESPONSIBILITY (B1)	FUNCTION (B5)	EVIDENCE (C1,D18,D28)	INTERNAL ASSURANCE
IDENTIFY SIGNIFICANT HAZARDS (INITIALLY, AND ON A CONTINUING BASIS-- INCLUDING LOCATION, ORGANIZATION, PROJECT, ETC.	FIRST LINE SUPERVISOR (FOR OWN ORGANIZATION ONLY) (B4)	PROVISION OF FACILITY/ PROJECT DATA (D1) PROVISION OF HAZARD LIST (D1,D4) PROVISION OF PROPOSED CHANGES (D3,D27) MONITORING OF - BUDGETS - SCHEDULES - DESIGNS - PURCHASE REQUISITIONS - ETC. (D3,D8,D9, D10,D27) INSPECTION OF - OPERATIONS - EQUIPMENT - FACILITIES (D22,D27) REVIEWS OF PLANS	ES&H PLAN INPUTS AS MEMOS TO ES&H COMMITTEE INSPECTION, MONITORING FORMS AND REPORTS VERIFICATION SIGNATURES ON DOCUMENTS REVIEW REPORTS	* FIRST CONCERN: PLAN REALLY BEING FOLLOWED (C9) * SECOND CONCERN: PLAN LEADS TO DESIRED RESULTS (IN THIS CASE, THE IDENTIFICATION OF HAZARDS, THE DEVELOPMENT OF CONTROLS, AND THE USE OF CONTROLS (E9) VERIFIED THROUGH AUDIT (E6) ACTIVITIES BASED ON * OBSERVATION -I.E., INSPECTION ACTIVITIES (E2,E3, E4, E5, E7) * REVIEWS OF EVIDENCE (E1, E2, E8) * INTERVIEWS (E2, E7) USING LINE CONTROL PROGRAM ELEMENTS AS BASE EVIDENCE: * AUDIT PLAN SHEETS FOR EACH PROGRAM ELEMENT AND ANY SUBSIDIARY MATERIAL GENERATED DURING AUDIT * AUDIT REPORT (E9)
	PERSONNEL (C4)	PLAN AS REQUESTED (D3,D4) PARTICIPATION IN ES&H MEETINGS (D4, D27) FORMAL REPORTS OF HAZARDOUS EQUIPMENT, FACILITIES, OPERATIONS (D18,D27) INFORMAL REPORTS TO ES&H COMMITTEE OR SUPERVISION (D27) FORMAL REVIEW ACTIVITIES, AS REQUESTED (D10)	MONITORING RECORDS FORM MEETING MINUTES FORMS COMMITTEE OR SUPERVISORY NOTES REVIEW REPORTS	
	ANALYSTS (C4)	INSPECTION ACTIVITIES (D22,D27)	INSPECTION REPORTS AND FORMS	
	SAFETY, STANDARD, AND CALIBRATION, MATERIAL TESTING, AND TRAINING DEPARTMENTS (D2,B7, B8)	MONITORING REPORTS, MEMOS, DATA SHEETS, AND REPORTS		
	ES&H COMMITTEE	INSPECTION ACTIVITIES (PERIPHERAL PURPOSE) (D4,D27) SOLICITATION OF INPUTS -DIRECTLY -ES&H MEETING (C4) PLAN UPDATE (D1, D2, D4) DISSEMINATE ES&H STAFF HAZARD IDENTIFICATION INFORMATION (D0)	INSPECTION REPORTS AND FORMS FORMS, COMMITTEE NOTES MEETING MINUTES PLAN (C3, D3) COMMITTEE NOTES AND MEMOS MEETING MINUTES	
	LINE MANAGEMENT	DIRECT DEVELOPMENT OF PLAN	DIRECTIVES PLAN	

Figure 5. A Partial Generic Administrative ES&H Plan at the Working Level of Line Organization

A second part of the question of why a hazard was not identified in the Departmental plan is why the ES&H Staff assurance reviews and audits did not find the plan inadequacy. For this, program elements B4, F40, G2, G3, G4, and G5 are to be used. As shown in Figure 2, the investigation is then to proceed to Step 5 in Figure 1.

If the responsible Department did not have sufficient information to identify the hazard, the next question is whether the ES&H Staff had information that would have enabled the Department to identify the hazard if it had been received. If the answer is "Yes," the matter of concern is why the Staff guidance function was inadequate. This should be investigated as follows (see Appendix A):

Guidance function elements: F4, F5, F6, F10, F11, F20, and F40

Management support elements: A1, A2, A3, and A4

Assignment of responsibility elements: B1, B2, B3, and C1

Assurance elements: G5

After checking the guidance inadequacy, the investigation is to proceed to Step 5 in Figure 1.

If information on the hazard was not available to the ES&H Staff, the final question in Step 1 is whether the information was available to specialists in the applicable fields (B7). The assistance of such specialists may be used, as required, for this determination. If these specialists have such information, the capability of the ES&H Staff should be checked, using elements F1, F2, F3, F21, F22, and F40, in order to determine why the Staff did not acquire the information. The investigation will then proceed to Step 5. When there is a general lack of knowledge of a hazard within the ES&H community (i.e., specialists do not know), it is classed as a new phenomenon, and the investigation proceeds to Step 4 in order to determine whether controls should be established over this new phenomenon so that the risk is acceptable and to determine possible control options.

Each instance in which the rating of one of the program element evaluations given above is below "good" according to Institutional policy qualifies as a negative program finding in the investigation and should be so reported and used as a basis for formulating recommendations.

Step 2. Step 2 is concerned with determining whether acceptable controls were established over the appropriate risk factors associated with the hazard(s) involved in the accident. According to Institutional policy regarding ES&H analyses, there are three subfunctions to consider here:

- Analysis of the hazard(s) to identify the factors upon which risk depends,
- Identification of possible controls over factors affecting risk, and
- Selection of acceptable controls to be used over these factors.

The Departmental ES&H plan is required by Institutional policy to describe all three of these subfunctions unless consensus or mandatory controls are used.* The plan should be used to answer the question, at this step, as to whether controls were established over the risk factors involved in the accident. Institutional ES&H program documents are to be used to determine whether the appropriate ES&H Staff organization controls were established, when this is relevant.

Step 2 is concerned with the establishment of controls that were acceptable a priori and not with their acceptability after the accident has occurred. Inclusion of controls over the risk factors involved in the accident (for the identified hazard(s)) in the Department's ES&H plan, approval of the plan by working level management, and review of the plan by the ES&H Staff (or inclusion of necessary Institutional level controls in the ES&H Staff Program Plans) that demonstrates acceptability in accordance with Institutional policy is sufficient evidence that this question should be answered "Yes." Further questions about the adequacy of the controls are resolved in Step 4.

To determine whether the risk factors involved in the accident possessed defined controls, the physical investigation of the accident (policy for which is given in the next section) must have progressed to the point where the failure modes involved in the accident are understood and the risk factors associated with these failure modes are known. If the failure modes and risk factors involved in the accident

*This is most likely to be the case when routine hazards that are accepted by the public are involved. In this case, the existence of acceptable controls is implied, and these are typically used.

are strictly hardware-dependent and if consensus or mandatory controls have been used, then, again, it may be assumed at this stage that the appropriate risk factors do have defined controls.

The point being made here is a rather crucial one. If approved and reviewed controls were indeed defined that would theoretically cover the way in which the accident happened, then there are two logical choices--the controls were not used, or the accident frequency is directly dependent upon the reliability of the controls. At this point, the investigation should determine that the controls were acceptable (*a priori*) in accordance with policy. This should have been addressed in the Staff review.⁴ The question of control use is addressed in Step 3, while the issue of the continuing acceptability of the controls (now logically linked to accident frequency) is addressed in Step 4. If controls deemed acceptable *a priori* exist over the risk factors involved in the accident, and they are used, then the accident can be regarded as "acceptable" at the time of its occurrence--and no blame is logically ascribable to any person or organizational entity. Only the question of whether the controls *are acceptable in view of the accident's occurrence* remains.

The approach to accident investigation presented here is the only one, to our knowledge, that permits blameless, acceptable accidents which do not automatically call for corrective action. Certainly the question of corrective action is raised, but it is addressed in a well-defined framework which simply questions the acceptability of risk in the presence of information about the controls and their reliability. It is essential that an approach to accident investigation have this character if one is not to pursue zero risk asymptotically with time--which is generally implied by other approaches that involve an automatic need for corrective action.

To achieve this state, it is essential that the failure modes and risk factors involved in the accident be known from the physical investigation. How this is to be accomplished is discussed below. The logic inherent in taking Step 2 of *Figure 1* is that shown in *Figure 6*. Here, an analysis is required by the ES&H Assurance Program Standard that identifies the risk factors upon which the likelihood of the occurrence of failure modes depends. Reference 10 discusses this in some detail. When only hardware factors are involved and consensus controls are used, the assumption may be made that the controls address

Figure 6. The Substeps Involved in Taking Step 2--"Were Approved and Reviewed Controls Exercised over the Appropriate Risk Factors?"

the appropriate risk factors. This should be verified, if practicable, for oversights in the development of consensus or mandatory standards can occur. Even were this the case, however, from the point-of-view of institutional mistakes, all reasonable and appropriate steps have been taken, and the accident should be regarded as blameless and acceptable at the time it occurred (assuming, of course, that the defined controls were also used--Step 3).

When an approved and reviewed set of controls over the risk factors associated with the accident does not exist, the investigation is to proceed as shown in Figure 3.

The first question to be answered in Figure 3 (paralleling the sequence in Figure 2) is whether the failure to establish controls over the risk factors is because of a change. If changes were responsible, element D27 from Appendix A should be used to evaluate the change control system incorporated in the Departmental ES&H plan. If the

Step 2

Figure 3. Investigation of Failure To Establish Controls

rating on this element is less than "good," the plan itself should be evaluated, as discussed under the next question. If the rating is "good," or better, it is assumed that the plan was operating properly but that the change occurred too late for the change control to be effective before the accident occurred. The investigation should then proceed to Step 4 to determine whether further or other change controls might be desirable.

When the failure to establish controls over the hazard was not due to change, the next question in Figure 3 asks whether the Department had sufficient information available to establish controls. If the information was available, the question becomes why the Departmental ES&H plan was inadequate in providing for establishment of controls. The plan may quickly be evaluated through use of the following program elements (see Appendix A):

Organizational elements:	B1, B2, B5, B6, B7, and B8
Elements concerned with program and control functions necessary for establishing controls:	C2, C3, C4, C5, D3, D5-D24, D26, D27, and D29
Internal assurance elements:	B6, E1, E4, E7, and E8

Again, the ES&H Staff assurance function's failure to find the Departmental plan inadequacy may readily be questioned using elements B4, F18, F40, G2, G3, G4, and G5.

When the Department did not have sufficient information to establish controls over the hazard, the next question in Figure 3 to be asked is whether the ES&H Staff organization had information that would have enabled the Department to establish controls if it had been received. If the answer is "Yes," the inadequacy in the Staff guidance function should be investigated using the following elements:

Guidance function elements:	F1, F2, F3, F4, F5, F6, F7, F8, F9, F12, F13, F14, F15, F16, F17, F39, and F40
Management support elements:	A1, A2, A3, and A4
Organisational and program elements:	B1, B2, B3, and C1
Assurance elements:	G2, G3, G4, and G5

After checking the guidance inadequacy, the Institutional program (including the ES&H Staff program) adequacy should be checked, particularly with regard to the pertinent controls (including the emergency

response program). The Institutional plan and ES&H Staff program plans are to be evaluated through use of the following program elements (only controls pertinent to the accident are to be checked):

Management support elements:	A1, A2, A3, and A4
Organizational elements:	B3 and B9
Elements concerned with program functions necessary for establishing Staff controls:	C1, C5, F18, F19, F23-F39, and G1

The investigation is then to proceed to Step 5 of Figure 1.

If information needed for establishing controls over the hazard was not available to the ES&H Staff, the final question in Step 2 of Figure 1 is whether the information was available to specialists in the applicable fields. If the assistance of such specialists is required for this determination, the investigation team Chairman may make such arrangements as he or she deems necessary. If specialists have the required control information, the capability of the ES&H Staff should be checked, using elements A2, A3, B1, F1, F2, F3, F21, F22, and F40, in order to determine why the Staff did not acquire the information. The investigation is then to proceed to Step 5 of Figure 1. When ES&H specialists do not have the required control information, the investigation proceeds to Step 4 to determine whether the establishment of controls is necessary.

Note that at this point, the formal investigation would terminate for the earlier example of the accident involving the toxic waste pond. The flow of the investigation would have followed that shown in Figure 7, in which the last three questions are answered "No" on the basis that the events were not reasonably foreseeable using best available evidence--illustrating the simplicity and completeness of the program analysis.

Each instance in which the rating of one of the program element evaluations given above is below "good" according to Institutional policy qualifies as a negative program finding in the investigation and should be so reported and used as a basis for formulating recommendations.

Step 3. Step 3 of Figure 1 is concerned with the use or implementation of the controls established over the risk factors involved in the accident. The primary evidence for use of controls is that which

Step 1

Was the hazard (toxic substance) identified?

Yes

Step 2 Were approved and reviewed controls established over the appropriate risk factors (earthquake)?

No

Because of change?

No

Information on requirements, and so forth, available to Line (frequency/intensity of earthquake)?

No

Information available to Staff?

No

Information available to specialists?

No

to Step 4--Should new controls be recommended?

Figure 7. Investigation Sequence for Example Accident Involving a Toxic Waste Pond

is documented in ES&H audit reports. Both internal and external audit reports for the area involved in the accident, particularly the most recent reports, should be examined for evidence that the pertinent controls have been consistently used. The physical analysis of the accident itself that is to be performed concurrently with this program analysis should be used, in part, to provide evidence about the use of controls.

When there is sufficient evidence that the controls were used, the investigation is to proceed to Step 4. If, however, there is evidence that the controls were not used, the investigation is to address the question of why the change system or the administrative portion of the Departmental ES&H plan was inadequate for assuring consistent use of the controls. Change is checked using element D27, while the plan is to be evaluated through the use of the following program elements (Appendix A):

Management support elements:	A1, A2, A3, and A4
Organizational and program elements:	B1, B2, B5, B6, B7, C1, C3, and C4
Control elements:	D6-D11, D15, D21, D23, D24, and D26-D29
Internal assurance elements:	B6, E1, E6, E8, and E9

The ES&H Staff assurance function's failure to find the inadequacies in the Department's administrative plan is also to be examined at this stage, using program elements B4, F40, G2, G3, G4, and G5. The required substeps of Step 3 are given in Figure 4.

Each instance in which the rating of one of the program element evaluations given above is below "good" in accordance with Institutional policy qualifies as a negative program finding in the investigation and should be so reported and used as a basis for formulating recommendations.

Step 4. Step 4 of Figure 1 is concerned with providing accident information that is needed to determine whether additional or altered controls might be needed. When all of the appropriate program elements associated with the first three steps have been rated adequate, as indicated in Figures 1, 2, 3, and 4, the investigation is to proceed to Step 4. Step 4 then is to be taken only when all necessary program actions were taken in "good" or better fashion, but the accident still occurred. As a matter of policy, this Institution recognizes that any system of controls will result in some risk since risk cannot be eliminated entirely. The policy of this Institution is to maintain levels of risk that are acceptable to those at risk. The necessary information for determining whether the risk is acceptable in view of the occurrence of the accident must be collected at this point in the investigation. It is not the responsibility of the investigation team to determine whether risk is acceptable to those at risk. This is a management responsibility within this Institution. There are, however, relevant inputs into this decision that are to be made by the investigation team.

Step 3

Figure 4. Investigation of Failure To Use Controls

The investigation team, during Step 4, is first to attempt to determine whether the risk estimated in the Departmental plan is statistically compatible with the occurrence of the accident and any similar or related accidents at this Institution or elsewhere. If the risk estimate in the Departmental plan is statistically compatible with the occurrence of the accident, this should be noted as a finding of the investigation, and the team should proceed to Step 5. If not, or if this determination cannot be made for statistical reasons, then the reliability of the controls that were being used during the accident should be compared with that assumed in the Departmental risk estimate, if possible. Where there is significant divergence, reasons should be sought (through the physical investigation), possible new controls should be studied, and those that are compatible with the previous risk estimate should be identified. In addition, the investigative steps indicated in Figure 5 should be taken to determine whether changes in program efforts are indicated to avoid future problems in estimating control reliability. When the comparison between actual control reliability and its estimate cannot be clearly made for statistical reasons or for lack of an a priori estimate, this constitutes a finding, and a study of other possible controls should be made before proceeding to Step 5 of Figure 1.

When an investigation team reaches Step 4, the implications are that the hazards involved in the accident were identified, the failure modes that led to the accident were recognized, the risk factors upon which these failure modes were dependent were known, and approved and reviewed acceptable controls (which may be none, based on the best available evidence) were truly being exercised over these risk factors; or that one of these things failed to occur on a temporary basis because of a lag in the change control system (which is judged to be "good" or better). The presumption may be made that institutional policy regarding the acceptability of controls has been followed, largely because of the nature of the review process (Reference 4). This is verified in Step 2. Thus, the original estimate of risk (as it is required to be discussed in the working level Line organization plan) should have been acceptable.

In Step 4, either the original estimate of risk was essentially correct, or it was not. If it was correct, then the only logical reason for any corrective action is that the nature of what constitutes acceptable risk has changed. Under these circumstances, measuring the

Step 4

Is the occurrence of the accident consistent with the previous (acceptable) estimate of risk? — (Yes) —> Step 5

Unknown

Was control reliability consistent with previous estimates? — (Yes) —> Step 5

Unknown

What controls exist for which there is evidence of performance consistent with prior reliability or risk estimate? —> Step 5

(No)

Why did not controls have appropriate reliability? (To be answered as part of physical accident investigation).

(No)

(No)

Are program changes indicated to avoid this situation in the future? — (Yes) —> Identify these.

Identify these.

Figure 5. Generic Inputs into the Decision Whether New or Additional Controls Are Required

acceptability of risk and determining appropriate a posteriori controls is a management control function.

If it is not possible to determine whether the original risk estimate was compatible with the occurrence of the accident, the reliability of controls is to be addressed. The compatibility of original estimates of control reliability with the control failure that has occurred may often be more easily determined. The assumption here is that acceptable risk is largely a function of acceptable controls,^{10,17} so that if the controls performed as intended, then an acceptable level of risk existed at the time of the accident. In pursuing this, of course, it may not be possible to tell whether the control reliability was at the intended level, or it may be found that it, indeed, was not. In these cases, appropriate actions to delineate new or further controls need to be taken.

Lastly, when the original estimate of risk is not compatible with the occurrence of the accident, then there is, logically, a lack of knowledge about the reliability of the controls that were being exercised at the time of the accident. This logical link exists because, at this stage of the investigation, the structural analysis of the failure modes and the factors on which these depend do relate to the actual accident, as verified by the investigation. In this case, it is still assumed that the original risk estimate represented an acceptable risk level but that the controls did not lead to that level of risk. A definition of possible actions that might be taken to actually achieve the originally intended level of risk is then the charge of the investigating team. It is at this stage that the question of possible changes in program elements involved in the estimation of control reliability needs to be addressed.

When Step 4 is arrived at because of a response lag in a change control system as described in Step 1, 2, or 3, Step 4 should be pursued in precisely the same manner. In this case, the change control system has been judged "good" or better in accordance with institutional policy, and if any discrepancies are found to exist, they should relate to the reliability of change controls.

The existence of appropriate institutional policies regarding risk can greatly facilitate this step of the program analysis. In particular, since risk can be discussed qualitatively (Reference 10), some

policy specifying the meaning of "low risk," and so forth, in terms of frequency and severity¹⁰ will assist in determining whether the occurrence of an accident is compatible with an existing estimate of risk. Such a policy needs to be accompanied by policy or guidance for determining how the estimator (the actual accident frequency) should compare with the allowable frequency for "low risk" (for example) in order that the accident occurrence and "low risk" be regarded as compatible.

When controls are, or may be, less reliable than originally intended, possible new controls are indicated, and the question of acceptability is automatically addressed in the process of instituting them. In this approach, real risk and acceptable risk are compared, but the actual underlying basis for decisions is the acceptability of the risk, while estimates of real risk are only one input to the determination of this acceptability (see Reference 10). The above approach does not automatically force a lowering of the level of acceptable risk, but this is a logical, possible option in the process of defining new controls.

Step 5. Step 5 is essentially the reporting function that is described below. Reporting will be based on both the program analysis, just described, and the physical analysis of the accident for which policy is next described.

Physical Accident Analysis -- The team undertaking a full-scale accident investigation is responsible for conducting an analysis of the accident to determine precisely how and why the physical events involved in the accident occurred. This activity should closely support the program analysis effort required in the previous section and should parallel the ES&H analysis in the Departmental ES&H plan.

In particular, in accordance with the implementing policy of this Institution, the Departmental ES&H plan should have

- *Identified the hazard(s),*
- *Itemized the potential impacts of the hazard(s),*

- **Analysed the hazard(s) to identify the events whose likelihood of occurrence needs to be controlled or that need to be mitigated against in order to limit the potential impacts,*
- **Determined the controllable factors upon which the likelihood of events depends (risk factors), and*
- *Defined controls over these factors and mitigation actions over uncontrollable events.*

The program analysis is structured to determine whether these steps were taken, while the physical investigation must provide the data, first to make this determination, and when a step was not taken, then to provide physical or operational information about the reason why it was not.

Whether an unusual or a routine hazard is involved, in a full-scale investigation, the physical investigation is to be focused on the circumstances surrounding the actual accident and is expected to answer the following questions based on reliable, physical evidence.

- *What hazard source(s) was (were) involved in the accident?*
This question should be answered in the framework of the Institutional policy, promulgated through the ES&H Staff, which categorizes hazards and hazard sources. If the hazard sources involved are not identified in Institutional policy, for example, this information is fed into Step 1 of the program analysis.
- *What were the actual impacts associated with the accident?*
During Step 2 of the program analysis, these will be compared with predicted potential impacts to determine whether Departmental and/or ES&H Staff planning, requirements, and reviews are adequate.
- *What physical or operational events took place preceding, during, and after the accident that led to the actual realization of the impacts?* *Again, the issue to be resolved programmatically is whether the events or event sequences that led to the accident were foreseen in the planning/analysis phase or in the derivation of ES&H Staff requirements. This comparison is made as a part of Step 2 of the program analysis, as directed in the previous section.*

**These steps are required only for unusual hazards--consensus or mandatory controls, which are assumed to have been derived in a similar fashion, may be used for routine hazards.*

- What risk factors were involved in the accident? The effort to answer this question must include consideration of hardware, human, administrative, and operational risk factor types. The results are used as inputs to Step 2 of the program analysis.
- What controls were actually used to control the risk factors or mitigate against uncontrollable events? In answering this question, both the existence and use of physical and administrative controls should be addressed. This information is used as input into Steps 2 and 3 of the program investigation. In particular, a finding that risk factors were involved for which no controls were defined clearly answers the question in Step 2 of the program analysis in the negative, while knowing what controls were being used permits Step 3 to be taken.
- How or why did the controls fail to prevent the accident? This question should focus on issues of control reliability. Specifically, what characteristics of the controls led them to be ineffective? The answer to this question supports Step 4 of the program investigation.
- What were the operational and administrative base data at the time the accident occurred? The answer to this question should include information about operational configuration, facilities, site characteristics, responsible management, personnel, schedules, training, and chain-of-command that is relevant to the occurrence of the accident. Information of this type, when it has not been gotten directly from answers to the earlier questions above, should be used in assessing the role that change played in the accident, as required in the previous section.

Physical accident analysis refers to that analysis aimed at defining the accident itself, including what happened and the physical or operational cause of each part of the accident.

A number of approaches to accident analysis exist. An approach that most nearly parallels the ES&H analysis guidance of Reference 10 and that automatically addresses the types of questions posed in the model above is based on the use of fault trees.¹⁰ The use of fault trees to analyze potential impacts from a hazard begins with the identification of the generic or specific events from which such impacts could arise. These events are then analyzed to determine the subevents which might lead to their occurrence. This process of identifying

sub-sub...events continues until events whose causative factors can be identified and conveniently controlled or mitigated against are found.

The generic example given in Reference 10 is shown in Figure 8. Here the generic types of events that can lead to injury from a pressure system are denoted "energy release" and "exposure." The energy release event is broken down into component ruptures, and for one of these, some of the types of factors that would influence the likelihood of component rupture are identified. For example, material strength is a factor influencing the likelihood of gauge, line, fitting, valve, or vessel rupture. Material strength is thus a risk factor over which control can be exerted (exercise of a quality program, for example).

The use of the same type of logic is possible in investigating accidents--but the number of "branches" of the fault tree that must be pursued should be limited. As an example, suppose that a pressure system *has* ruptured, but that because personnel were removed to a reinforced control room, no personnel were injured. Further suppose that the rupture occurred in the vessel. Then the generic tree that would underlie the investigation does not involve injury, exposure or rupture of valves, gauges, fittings, or lines. The starting point in this case is well down the generic tree in Figure 8. In starting an investigation, the pressure vessel may be analyzed in terms of its component

Figure 8. A Partial Generic Fault Tree for a Simple Pressure System

parts if it is not an integral unit. Suppose, then, that the vessel had bolted-on ends and one bolted-on access port, and that the accident involved the rupture of one end, which severed most or all of the bolts that held the end in place. Immediately, one is concerned only with this particular rupture mode and can discard, on the basis of immediate visual evidence, failures of vessel materials per se, port bolts or ports, and so forth. This is illustrated in Figure 9.

Continuing, it is a tautology that the rupture occurred at the End 1/Cylinder interface because the force on the end exceeded the ability of the bolts to withstand the force. To proceed, in this abstract example, it is assumed that a design limit on that force had been set. When true, this would be determined by the investigation. Then, the next level events might be structured as shown in Figure 10--in which the interface rupture is envisioned as being caused by either a force which exceeded the design limit or by a failure (of the bolts, in this case) to withstand a force below the design limit. The "OR" in Figure 8 is not exclusive, and both may have been true.

Figure 9. First Three Steps Using a Fault Tree Logic in an Example Accident Investigation

At this point, the investigation must begin to involve more data collection and less logic, for evidence must be found which permits a choice between the two branches in Figure 10 to be made. How this might be done will depend highly upon circumstances. For example, if the pressure source for the vessel was not capable of generating pressures in excess of design limits of the vessel, the left branch in

Figure 10 can be eliminated. Similarly, if the pressure source for the vessel was connected to the vessel through a line containing a pressure relief valve designed to operate below the design limit of the vessel, and if investigative tests show that the relief valve was actually present and operating properly, then the left branch could be eliminated--if the only source of force on the door was pressure from the pressure source.

Fundamentally, to eliminate the left branch in Figure 10, investigators must identify *all* sources of force on the door, examine their temporal relationship to one another, and show, on the basis of hard evidence, that at no time might they have been combined to exceed design limits. During such an investigation, other relevant factors must be examined. Even if the design limit were not exceeded, it may be found that changes had taken place that caused the force to be greater at the time of the rupture than had previously been permitted (for example, a new pressure relief valve operating at higher pressures than the old one--but still below design limits--might have replaced an old one). Indeed, if design limits had not existed, the choices in Figure 10 might have been phrased something like "Force greater than 'normal'" and "interface not capable of withstanding 'normal' force." This leads one to analyze changes, a subject which is discussed below.

Figure 10. Fourth Investigative Step in the Fault Tree

To pursue the example, assume that the left branch of Figure 10 can be definitely eliminated. The right branch must be investigated (in practice, both would probably be investigated simultaneously). The integrity of the interface depends, as envisioned here, upon the integrity of the bolting arrangement that holds the door to the cylinder. The issue, then, is how this might fail. Some of the possible failure modes are shown in Figure 11.

Figure 11. Possible Fifth Investigative Step in the Fault Tree

Relative to Figure 11, visual examination should provide evidence for making a choice. Assume that the bolts sheared, as indicated in Figure 11. At this point, the possible factors that caused the bolts to shear could be identified. These might include such items as

- Material strength,
- Tightness of bolts, and
- Number of bolts (all present?).

If for example, one bolt were clearly missing or several were loose, and evidence can be found that this condition existed during the rupture, then a possible explanation of the rupture event exists. *That the material strength of the bolts was not degraded still would need to be verified through material tests.* If it is found that configurational circumstances were responsible, then the investigators should

next seek to determine whether procedural controls existed which addressed configurational issues. If procedures existed, they may have been inadequate or not used. The physical investigation should pursue possible evidence of use. The complete sequence of steps in this example is shown in Figure 12, which illustrates the self-limiting character of this approach and its interface with the program analysis phase of the investigation.

The program analysis and physical analysis converge strongly at this point in this example, for the basic issue involves questions about the adequacy and use of procedures as a part of the working level Line organization ES&H plan. Thus, for example, questions relative to Step 3 (addressing control use) of the program analysis may be appropriate (depending upon the outcomes of Steps 1 and 2). If Step 3 is involved, then the ES&H plan should have specified program elements which cover the known ways in which procedures can fail to be used. This is discussed in References 10, 14, and 16. The program elements specified in the previous section cover these failure modes.

This is only one possible approach to the physical investigation of accidents. The intent in any approach, however, should be to determine the relevant events that occurred, what factors the occurrence of these events depended upon, what controls were exercised over the important factors, and whether the controls were used. In the course of an investigation, it is not unreasonable for investigators to identify better approaches to physical or administrative control for use in Steps 4 and/or 5 of the program analysis phase of the investigation, and the two phases should be carefully coordinated. In addition, through this approach, inadequacies in consensus or mandatory controls will be identified.

The approach to physical accident investigation outlined above depends heavily upon one's ability to logically structure the possible failure modes at each level of the partial fault tree. Other approaches exist that, while they may bring in much extraneous information, may offer less chance of overlooking a failure mode when individuals not familiar with fault tree logic are responsible for the investigation. One of the better forms of accident analysis that has this character of "automatic comprehensiveness" is "Events and Causal Factors Charting," discussed in Reference 23. For this, the temporal sequence of events leading up to the accident is charted in block

Figure 12. Steps in Fault Tree Approach Illustrating Self-Limiting Character

diagram form, and for each block (or independent temporal event), factors affecting that block are added. An incomplete version of this approach, treating the above pressure system example, is shown in Figure 13.

In Figure 13, more detailed events are added the nearer one comes, temporally, to the actual accident. Thus, for example, one would add events such as "Bolts not all tightened" prior to the "Turn on" event. To promote efficiency, judgment is clearly called for in determining what events to include, and indeed, these may alter with the progress of the investigation. Pertinent factors are added as information is gained. However, it is theoretically possible to deal with *all* temporal events and *all* related information in such a setting and thus not to overlook important occurrences. In using either the earlier fault tree approach or temporal events and causal factors charts, one first finds that the bolts were not properly placed, then seeks reasons for this. When all appropriate temporal events are identified, the actual final failure events of the fault tree will be among them.

As suggested by the discussion of, and figures associated with, each of these approaches, the need to examine changes that have occurred--in relation to either failure events or temporal events--should be clear. It is known that change plays a large role in accidents,²¹ and the questions posed in the program analysis of the previous section (and inherent in the six criteria earlier in this document) emphasize this. One potentially useful technique for assessing change is "Change Analysis,"²⁴ particularly if the basic causes of the accident are unclear. Change analysis consists of systematically recording all conditions involved in the accident and the corresponding conditions in the same operation at a time when no accident occurred. The changes identified through this process can also lead to the basic causes of the accident. This approach tends to be comprehensive and may lead to much unneeded information, but oversights tend to be reasonably unlikely. In ES&H Assurance Programs, it is often sufficient to seek only changes relative to ES&H plans (and referenced procedures, and so forth) as suggested in the previous section.

Reporting on Full-Scale Accident Investigations -- When both the physical and program analyses have been completed, the investigation team should be able to identify the physical occurrences involved in the accident and the inadequacies (if any) in the ES&H program that

Figure 13. Temporal Events and Causal Factors Chart

allowed them to occur, be able to make an overall evaluation of the program, and be in a position to present recommendations for improvement, as appropriate. This information will be part of an investigation report. The report should include

- A description of the facility, the operation, or the product involved in the accident,
- A description of the accident, with the sequence of events and the extent of damage, injury, or illness, in categories prescribed by Institutional ES&H analysis policy,
- A compilation of all the facts collected during the investigation that relate to hazard recognition, events, and risk factors involved in the accident; and defined controls, their use, and evidence of their acceptability,
- A prioritized listing of findings (positive and negative) discovered,
- Conclusions drawn as a result of these, and
- A statement of recommended options for improvement, if appropriate.

In the case of an Institutional investigation team, the completed report is to be submitted to the President of this Institution, and the Vice-President, ES&H Staff. When a Departmentally-appointed investigation team is involved, a draft report is to be submitted to the ES&H Staff for review, and a final report, formally approved by the ES&H Staff, is then to be sent to the President and the responsible Department manager. Minority opinions may be included as appendices to the report. The report should be prepared for external release should management decide to use it in this way. Qualifications of investigators should be included in an appendix.

The investigation report should sensibly prioritize information and recommendations. Irrelevant information should be omitted and important deficiencies addressed more strongly than less important ones. A conclusion that

- The hazard was recognized,
- All pertinent failure modes and risk factors were identified,
- Approved and professionally reviewed controls consistent with mandatory requirements and Institutional criteria for acceptability were defined and used,

- The accident is compatible with estimates of risk or control reliability, and
- No corrective action is recommended

is permissible when investigation findings so warrant. Options for possible actions, if determined in the course of the investigation, should be included even in this case.

In addition, in all cases, recommendations for the use of the data derived from the accident investigation should be made, and issues that warrant further research, in the opinion of the investigators, should be identified.

Restricted-Scale Investigations

Personnel Performing Restricted-Scale Accident Investigations

When the ES&H Staff management determines that a restricted-scale investigation is appropriate, the Department manager in whose organization the accident has occurred will select an individual or team (and in this case appoint a Chairman) to investigate the accident, with ES&H Staff concurrence in the selections. At least one investigator must be trained in accident investigation techniques by the ES&H Staff in accordance with the policy contained in this document. Individuals selected should not be members of the involved Department. The majority of persons selected are expected to serve as investigators on a priority basis for up to 3 weeks, as determined by the ES&H Staff management. A member of the ES&H Staff is to be designated as a consultant, and for liaison purposes, at the time a decision for a restricted-scale investigation is made.

Investigator Responsibilities

Immediate actions of the investigator(s) should be of the same types as those of a full-scale investigation team--with emphasis placed on recording physical data pertinent to the accident and interviewing persons who were involved in, or observed, the accident. The time during which the accident site is secured should be minimized, consistent with the needs of the investigation.

No formal investigation plan is required for restricted-scale investigations; however, informal planning is encouraged in order to promote the efficient use of time of those involved in the investigation. While less formal, and restricted in scope, restricted-scale investigations will still involve four phases,

- Data collection,
- Program analysis,
- Physical accident analysis, and
- Reporting,

that are to be undertaken in accordance with the policy described below.

Within the context of this policy, the investigator(s) is responsible for determining probable physical and programmatic causes of

the accident, making appropriate recommendations for action, and preparing a memo describing the investigation.

Phases of a Restricted-Scale Investigation

Data Collection -- The scope of the data collection effort should be a function of the nature of the program analysis and physical accident analysis phases discussed next.

Program Analysis -- In accordance with the general policy given in Table 1 in an earlier section, all accidents that warrant restricted-scale investigations involve only hazards judged to be a routine or routine-like. As a result, the controls exercised will normally be those specified in Institutional policy documents or modifications thereof made as a result of Line organization inputs and approved by the ES&H Staff. Because of this, the adequacy of the controls is often an ES&H Staff responsibility.

In restricted-scale investigations, the scope of the formal investigation is normally to be restricted to the Departmental program and responsibilities. The investigation is to determine

- Whether the hazard was recognized,
- Whether approved and reviewed controls consistent with Institutional requirements were defined over the hazard,
- Whether these controls were used at the time of the accident, and
- Whether the occurrence of the accident is consistent with statistical expectation, and if not, why, and what actions might be recommended.

Thus, the first four generic steps of a full-scale investigation, given in Figure 1, with slight modification, are to be taken, but substeps shown in Figures 2, 3, and 4 are generally to be restricted only to audits of the Departmental program. Indications of possible deficiencies in the Institutional program are to be referred to the ES&H Staff for further investigation. In addition to this restriction, the preliminary substeps required in Step 2 are to be those shown in Figure 6.

Step 4 of a restricted-scale investigation should follow the substeps given in Figure 7. Where there are indications that either the Institutional program or the mandatory requirements are inadequate,

Figure 6. The Preliminary Substeps Necessary in Step 2 in a Restricted-Scale Accident Investigation

Step 4 (Restricted-Scale)

Figure 7. Generic Inputs into the Decision Whether New or Additional Controls over Routine Hazards Might Be Needed

further investigation will be undertaken by the ES&H Staff under the direction of the designated consulting Staff member if deemed necessary by ES&H Staff management.

In the model presented here, there are two types of restrictions that may serve to limit the scope of restricted-scale investigations:

- Limitation of the investigation to working level Line organizations' programs and
- Avoidance of direct consideration of events, or event sequences, and risk factors.¹⁰

Limitations of this sort are arbitrary and their use should be controlled by the ES&H Staff. In particular, the Staff should have the discretionary authority to direct or conduct the investigation into broader areas as it deems necessary.

Because formal ES&H analyses, if they exist for routine hazards, are done as a part of mandatory or consensus standard development generally, possible inadequacies in analyses and/or the program designed to perform them should normally be referred to the ES&H Staff, just as are possible inadequacies in other portions of the institutional program.

For routine hazards, the assumption is that if appropriate mandatory controls are defined and used, then the accident is acceptable at the time of its occurrence. However, "appropriate" in this case involves both a determination

- That the controls applied to the physical failure mode actually involved in the accident (Step 2) and
- That the mandatory controls were adequate in view of operational circumstances (Step 4).

In the former case, if the accident occurrence involved *no control failure*, then the failure mode was not controlled--implying that mandatory controls may be incomplete and should be investigated by the ES&H Staff or that the frequency of the failure mode was judged to be sufficiently low that controls were not required, the correctness of which may need to be pursued by the ES&H Staff.

The final result of a restricted-scale investigation should, again, be the provision of the background information needed to determine whether risk is acceptable or what actions might make it so. In

particular, any program deficiencies involved in the accident should be found by the investigators and/or the ES&H Staff.

Physical Accident Analysis in Restricted-Scale Investigations --

The physical accident analysis portion of a restricted-scale investigation should answer the following questions based on either reliable, physical evidence or the best judgment of the investigator(s) (see the full-scale investigation section for a discussion of appropriate questions).

- *What hazard source(s) was (were) involved in the accident?*
- *What were the impacts associated with the accident?*
- *What was the failure mode (event sequence) involved in the accident?*
- *What controls were exercised over this failure mode?*
- *Were the controls consistent with mandatory requirements?*
- *Were circumstances such that the controls were appropriate?*
- *What were the operational and administrative base data at the time of the accident?*

Whenever the investigation finds that mandatory requirements, or modifications thereof, may have been inadequate, accident data sufficient for any further investigation required by the ES&H Staff should be taken and preserved. The material required should be decided on through consultation with the designated ES&H Staff member.

During a restricted-scale accident investigation, it is still important to determine whether there is evidence that the accident was anticipated in theory, and if so, whether the theory is consistent with the occurrence of the accident. Since controls over routine hazards are largely presented as mandatory or consensus requirements, the basic question is not whether the failure mode was foreseen in the ES&H plan at the working level of the Line organization, but whether one or more controls failed (implying that the failure mode was controlled) and whether the control(s) was (were) consistent with the requirements.

If controls consistent with mandatory requirements were used and failed (permitting the accident), then the accident should be regarded as acceptable at the time of its occurrence and therefore blameless. Questions relating to the continuing technical adequacy and acceptability of the controls then arise that are best addressed by the ES&H Staff and institutional management.

Reporting on Restricted-Scale Accident Investigations -- The accident report for a restricted-scale investigation shall be in memo form suitable for internal distribution. It should address all of the points required (earlier) in a full-scale accident investigation but in a less formal fashion consistent with the above policy. A draft report must be submitted to the ES&H Staff for review and approval prior to the issuance of a final report. The final report must be countersigned by the ES&H Staff, based on the ES&H Staff review, and accompanied by a report of any appropriate ES&H Staff investigation activities whose need was identified by the accident investigation. The final report and accompanying documents, if any, must be distributed according to the seriousness of the accident, a decision that is to be made by the ES&H Staff management. The responsible Department manager should always be on distribution.

Restricted-scale accident investigations, as described in the above model, are indeed more limited in scope and depth from the perspective of the investigator(s). Both program concerns beyond those that are the responsibility of the involved working level Line organization and technical concerns about the adequacy of ES&H analyses and controls are issues to be addressed by the ES&H Staff, as required. In addition, the judgment of the investigator(s), provided the ES&H Staff concurs, is relied upon more than in full-scale accident investigations. The general intent in both full-scale and restricted-scale investigations is the same, however: to understand the basic elements of the accident in order to determine whether program deficiencies permitted it to occur and whether new or altered controls are needed to maintain or achieve an acceptable level of risk.

As in a full-scale investigation, there are either program deficiencies that are involved in the accident, or (with the caveats previously discussed) the hazard was recognized; the failure mode had defined, acceptable controls (which could be none, because the failure mode was judged not to require them); and the controls were used. In a restricted-scale investigation, which involves only routine hazards, the measure of the acceptability of controls--and thus risk--involves the use of mandatory or consensus controls,¹⁰ possibly modified by the working level Line organization or ES&H Staff, based on employee participation.¹⁴ The presumption is, of course, that hazards routinely encountered and accepted by the general public have, by implication, acceptable controls that are normally stated as requirements or standards. If requirements are met or consensus standards are used that

are genuinely applicable to the situation, then the basic issue to be resolved is whether they remain acceptable in view of the occurrence of the accident. If modified controls are used, then the question of whether they were truly as good as or better than requirements or standards must be raised. These issues are addressed in Step 4, as before. The adequacy of the controls to the particular circumstances is also investigated.

As mentioned earlier, audits associated with accident investigations are restricted to portions of a program logically relevant to the investigation. In the case of restricted-scale investigations, the audit efforts of the actual investigator(s) are further restricted to the responsible working level Line organization program--with any needed audits beyond this becoming the responsibility of the ES&H Staff.

To illustrate how the investigation team and ES&H Staff share responsibilities, and how judgment is used, in a restricted-scale accident investigation as described in the above model, imagine a vehicle accident involving a corporate vehicle driven on business in which a brake failure caused the car to impact an abutment on a freeway, injuring only the driving employee. The hazard source in this case is the automobile--a routine hazard. A potential for injury to persons other than the employee existed but was unrealized. Depending upon the injuries sustained and the likelihood of public involvement, this could realistically be judged to require a restricted-scale investigation.

Further imagine that a single investigator is appointed and the physical and program data collected are those shown in Table 1* under the first heading of data collection. The accident occurred under good conditions and no evidence of driver malfeasance was found. Upon physical analysis, the vehicle's brakes were found to have failed because of a failure in the automobile's brake lines--which were not examined for cause but saved for the ES&H Staff. This failure mode was judged to have been controlled from the perspective of the working level Line organization by a requirement for regular 5,000-mile inspections to be

* As with figures, italicized table numbers run consecutively through the model only, while table numbers given in roman type run consecutively through the entire document.

Table 1

An Illustration of a Restricted-Scale Accident Investigation

Table 1 (Continued)

An Illustration of a Restricted-Scale Accident Investigation

ES&H Staff Investigation (Refer to Full-Scale Investigation Section)	
Data Collection	Program Analysis
<ul style="list-style-type: none"> • Maintenance inspection of brake lines scheduled every 15,000 miles. No initial quality acceptance inspection required. No previous failures over 15-year period, 2,000,000 vehicle-miles. • Records and interviews indicate procedures followed--no inspection of brake lines of car with 7,541 miles. • Concur with view that Line controls used. • Concur with view that risk not consistent with statistical risk. • Make of auto not previously purchased. 	<p>Approved and reviewed controls exist over failure mode?</p> <p>Yes</p> <p>Consistent with mandatory requirements?</p> <p>Yes</p> <p>Were established controls used?</p> <p>Yes</p> <p>What operational differences exist to explain inconsistency with statistical risk?</p> <p>New make of auto</p> <p>More appropriate controls?</p> <p>Quality acceptance inspection and test and 5,000-mile inspections and tests of safety systems until statistical base is obtained on new make autos.</p>

performed by the institution's maintenance organization. The investigator only notes, but need not investigate, that a question of whether maintenance efforts truly include brake and brake line inspections still remains. The controls specified in the working level plan were found to be those required institutionally, and records and interviews indicated that they were followed by the Line organization--in the best judgment of the investigator. The investigator notes that the actual *use* of the inspection control (if it exists) is outside the scope of his or her restricted investigation.

Thus, at this stage in this relatively straightforward investigation, the investigator concludes that the hazard was recognized, and acceptable controls were defined and were used at the working level. From the perspective of the working level Line organization, the accident was blameless, and its overall acceptability at the time it occurred depends upon questions about the performance of the maintenance department.

Further, the scenario given in Table 1 includes data that the auto had been driven only 7,541 miles when the accident occurred and that it had been driven under no extreme conditions. The investigator felt that under these circumstances, the failure mode was unusual and not consistent with normal statistical expectation (best judgment). This raises the question of the inadequacy of requirements or strengthens the question about deficient performance by the maintenance organization. However, from the point-of-view of the working level Line organization, the investigator felt that additional controls should not be necessary. In this scenario, no Line program audits were undertaken--only audit activities needed to verify that controls were used were performed--because the logic of the investigation did not require them.

With this investigation as a background, and concurred in by the ES&H Staff, the Staff must proceed to investigate the areas external to the working level Line organization that may have a relevance to the accident. The first such area relates to the existence of controls over vehicle brake line failure as a part of the maintenance organization's ES&H plan. Here, the service of an auto is regarded as the service of a *product* whose safety is to be assured in the plan. The maintenance organization's plan was found to recognize the product as a hazard and to require routine inspection and replacement of safety-related systems including brake lines. In this case, 15,000-mile

inspections and mandatory replacement of lines at 45,000 miles were required. These requirements were approved by the ES&H Staff, and there had been no previous brake line failures over a 15-year period involving over 2,000,000 vehicle miles.

With further reference to Table 1, records and interviews indicated that the inspections were performed by knowledgeable maintenance personnel, generally, but the nature of the requirements was such that the vehicle involved in the accident (at 7,541 miles) had not had its brake lines inspected. The Staff investigation, at this point, concludes that the maintenance department is blameless and the accident must be viewed as acceptable at the time of its occurrence. There remains only the question of the continued acceptability of the controls being exercised.

In this example, imagine that the ES&H Staff concurs in the judgment that the accident was not consistent with statistical risk--in particular all previous data indicated that the failure mode was highly unlikely at 7,541 vehicle miles. The Staff then seeks operational differences which might explain this and, in the scenario of Table 1, determines that the car involved was a make that had not been previously purchased by the institution. This suggests certain controls shown in Table 1 that might need to be instituted for the new make of automobile. Other obvious steps not indicated in Table 1 might have been elected by the ES&H Staff instead.

Nevertheless, in the scenario above, new institutional requirements for quality acceptance inspections and tests and more frequent inspections and tests of all safety-related systems in the new make of automobile were recommended by the ES&H Staff on an interim basis until a reasonable statistical base on failures is derived from the testing.

In this example of a restricted-scale accident investigation, the conclusion can fairly be drawn that the hazard was recognized and that controls deemed acceptable based on the best available data had been defined and exercised. In spite of this, an accident occurred which was judged not to be consistent with expected statistical frequency and was therefore judged not to be acceptable on a continuing basis. This logically necessitated consideration of new or altered controls, and a rational recommendation was made on the basis of expert judgment of the changed circumstances that led to the previous controls being apparently less reliable than they had been in the past. Other approaches

could have been taken. No blame for the accident should be ascribed to institutional personnel or program failure. The legal culpability of the automobile manufacturer is left as an unresolved question in this example.

Routine Investigations

Accidents that involve routine hazards that had only a potential for causing significant injury, illness, or damage at the work site (no actual significant impact), or accidents judged to have had no potential for significant impact, are to be investigated by the responsible supervisor. The form given in Appendix B is to be used for such a routine investigation, and it should be delivered to the ES&H Staff within 3 working days of the occurrence of the accident. The decision to undertake only a routine investigation of this sort must be made, or concurred in, by the ES&H Staff management. If there is any doubt about the appropriateness of a routine investigation on the part of Line management, a Staff opinion is to be immediately solicited by contacting the ES&H Staff Emergency Coordinator (Extension HELP).

In completing the Routine Accident Investigation Form in Appendix B, the responsible supervisor is asked to use his or her best judgment--formally checking only whether

- The hazard was identified and
- Controls over the failure mode were defined

in the Departmental ES&H plan, and if either of these failed to be the case or if controls were not used, then formally checking to see which program elements were deficient. The supervisor should make reasonable use of past audits performed by the Departmental ES&H Committee* and may use the assistance of this committee in the investigation as deemed appropriate. Information related to events and risk factors should be provided when available. Work schedules are to be disturbed as little as possible, but accurate observation of the circumstances surrounding the accident is to take precedence over work schedules. In the absence of a supervisor, any other member of supervision or any qualified project leader within the involved Department may undertake the investigation.

The form in Appendix B is slightly modified from one given in Reference 14. The logic is not significantly different from that involved in a restricted-scale investigation, but because unusual hazards may be involved (but judged to have had no potential for significant impact),

* A committee used to perform ES&H assurance functions at the working level of Line organization in this model (see Reference 9).

data about events and risk factors are requested (as appropriate). When an accident (unplanned event) occurs that is judged to have had no potential for significant impact, the primary concern is whether a program failure or inadequate understanding of control reliability was involved that could also lead to more serious accidents. No significant impact having been incurred, the basic issue is one of gaining knowledge.

When a potential for significant onsite impact from a routine hazard is judged to have existed, the questions of

- Program deficiencies,
- Control reliability, and
- Continued acceptability of controls or risk

must be of primary concern. Here, the question of acceptability is restricted to involved personnel and can reasonably be answered by the working level Line organization (with subsequent expert review of changes by the ES&H Staff).

APPENDIX A

Standard ES&H Audit Checklist for Use in This Institution's Accident Investigation Program

This list of program elements was derived directly from the ES&H Assurance Program Standard.¹ It represents the complete collection of program elements required by the Standard, appropriately interpreted for application at the working level of the Line organization or the institutional level, as described in References 3, 11, and 22. Example criteria for evaluating performance of each element are also given in these references.

The following program elements are to be used in conjunction with accident investigations in this Institution, as prescribed by policy. Elements denoted "nI" are to be used when Institutional programs are being analyzed, while program elements denoted "nD" are to be used when Departmental programs are being analyzed. Appropriate portions of Section D are to be used in analysing ES&H Staff control programs.

A. Management Support

- 1I. Institutional or middle-management policy statement
- 1D. Departmental policy statement
- 2I. Adequate staffing
- 2D. ES&H Committee defined
- 3I. Adequate funding
- 3D. Adequate funding for ES&H program
- 4I. Management involvement
- 4D. Management involvement

B. Organisation

- 1I. Assignment of responsibility and authority,
Institutionally
- 1D. Assignment of responsibility and authority within
Department
- 2I. Established lines of communication, Institutionally
- 2D. Established lines of communication with the Department
- 3I. Provision of independent Institutional ES&H Staff

- 4I. Provision of audit function associated with ES&H Staff
- 5D. ES&H functions in Department defined
- 6D. Independence of Departmental ES&H assurance functions
- 7D. Use of specialists in ES&H program of Department
- 8I. Provision for collaboration between organizations on ES&H matters
- 8D. Provision for collaboration between Departments on ES&H matters
- 9I. Provision of occupational health program

C. Program

- 1I. Documentation of Institutional ES&H Assurance Program (through middle-management)
- 1D. Documentation of Departmental ES&H Assurance Program
- 2I. Policy for varying ES&H controls in accordance with degree of risk
- 2D. Provision for varying ES&H controls in accordance with degree of risk
- 3D. Departmental ES&H assurance plans
- 4D. Provision for participation by personnel in Departmental ES&H functions
- 5D. Provision of controls over equipment and environment

D. Departmental ES&H Control Functions (to be used also in ES&H Staff control programs)

- 1D. Provision of facility/project information
- 2D. Classification of facilities/projects by ES&H categories
- 3D. ES&H considerations in planning
- 4D. Maintenance of hazard list
- 5D. Documentation of risk assessments
- 6D. Correlation of requirements with hazards
- 7D. Reporting of ES&H control activities
- 8D. Budget proposal reviews
- 9D. Schedule proposal reviews
- 10D. Design reviews
- 11D. Design verification controls
- 12D. Calibration program
- 13D. Maintenance program
- 14D. Qualification of equipment
- 15D. Storage and handling controls

- 16D. Material and equipment identification
- 17D. Status identification of material and equipment
- 18D. Provision of fabrication process procedures
- 19D. Quality documentation
- 20D. Quality corrective action program
- 21D. Procurement controls
- 22D. Test and inspection program
- 23D. Qualification and training for job assignment
- 24D. ES&H training
- 25D. Maintenance of training records
- 26D. Written operating procedures
- 27D. Change control
- 28D. Record storage and retrieval
- 29D. ES&H corrective action program

E. Department ES&H Assurance Functions

- 1D. Review of assurance plan
- 2D. Verification of control and control change implementation
- 3D. Monitoring for new hazards
- 4D. Monitoring of risk factors and controls
- 5D. Monitoring of environmental conditions in work areas
- 6D. Provision of audit program
- 7D. Verification of corrective action
- 8D. Evaluation through record reviews
- 9D. Evaluation of monitoring and audit data

F. Staff Control Functions

- 1I. Maintenance of requirement files
- 2I. Monitoring of requirements
- 3I. Plan for revising and developing requirements
- 4I. Provision for storage and retrieval of all ES&H data
- 5I. Provision of consultation to Line organizations
- 6I. Provision of ES&H reference material
- 7I. Guidance in preparation of ES&H plans and procedures
- 8I. Guidance in prioritisation of mitigation plans and procedures
- 9I. Guidance in operation of ES&H Committees
- 10I. Guidance in conducting ES&H meetings
- 11I. Guidance in identification of hazards
- 12I. Guidance in requirement awareness

- 13I. Guidance in establishing mitigation measures
- 14I. Guidance for ES&H analysis
- 15I. Guidance in continuous-operation monitoring
- 16I. Guidance in decontamination activities
- 17I. Guidance in ES&H inspections and audits
- 18I. Mandatory design reviews by Staff
- 19I. Mandatory participation by Staff in hazard investigations
- 20I. Provision of ES&H training programs for Line organizations
- 21I. Performance of ES&H research and development activities
- 22I. Availability of laboratory facilities
- 23I. Approval requirements for procurement of hazardous material
- 24I. Control of handling and storage of hazardous material
- 25I. Provision of personnel restrictions in hazardous areas
- 26I. Provision of dosimetry control
- 27I. Provision of protective equipment specifications
- 28I. Requirements for special work permits
- 29I. Provision of continuous-operation controls
- 30I. Provision of fire protection equipment maintenance controls
- 31I. Provision of decontamination and waste disposal program
- 32I. Exercise of radiation source control
- 33I. Development of explosive safety program
- 34I. Development of pressure safety program
- 35I. Determination of bioassay requirements
- 36I. Conduct of emergency drills
- 37I. Maintenance and calibration of special instruments
- 38I. Establishment of policies and practices for accident investigations
- 39I. Provision of emergency response program
- 40I. Qualification of ES&H Staff personnel

G. Staff Assurance Functions

- 1I. Monitoring of environmental conditions
- 2I. Review of Line organization ES&H plans
- 3I. Audits of Line ES&H operations
- 4I. Recommendation and verification of corrective action
- 5I. Performance and reporting of ES&H program evaluations
- 6I. Participation in ES&H impact analysis

APPENDIX B

Institutional Routine Accident Investigation Form

<i>Supervisor's Name and Signature</i>		<i>Accident Location and Organization</i>	
<i>Acc. Day of Week</i>	<i>Accident Date</i>	<i>Accident Time</i>	
<i>Brief Accident Description (Including Events) as Appropriate</i>			
<i>Number of Persons Potentially or Actually Exposed</i>			
<i>Potential or Actual Environmental Damage (by category)</i>			
<u><i>Program and Physical Analysis</i></u> <ul style="list-style-type: none"> ● <i>Hazards involved (by source)</i> ● <i>Previously recognized? (yes or no)</i> ● <i>Risk Factors involved</i> ● <i>Uncontrolled Risk Factors</i> ● <i>Inadequately controlled Risk Factors</i> ● <i>Control failures (if applicable) or failure to use controls</i> ● <i>Compatibility of controls with requirements and reliability judgments</i> ● <i>Change, if any, involved</i> ● <i>Program failures involved</i> 			
<u><i>Risk</i></u> <ul style="list-style-type: none"> ● <i>In view of occurrence, is risk still deemed acceptable by involved personnel if previous controls are used? (yes or no)</i> ● <i>If no, under what new conditions, or with what alteration in controls will risk be acceptable to you and your employees? (Use reverse side for answer.)</i> ● <i>Are there issues which, in your view, should be pursued by ES&H Staff personnel? If so, what? (Use reverse side for answer.)</i> 			

Discussion

As an important part of an institution's ES&H Assurance Program, the ES&H Staff establishes policy and practices for the investigation of all accidents either involving, or having the potential for involving, injury, illness, or damage. The model plan presented here illustrates how the policy and practices may be documented in a reasonably concise, but flexible, plan for accident investigations.

The philosophy of accident investigation in ES&H Assurance Programs possesses several novel features. In summary, these are as follows:

- A focus on the *acceptability* of risk rather than automatic corrective action. This approach recognizes that zero risk is unattainable and that traditional approaches often strive for zero risk by emphasizing the need for corrective action under all sets of circumstances. In the approach presented here, corrective action is required only if either
 - the originally proposed approach to achieving acceptable risk levels was technically inadequate (in view of the accident), or it was not properly implemented, or
 - the perceptions of acceptability have changed as a result of the accident.
- A focus on correcting *program* deficiencies (when they exist) that become evident as a result of the accident investigation. In theory, the ES&H Assurance Program, when properly implemented, should lead to a level of risk that is acceptable to those at risk, or whose environment is at risk, at any time.^{10,17} Thus, logically, when an accident occurs, either
 - the associated risk was (at that time) acceptable or
 - the program was deficient.

With this framework, a program analysis (carefully correlated with a physical accident analysis) is a natural requirement. If no program deficiencies are found, the question of whether or not new knowledge or changing perceptions of acceptability warrant changes in the definition of acceptable controls can be asked in a setting that is both "blameless" and not insistent upon automatic corrective action.

When program deficiencies are found that have led to the accident, emphasis is placed on correcting these so that the

technical deficiencies associated with the accident, *and others like them that might lead to similar or related potential accidents*, are controlled so that acceptable levels of protection are provided.

- The use of logical, interrelated, and self-limiting analysis techniques to investigate both the accident itself and the ES&H program. Program investigations are logically structured in a tree fashion to eliminate the pursuit of information that is basically irrelevant to finding the primary programmatic causes of the accident, if they exist. Only those primary areas of program deficiencies are sought during the accident investigation per se. The possible need for a full program audit when an accident has occurred is discussed elsewhere in this series of guidance documents (see References 2, 3, and 11).

In the case of the physical accident investigation, the approach discussed here parallels the ES&H analysis portion of the program planning process.¹⁰ This correlates automatically with the program analysis portion of the investigation and limits the scope of the physical accident investigation to those areas which support the program analysis. This is possible in ES&H Assurance Programs because of the requirement for well-defined ES&H analyses that are designed to lead to the definition of controls that have an associated level of risk that is acceptable.¹⁰ Following the same logic in physical investigations of accidents provides, in effect, an independent check of the adequacy of the ES&H analysis and the underlying program that produced it.

In an ideal setting, the basic aim of an accident investigation should be to learn, not to blame. Such an aim is fundamentally impossible in settings which strive *only* to find "deficiencies" and "correct" them. When deficiencies exist, of course, these need to be identified and corrected, but more fundamentally, one needs a definition of "deficiency" that distinguishes between such things as poor performance and a universal lack of knowledge. Blame should be attached to poor performance, but it should be possible to have an accident while having taken all "reasonable and prudent" actions that are expected to lead to an acceptable level of risk. If the latter is permitted to occur in a blameless way, then the process of learning from experience can be facilitated. Only in programs designed to

provide *evidence* that appropriate positive actions have been taken to limit risk to acceptable levels can such an approach be adopted. Thus, ES&H Assurance Programs can offer a rather different approach to the investigation of accidents.

Notes and References

1. This Standard occurs in several references. The first version was preliminary and was altered as a result of a broad review process. It is found in A. C. Ellingson, C. A. Trauth, Jr., and M. S. Tierney, A Proposed Standard for ES&H Assurance Programs, SAND79-0240 (Albuquerque: Sandia Laboratories, March 1979).

A version, revised as a result of this review, is given in A. C. Ellingson and C. A. Trauth, Jr., An Environment, Safety and Health Assurance Program Standard, SAND79-1536C (Albuquerque: Sandia Laboratories, October 1979).

and in

A. C. Ellingson and C. A. Trauth, Jr., An Environment, Safety and Health Assurance Program Standard: An Analysis in the Context of DOE ES&H Requirements, SAND79-1536 (Albuquerque: Sandia Laboratories, September 1979).

See also Reference 17, below.

References 2 through 16 are a part of a series generically entitled "Guidance for Implementing an Environmental, Safety and Health Assurance Program." Separate volume titles are as follows.

2. C. A. Trauth, Jr., A. C. Ellingson, and K. Marston, Volume 1. A Model Plan for Institutional Environmental, Safety and Health Assurance Programs, SAND81-0632 (Albuquerque: Sandia National Laboratories, June 1981).
3. A. C. Ellingson, Volume 2. A Model Plan for Environmental, Safety and Health Staff Audits and Appraisals, SAND81-0633 (Albuquerque: Sandia National Laboratories, September 1981).
4. A. C. Ellingson and C. A. Trauth, Jr., Volume 3. A Model Plan for Environmental, Safety and Health Staff Review Activities, SAND81-0634 (Albuquerque: Sandia National Laboratories, January 1982).
5. A. C. Ellingson and E. L. Gunderson, Volume 4. A Model Plan for Institutional Emergency Response Programs, SAND81-0635 (Albuquerque: Sandia National Laboratories, June 1981).
6. C. A. Trauth, Jr. and A. C. Ellingson, Volume 5. A Model Plan for Institutional Accident Investigations, SAND81-0636 (Albuquerque: Sandia National Laboratories, January 1982).
7. "Volume 6. Model Documentation for an Environmental, Safety and Health Assurance Information System," SAND81-0637 (Albuquerque: Sandia National Laboratories, to be published).
8. A. C. Ellingson, C. A. Trauth, Jr., and K. Marston, "Volume 7. A Model Plan for Institutional Environmental, Safety and Health Assurance Training Programs," SAND81-0638 (Albuquerque: Sandia National Laboratories, to be published).
9. A. C. Ellingson, C. A. Trauth, Jr., and L. M. Jercinovic, Volume 8. Model Guidelines for Line Organization Environmental, Safety and Health Committee Operations, SAND81-0639 (Albuquerque: Sandia National Laboratories, June 1981).

Notes and References (Continued)

10. C. A. Trauth, Jr. and K. Marston, Volume 9. Model Guidelines for Environmental, Safety and Health Analysis Activities, SAND81-0640 (Albuquerque: Sandia National Laboratories, June 1981).
11. A. C. Ellingson, Volume 10. Model Guidelines for Line Organization Environmental, Safety and Health Audits and Appraisals, SAND81-0641 (Albuquerque: Sandia National Laboratories, October 1981).
12. A. C. Ellingson and C. A. Trauth, Jr., Volume 11. Model Guidelines for Line Organization Environmental, Safety and Health Review Activities, SAND81-0642 (Albuquerque: Sandia National Laboratories, January 1982).
13. A. C. Ellingson, Volume 12. Model Guidelines for Line Organization Environmental, Safety and Health Inspection and Monitoring Activities, SAND81-0643 (Albuquerque: Sandia National Laboratories, September 1981).
14. A. C. Ellingson, C. A. Trauth, Jr., and L. M. Jercinovic, Volume 13. Model Guidelines for Line Organization Environmental, Safety and Health Meetings, SAND81-0644 (Albuquerque: Sandia National Laboratories, June 1981).
15. A. C. Ellingson, Volume 14. Model Guidelines for Utilizing Quality Assurance Support in ES&H Assurance Programs, SAND81-0645 (Albuquerque: Sandia National Laboratories, September 1981).
16. A. C. Ellingson and C. A. Trauth, Jr., "Volume 15. A Model Plan for Line Organization Environmental, Safety and Health Assurance Programs," SAND81-0646 (Albuquerque: Sandia National Laboratories, to be published).
17. C. A. Trauth, Jr., A. C. Ellingson, H. Hollister, and L. M. Jercinovic, A Program Standard for Assuring That Today's Management Obligations in Environmental, Safety and Health Areas Are Met, SAND81-1359C (Albuquerque: Sandia National Laboratories, June 1981).
18. Two papers are of relevance here. First, C. A. Trauth, Jr. and Jay B. Sorenson, "A New Approach for Assuring Acceptable Levels of Protection from Occupational Safety and Health Hazards," an invited presentation to the Southwest Labor Studies Conference held at the University of New Mexico, 1 May 1981.

The second paper is

Jay B. Sorenson and C. A. Trauth, Jr., "The Political Side of Risk: A New Approach," in the Proceedings of the 1980 Annual Meeting of the American Political Science Association, August 1980, Washington, D.C.
19. The National Environmental Policy Act (42 U.S.C. 4321 et seq.), as amended, and regulations issued by the Council on Environmental Quality (40CFR Part 1500, 36FC 20550).
20. The Occupational Safety and Health Act of 1970 (84 Stat. 1593, 1600; U.S.C. 655, 657), as amended.

Notes and References (Continued)

21. C. A. Trauth, Jr., A. C. Ellingson, D. E. Farr, and L. M. Jercinovic, A Study of the Application of Quality Assurance, Human Factors and Reliability Principles to the Prevention of Major Environmental, Safety and Health Incidents, SAND78-2176 (Albuquerque: Sandia Laboratories, December 1978).
22. A. C. Ellingson, Audit/Appraisal Guidelines for Organizational ES&H Assurance Programs, SAND79-1812 (Albuquerque: Sandia Laboratories, November 1979).
23. J. R. Buys and J. L. Clark, Events and Causal Factors Charting, DOE 76-45/14, SSDC-14 (Idaho Falls: EG&G Idaho, Inc., August 1978).
24. M. G. Bullock, Change Control and Analysis, DOE 76-45/21, SSDC-21 (Idaho Falls: EG&G Idaho, Inc., March 1981).

DISTRIBUTION:

U.S. Department of Energy (2)
Office of Environmental Protection, Safety
and Emergency Preparedness
Washington, DC 20585
Attn: Mr. Hal Hollister

U.S. Department of Energy (10)
OOS
Washington, DC 20545
Attn: Mr. Henry Rosenthal

U.S. Department of Energy
OQA
Washington, DC 20545
Attn: Mr. J. T. O'Connor

DOE -- Albuquerque Operations Office (6)
P.O. Box 5400
Albuquerque, NM 87115
Attn: Mr. J. R. Roeder, Director, OSD

Ms. Karen Marston (5)
Tech. Reps., Inc.
5000 Marble NE
Albuquerque, NM 87110

Ms. Kelly King (2)
Safety Sciences, Inc.
7586 Trade St.
San Diego, CA 92121

Mr. Leslie M. White
Safety Sciences, Inc.
291 G Street, SW
Washington, DC 20024

400	C. Winter
1220	J. M. Wiesen
1400	L. J. Heilman
1410	W. C. Kraft
1417	F. W. Muller
1418	A. C. Ellingson
1418	C. A. Trauth, Jr. (70)
3300	P. B. Mossman
3310	W. D. Burnett
3400	D. S. Tarbox
3440	L. M. Jercinovic
3442	D. L. Rost
3442	M. M. Carroll
3652	V. L. Duke
8275	P. K. Lovell
8214	M. A. Pound
3141	L. J. Erickson (5)
3151	W. L. Garner (3)
3154-3	C. Dalin (25)

DOE/TIC (Unlimited release)