

R. + B. Frei-Rischoff
Dättlingerstrasse 25
8406 Winterthur

SAN 821-2

UC-41

THE MANAGEMENT OVERSIGHT AND RISK TREE-MORT

**INCLUDING SYSTEMS DEVELOPED BY THE
IDAHO OPERATIONS OFFICE AND
AEROJET NUCLEAR COMPANY**

by

W. G. JOHNSON
Grandjean
Lowman, Idaho 83637
(4566 River Street
Willoughby, Ohio 44094)

Prepared for the
U.S. ATOMIC ENERGY COMMISSION
Division of Operational Safety
Under Contract No. AT(04-3)-821
Submitted to AEC
February 12, 1973

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Atomic Energy Commission, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, expressed 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.

Abstract

A Management Oversight and Risk Tree (MORT) has provided a technique for thorough, searching investigation of occupational accidents and analysis of safety programs. MORT has been used to improve safety in specific activities and in organizations. The announced goal is an order of magnitude reduction in already low accident rates or probabilities.

MORT is a formal, disciplined logic or decision tree to systematically relate and integrate a wide variety of safety concepts:

Sequential roles of energy, barriers to energy transfer, error, change and risk. From these:

A new, functional definition of an accident.

Present best safety practices, system safety technology, and behavioral, organizational and analytic sciences. From these:

Methods of enhancing safety form a dynamic safety system congruous with general systems for management of high performance.

Safety program features, some old and some new -- management implementation, hazard and human factors analysis processes, work processes, monitoring, information and organization systems and services. From these:

A structure and specific analytic questions to more fully utilize accident facts to improve the system.

Trials of MORT have shown an ability to assist persons from a discipline -- safety, management, engineering, sciences or other staff specialties and experienced craftsmen -- to quickly apply and broaden their skills in accident analysis and safety review, and have provided a common base for communication, cooperation, and planning for greater accident control.

At the same time, the disciplined MORT format has shown flexibility in rapid evaluation and assimilation of new experience, judgment, findings or technology.

Specific safety innovation and acceptance methods and projects have been outlined for transition to a comprehensive, superlative safety system -- for the long term a "safer way of life."

Details of program application are provided in text, figures, examples, appendices and exhibits.

Contents

	<u>Page</u>
Abstract	1
Preface	i
Abbreviations	v
I. <u>Introduction</u>	1
The Study Plan	4
MORT	13
II. <u>What Produces Hazards?</u>	25
1. Accident/Incident	27
2. Energy and Barriers	31
3. Frequency-Severity Matrices as a Management Tool	37
4. Error as Accident Cause	49
5. The Role of Change in Accidents	59
6. Sequences in Accident Causation	79
7. The Role of Risk Management	85
III. <u>How To Reduce Hazards</u>	93
8. Integrating System Safety with Present Best Practices	95
9. Method vs Content	103
10. Safety, Efficiency and Performance are Congruous	107
11. A Safety System as a General Management System	111
12. General Safety Program Theses	131
IV. <u>MORT</u>	133
13. Development of "Accident Tree" Analysis	135
14. The MORT Diagrams - Introduction	139
15. Definition of Symbols	143
16. MORT Charts	149
17. Fourth Generation of MORT	159
18. MORT Values, Styles and Obstacles	165
V. <u>Management Implementation of the Safety System</u>	173
19. Management Policy and Direction	175
20. Management Implementation	185
21. Risk Assessment System	205
VI. <u>Hazard Analysis Processes</u>	223
22. System Safety and Hazard Analysis	225
23. Hazard Analysis Process Defined	233
24. Concepts and Requirements--The Conceptual Phase	237
25. Design and Development Phase	267

	<u>Page</u>
Contents, continued.	
26. Human Factors Review	273
27. Design Organization, Reliability and Quality	281
28. Independent Review	283
VII. Work Flow Processes	291
29. General Schematic of Work Flow Processes	293
30. Supervision	297
31. Maintenance and Inspection	311
32. Procedures	315
33. Employee Selection and Training	325
34. Performance Errors	331
35. Employee Motivation, Participation and Acceptance	337
VIII. Information Systems	343
36. Technical Information	349
37. Monitoring Systems	351
38. Accident Investigation	375
39. The Organization's Information System	391
40. National Information Systems	411
41. Measurement Techniques	415
42. Management Assessment Methods	435
IX. Safety Program Review	445
X. Transition	457
Appendices	
Exhibits from Aerojet Trials	
Bibliographies:	
General	
Change Phenomena	
Human Factors Engineering	
Index	

Preface

This document was prepared under contract AT(04-3)-821 with the United States Atomic Energy Commission as Phase VIII of a study, "Development of Systems Criteria for Accident Reporting and Analysis and for the Measurement of Safety Performance."

The contract resulted from an original proposal by the author based on earlier developmental work while on the staff of the National Safety Council (NSC), consultation work for government and private organizations, and seminars conducted in Europe. In this latter connection two texts were prepared, "New Approaches to Industrial Safety" and "Product Safety" (1970), and these described much of the conceptual basis for the study.

The general proposal was as follows:

"The U. S. Atomic Energy Commission has exemplary programs for the control of accidents and fires, signalized by numerous awards. Its work in such areas as reactors, radiation, weapons, and research has developed new methods of controlling unusual and exotic problems, including safe methods of utilizing new materials, energy sources, and processes.

"Despite past accomplishments, human values and other values stimulate a continual desire to improve safety performance. Emerging concepts of systems analysis, accident causation, human factors, error reduction, and measurement of safety performance strongly suggest the practicality of developing a higher order of control over hazards.

"This is a proposal to formulate an ideal, comprehensive systems concept of accidents and their control, and to test the usefulness of the concept in two ways:

1. Design of improved accident report and analysis techniques.
2. Development of improved measurements of safety performance.

"The formulation of an ideal system appears to be a valuable precondition for knowing what information to seek after an accident and what aspects of performance to seek to measure.

"The judgments of 'improvement' in reports and measurements will be largely subjective, but will be formulated by representatives of three kinds of groups within the Commission and its contractors:

1. Professional safety staff,
2. First line supervisors,
3. Management (government and contractor).

"The criteria suggested to these groups will include:

1. Improved understanding of accident-producing situations and sequences.
2. Improved understanding of control systems (and gaps).
3. Practical usefulness (i.e., action potential) of certain questions and measurements:
 - a. on a day-to-day or other routine basis, or
 - b. for occasional review

"And for first line supervisors, two additional criteria:

4. Improved sensitivity to changes and error-producing situations.
5. Improved control over non-safety aspects of work.

"Some objective measurement of accident reduction may be feasible in the pilot phase.

"Although the formulation of an ideal systems concept seems a reasonable goal today, there is a substantial number of aspects warranting separate investigation and experiment, which preclude a full-scale test of a comprehensive system. Thus, two short-range, attainable goals -- reports and measurements with a systems flavor -- have been proposed above. Nevertheless, it can be expected that information and insight would be gained in the following major areas:

1. Methods of balancing the amount of safety analysis and risk management against the size of the risk. Specifically, is a requirement for formal systems safety analysis economically justifiable for major risks?
2. Methods of training, especially for supervisors. Specifically, can the logic and methodology of systems analysis be applied practically and economically to routine problems?
3. Role of change in causing error, and the classification of changes.
4. Role of errors in accidents, the classification of errors, and the congruence of errors, accidents and other degradations in processes."

Phase I of the study produced a draft text combining the best occupational safety practices, system safety concepts of the aerospace and nuclear industries, and other concepts advanced by behavioral and organizational scientists. Phase II produced a revised text based on an extensive literature search and critique by the NSC staff, and review by the Division of Operational Safety (DOS) of the United States Atomic Energy Commission (AEC).

In Phases III and IV of the study, emerging concepts were compared with safety programs of contractors at three AEC-supported research sites--Lawrence Radiation Laboratory, now Lawrence Berkeley Laboratory, of the University of California at Berkeley (Lawrence); Sandia Laboratories, Albuquerque (Sandia); and Idaho Nuclear Corporation at the National Reactor Testing Station near Idaho Falls (INC). Some concepts were tested preliminarily, a few concepts were adopted by contractors, and considerable useful data were compiled on effective operating safety programs as they might be compared with or contribute to even higher ideals of protection.

The most important result of Phases III and IV was the evolution of a new form of accident analysis and program evaluation, The Management Oversight and Risk Tree (MORT). This logic tree began as an effort to apply the Fault Tree (a system safety technique) to accident investigation, but developed into a method of evaluating program features, as well as the specific failures which led to accidents. MORT became the principal basis for organization and preparation of a manual (Phase V) for trial application of the system at Aerojet Nuclear Company (Aerojet) on the National Reactor Test Station, Idaho (Phase VI), and this latter phase is continuing.

Phase VII will consist of a series of four seminars or workshops (one has been held).

Phase VIII of the study consists of preparation of this text which incorporates results of an eighteen-month test, primarily in the Reactor Operations Division of Aerojet (successor organization to INC). Also incorporated are results of other consultation work (for example, for the National Transportation Safety Board (NTSB) and National Aeronautics and Space Administration (NASA), and further seminars at five European cities.

Purposes of This Manual.

The manual is intended to summarize the results of the study to date and form the basis for further applications of the concepts, either in whole or as separable concepts.

Accordingly, only so much of the detailed findings and experience in Phases I to VI as would contribute to understanding and application of the techniques has been included. Additional detail was included in interim reports to AEC on the earlier phases.

Credits.

Great credit is due the AEC for its willingness to undertake this study. AEC's occupational accident experience has been exemplary by comparison with general industrial experience, and equals the best performance of leading companies. The desire to further improve is most commendable.

Assistance of the National Safety Council staff in the form of literature searches and critiques has been invaluable. This manual incorporates many key concepts collected and developed by NSC staff in its training and publication programs. Advance papers and deliberations of the NSC Symposium on Industrial Safety Performance Measurement were also valuable.

A special debt to European friends is acknowledged. In January 1970, Industrial and Commercial Techniques Ltd. sponsored two-day seminars on "New Approaches to Industrial Safety" and "Product Safety" and the comments and experience of British safety professionals and management personnel were helpful. British injury trends have paralleled our own and they too seek improved methods. The seminars were extended to Switzerland and Germany in mid-1971, and to Amsterdam and the Danish AEC in late 1972, and the MORT analysis was utilized. Leading European business and government agencies are moving away from a primary emphasis on regulations toward a greater emphasis on system safety. For example, Royal Dutch Shell's new chemical complex in England is a valuable full-scale application of hazard analysis in private non-governmental work.

The Divisions of Operational Safety at AEC Headquarters and at the San Francisco, Albuquerque and Idaho Operations offices have given indispensable assistance, not just in arrangements, but in technical advice and critique, and in trials of new approaches.

Most particularly, the highest tribute should be paid to the staff members, both operational and safety, of the three research contractors (Lawrence, Sandia and Aerojet). These people are working assiduously and intelligently to control hazards in difficult research and development work. Their willingness to help evaluate present safety programs against new, high standards and ideals was an inspiration and a major contribution to this study.

Emphasis must be given to the point that the early work at the three sites was intended to test new methods of measurement, not to test programs at the sites. Could a measurement system be designed to cope with the varied programs at the

sites? Notwithstanding this purpose, an impression of judgment was often inevitable, and the temptation to offer recommendations was often present. Therefore, an explicit statement is in order, namely, their programs are outstanding by conventional standards.

The trial at Aerojet (still continuing) has been extremely valuable. The author was fortunate that Aerojet was chosen for the trials because Aerojet already had extremely low accident rates and had in place many of the program elements which had been incorporated into MORT. Further, some features of Aerojet's program could be assimilated in their entirety to fill weak spots in the prior MORT analysis; independent review is an example. Other concepts in MORT were greatly improved in the process of adaptation to Aerojet use.

Fred McMillan, Manager of the Reactor Operations Division (ROD), brought intelligence and determination to his effort to "buy as much of the book as I can afford." Richard O'Brien, Manager, Nuclear and Operational Safety Division (NOS) and his staff were always cooperative and helpful. Dr. John Morfitt chaired an advisory committee which gave excellent counsel.

Dr. Robert J. Nertney and Jack Clark of NOS, and Jack Ford, McMillan's assistant, with the author, made up the MORT Team. Without the energy and skill of these three associates, progress in developing MORT would have taken much longer. Bob Nertney's prior work on human factors, as well as his energy, imagination and intelligence were invaluable.

Many of the contributions of Aerojet and its employees are specifically acknowledged in the text, but there are dozens of others which helped polish and develop MORT concepts. Warm friendships with AEC and Aerojet personnel have been an extra bonus from the trials.

The author has also appreciated the efforts of safety staffs of NASA, NTSB, the U.S. Geological Survey, and the National Bureau of Standards, whose critique, exploration and use of MORT helped both improve and validate concepts.

A general tribute should be paid to the vast efforts of members of NSC and the American Society of Safety Engineers (ASSE) whose publications and discussions made numerous contributions which are acknowledged in the text.

The permissions of publishers for use of copyrighted material is gratefully acknowledged. Two management texts--J. M. Juran's Managerial Breakthrough and Kepner-Tregoe's The Rational Manager, both published by McGraw-Hill Book Company--provided substantial additions to safety methodology, as evidenced by numerous citations, the Juran figures reproduced by permission.

Synthesis.

Synthesis of concepts is a dangerous business, particularly when research has been sparse and poorly funded. However, a synthesis of best practices may be a helpful precondition for further research and for assimilation of new ideas, as relevant variables are more clearly perceived.

The responsibility for this particular synthesis rests with the author, not with those whose ideas and concepts have been so freely appropriated.

Abbreviations

Aerojet	Aerojet Nuclear Company
AEC	U. S. Atomic Energy Commission
ANC	Aerojet
ANPP	Aerojet Policies and Procedures
ANSI	American National Standards Institute
ASSE	American Society of Safety Engineers
DOD	Department of Defense
DOP	Detailed Operating Procedure, Aerojet
DOS	Division of Operational Safety, AEC
DOT	Department of Transportation
FS&OC	Fire Safety and Adequacy of Operating Conditions list, AEC
HAP	Hazard Analysis Process (p.223)
HIPO	High Potential Incident (p.233)
HP	Health Physics
I/B/V/T	Investment/Benefit/Value/Threat (p.256)
INC	Idaho Nuclear Company (predecessor to Aerojet)
JIT	Job Instruction Training (p.317)
JSA	Job Safety Analysis (p.317)
JSA-JIT-SO	Safety Observation plan (p.317)
Lawrence	Lawrence Radiation Laboratory, University of California, Berkeley (now known as Lawrence Berkeley Laboratory)
LC	Life Cycle (p.225,263)
MORT	Management Oversight and Risk Tree
NASA	National Aeronautics and Space Administration
NFPA	National Fire Protection Association
NOS	Nuclear and Operational Safety Division, Aerojet
NRTS	National Reactor Testing Stations, Idaho Falls, Idaho
NSC	National Safety Council
NSIC	Nuclear Safety Information Center, Oak Ridge, Tennessee
NTSB	National Transportation Safety Board
OSHA	Occupational Health and Safety Act (Administration)
PJA	Pre-Job Analysis (p.293)
PPL	Priority Problem List (p. 435)
R & QA	Reliability and Quality Assurance
ROD	Reactor Operations Division, Aerojet
RSO	Recorded Significant Observation (a critical incident)
Sandia	Sandia Laboratories, Albuquerque, N. M.
SAR	Safety Analysis Report, AEC
SOP	Safe Operating Procedure (Sandia)
SP	Safe Practice (divisional), Aerojet
SPIP	Safety Program Improvement Projects (Exhibit 17)
SPS	Safety Precedence Sequence (p.225)
SWP	Safe Work Permit, Aerojet (p.332)
T & Q	Test and Qualification

I. INTRODUCTION

Many leading employers have attained low occupational injury rates.
However, after some four decades of accident rate decline, a plateau, followed
by a decade of upturn in the rates, has been a widespread experience both in
the U. S. and abroad.

Occupational injuries in the U. S. had the following results in 1971¹:

Death -- 14,200 persons

Permanent impairment -- 90,000 persons

Temporary total disabilities -- 2,200,000 persons

In addition (with some discontinuity of definitions), occupational injuries which were "not bed disabling" had the following effect:

Activity restriction -- 2,635,000

Medically attended -- 3,912,000

Thus a total of some $8\frac{1}{2}$ million of 79 million people experienced pain and suffering ranging from slight to disastrous from occupational injury. First aid cases (not medically attended) would further swell the totals. And, if we knew the facts about occupational-related health problems, the numbers would further grow.

Tabulatable economic losses born by employers and employees totaled \$9,300,000,000. This is only an accumulation of selected costs for which data are available. True costs are certainly substantially higher.

Accident costs are only a fraction of total error costs, if we consider together the errors which produce both accidents and other losses.

The data include agriculture and self-employed, largely outside the purview of employer-based programs. Further, employer-based programs of the historic types have had little effect in organizations (business and other) with 5 or 25, or even 100 employees. The Occupational Health and Safety Act (OSHA) is currently having impacts in this type of establishment.

These shocking losses occur despite the occupational safety progress in this century. Indeed the losses have increased in recent years.

Death rates in U. S. manufacturing hovered at 9, 10, or 11 deaths per 100,000 workers for the years 1960-71. However, in non-manufacturing, death rates declined from 25 to 20, perhaps because non-manufacturing organizations only recently began use of preventive techniques earlier applied in manufacturing.

NSC member rates for fatalities and permanent disabilities continued to decline during the plateau period, but as temporary disability rates increased

1. Accident Facts. National Safety Council, 1972 edition.

by 62% in ten years, the more serious injury rates seemed to move to their own plateau.

Large companies with the best programs have not found that "more of the same" renews progress. The situation has been the cause of widespread concern in business and government. (See, for example, "Has Safety Progress Ended," National Safety News, October 1969, or in great detail, the hearings on OSHA.) OSHA itself is reaction to the apparent inability of the safety community to deal constructively with the plateau and upturn.

Thus, accidents (despite low rates in some organizations) produce significant numbers of injuries to people, result in substantial economic loss, and have been generally increasing.

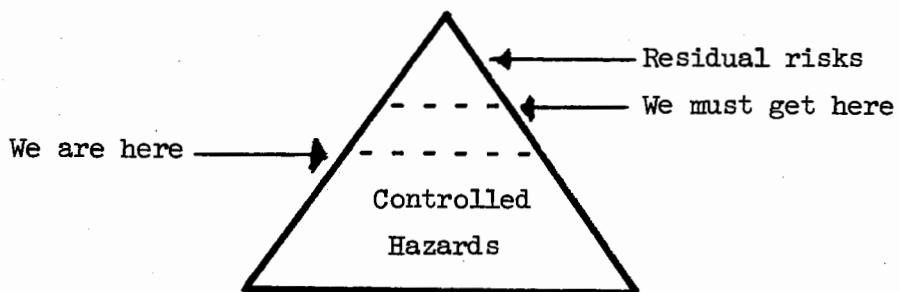
Our concern for improved preventive methods, nevertheless, does not stem from any specific, describable failure of old methods as from a desire for greater success. Many employers attain a high degree of safety, but they seek further improvement.

It is increasingly less plausible that the leading employers can make further progress by simply doing more, or better, in present program. Indeed, it seems unlikely that budget stringencies would permit simple program strengthening. And some scaling down in safety expenditures (in keeping with other budgets) may be necessary.

Consequently, the development of new and better approaches seems the only course likely to produce more safety for the same or less money.

Further, a properly executed safety system approach should make a major contribution to the organization's attainment of broader performance goals.

Figure I-1. How Can We Climb Toward the Summit?



Improved methods for attaining high ideals of safety are available today. They set a high and different goal: First Time Safe. The records of the weapons, space and reactor programs attest to the effectiveness of the methods.

We cannot enter some new areas of human activity on the basis of the traditional safety approaches. You simply cannot get to the moon by examining

the ashes of failures!

System safety concepts have been highly developed by AEC and the Defense and Space agencies and their contractors. Existing contract and licensing specifications require forms of risk analysis and evaluation which provide a high degree of protection of both systems and personnel, where necessary, by complex and sophisticated methods.

Some concepts more or less new to safety can be borrowed from other fields of control of work, such as reliability, quality and error control, or the broader field of management science.

An improved order of occupational safety system seems possible if the best of present practices is synthesized with the emerging system safety practice and the concepts articulated by behavioral scientists, including those studying organizational systems. Better understanding of technologic and organizational sciences, as well as of the exponential effects of change, is necessary.

If we say that safety is a special aspect of reliable control of work, we take a giant step toward useful orientation toward management's objectives in public or private enterprise. When we use a concept that accidents are one member of the broad family of errors and malfunctions, we take two additional steps: first, we show awareness of management's problem of control; and second, we open the literature on error control for safety adaptation. Errors are easier to study than accidents. On the other hand, observation of errors requires a more active, comprehensive and sophisticated recording system.

The new approaches hold great promise for renewing safety progress recorded prior to the last fifteen years. Some new approaches are more soundly based in the management process, as well as technically superior. They deal more realistically with the most difficult variable, the human. Most important, they may give insight into a safety process which helps all of us to more rapidly evaluate our own experience and those of others, and assimilate new ideas.

The concepts of an improved order of occupational safety system, an ideal, can help establish criteria and methods for measuring safety performance. The concepts can also guide accident investigation and analysis to obtain the facts needed to renew safety progress.

Industrial application of system techniques, particularly for new projects, is needed even though we cannot redesign and rebuild all plants. A considerable number of essentially new concepts and procedures are available today for use individually or collectively to build greater control over work

hazards, and thereby upgrade conventional safety programs. New plants, products, machines and materials provide a heavy flow of opportunities for use of improved concepts.

The emphasis in this text is on occupational safety, but applications of system safety to product, public, transportation and environmental accidents are also desirable and practical.

Goals of the Study.

For the study title, "Development of Systems Criteria for Accident Reporting and Analysis and for the Measurement of Safety Performance," an extremely high goal was conceptualized:

An order of magnitude reduction -- minus 90% --

For already low accident rates and probabilities -- by a
System congruous with management for high performance.

. Safety programming can be visualized at five levels:

1. Less than minimal compliance with regulations.
2. Minimal compliance with enforced regulations.
3. Application of manuals and standards.*
4. Advanced programming exemplified by AEC and leading industries.**
5. System safety, or as developed herein, a safety system (perhaps a sixth level).

There are enough data to suggest that the levels of programming may produce order of magnitude differences in annual rates for events disastrous to the enterprise, along the following lines:

<u>Program Level</u>	<u>Disaster Probability</u>
1. Sub-minimal	1×10^{-3}
2. Minimal	5×10^{-4}
3. Manuals*	1×10^{-4}
4. Advanced**	1×10^{-5}
5. Systems	1×10^{-6}

The reactors, for example, appear to have attained the fifth level of excellence.

On the other hand variables of size and difficulty cloud the data. Small organizations have some advantages, as well as disadvantages. For example,

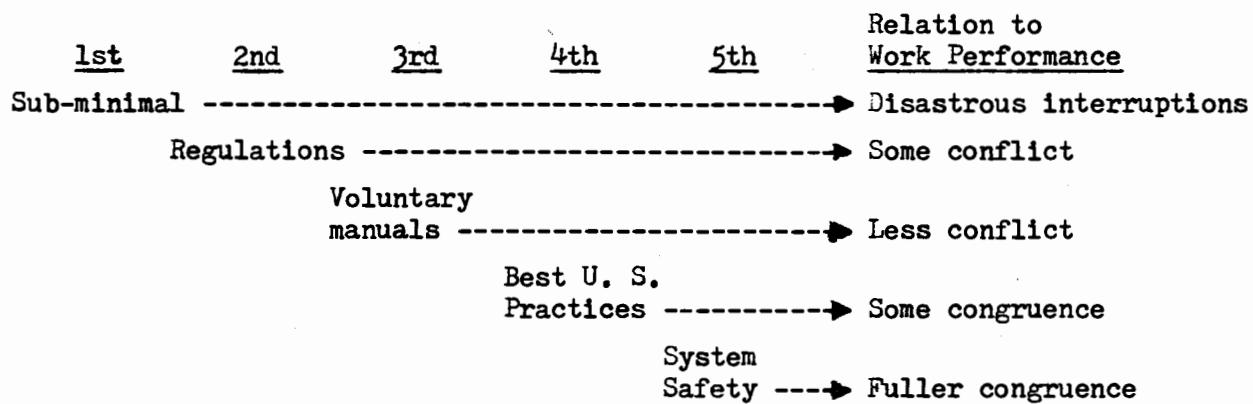
* For example, NSC's "Accident Prevention Manual for Industrial Operations."

** For example, ASSE's Bibliography (1967) may be a guide to this and to systems, but only as a reference list.

small size favors personal communication about hazards, but almost precludes professional or sophisticated hazard analysis. Activities which cross technologic borders -- e.g., a round trip in space -- may increase probabilities of major and disastrous events, even when fifth level techniques are used to achieve performance.

The relation of safety programming and performance requires further conceptual study, but a useful picture seems to emerge, as portrayed in the following figure:

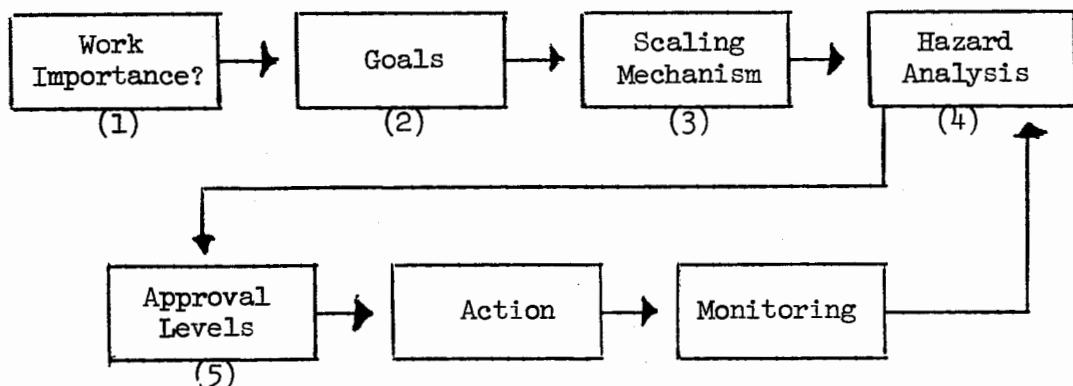
Figure I-2. Safety Program Levels.



Accidents are congruent with errors, and safety can be congruent with reliable control of work, that is, performance. Therefore, the superlative safety program can be a means of assuring attainment of general performance objectives.

A schematic which leads to intelligent and rational risk reduction or acceptance begins to show how greater safety can support performance:

Figure I-3. Safety Action Sequence.



From this, some questions:

- (1) Is the work important? How important? How certain do you want to be that things won't go awry?

- (2) Can you state performance and safety goals in probability terms?
- (3) Do you have a rational classification mechanism whereby the organization knows what level of safety effort is desired?
- (4) Have you defined the nature of hazard analysis?
- (5) Do you have definitions as to level of approval required for residual risk reduction or acceptance?

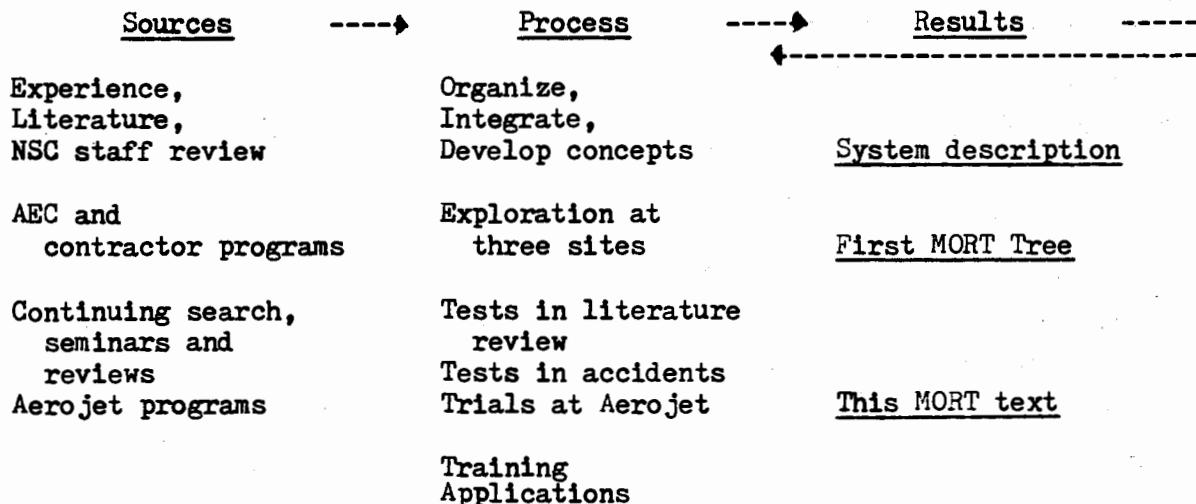
As with so many system processes, the action sequence in Figure I-3 may provide useful feedback to the safety program levels shown in Figure I-2. The most advanced organizations should show the congruence of safety and performance, and lead the way in methods. Then the organizations which lag and show the greatest opposition to OSHA's minimal regulations may gain insight and motivation for higher levels of performance planning. These can go well beyond OSHA levels of protection, and can aid and abet high performance.

Current pressure for alleviating OSHA impact may be doubly misdirected. It would weaken protection of people, and it would negate the desired relation of safety to high performance.

On the other hand, current emphasis on OSHA can impair the pursuit of excellence -- and greater excellence in safety programs is unquestionably the long-term requirement for balanced emphasis on enforcement and voluntary approaches. (A recent British study by a national Committee on Safety and Health at Work emphasizes need for strong voluntary programs to complement and support enforcement.) The goal -- a more effective safety system -- is of major importance to the proper role of enforcement as well as to voluntary leadership.

The Study Process.

The study has consisted of a series of cycles -- input-processing-output -- each output being used in the succeeding phase. Briefly, the major phases were as follows:



The type of work shown in the initial phase has continued throughout the project.

Sources.

In the mid-60's the accident rate plateau (in traffic and other fields, as well as occupational) motivated the NSC staff to search for and endeavor to apply the system safety techniques which developed in aerospace programs.

To this effort was coupled trial use of systematic methods of changing behavior in larger groups, even the general public, by such techniques as human factors study and "Innovation Diffusion," which latter seemed effective in the earliest efforts to build acceptance of seat belts (See Appendix H).

Simultaneous recognition of two related developments - the apparently exponential effects of changes over time, and a problem solving technique based on change detection (Kepner-Tregoe, 1965) - led to a 1967 presentation to the NSC, "Effects of Changes Time Exponential." However, the implied needs for more effective action were vast and somewhat vague, and action implications were not clear.

The NSC staff did develop a "system safety" short course which covered these diverse elements - aerospace techniques and behavior and change control - but practical applications back on the job did not seem to follow. The author's British text and seminars, "New Approaches to Industrial Safety" (1970) represented a further effort to crystalize and apply these emerging ideas, but again rapid application has not been evident.

Simultaneously there was increasing concern over the limited usefulness of existing measurements of safety performance, as exemplified by the NSC symposium (1970). Most important for this study, AEC-DOS desired a searching reexamination of AEC's occupational accident report and analysis systems which conformed with and also exceeded national standards, but had been largely unreviewed for some time.

Thus, the five factors which principally contributed to both motivation and substance of this study were:

1. A plateau, and an upturn in rates,
2. Dissatisfaction with traditional measures of performance,
3. Successes with system safety,
4. Change control as an increasing need,
5. Behavior and organizational science findings.

The literature of the National Safety Council (NSC) and the American Society of Safety Engineers (ASSE) provided a wealth of material. The exten-

sive bibliography appended to this text shows the wide range of other sources utilized.

AEC Program. Findings in this study are believed applicable to safety generally; the illustrations and conclusions are drawn so largely from nuclear energy research operations that a general picture of AEC occupational safety programs is useful as a backdrop.

Contractor occupational safety programs are governed by AEC policies and directives and monitored by AEC staff. Consequently, a general description of AEC requirements serves as a framework for study of contractor programs.

Patterns of health and safety responsibilities have generally distinguished or separated:

1. Weapons safety,
2. Reactor safety (including criticality in general),
3. Radiation safety and health,
4. Occupational safety, including fire, motor vehicle and damage accidents,
5. Environmental impact.

This study is primarily concerned with the occupational safety category. However, many features of "system safety" are already utilized in the first three categories and could be more fully transferred to the occupational field; conversely, an analysis of system safety for general occupational purposes is seeming to suggest improvements for the other four programs.

One focal point of AEC program is the extensive list of standards provided by AEC Manual Chapter 0550, "Operational Safety Standards." In both its length and its comprehensiveness, the list is equal or superior to that of any other organization. By including as recommended standards certain comprehensive manuals, the scope is extended well beyond the physical aspects and embraces management policy and support, organization, staff, training, communications, inspections and measurement of performance.

Further, the AEC program requires periodic appraisals of contractor safety programs. (Chapter 0504.)

Accident investigation and reporting requirements (Appendix 0502) fulfill and exceed national standards. Requirements for Boards of Investigation and in-depth investigation of serious events are exemplary and unique, and provide good examples of investigation. A "Serious Accident" newsletter, and many technical bulletins disseminate special information.

The variety and number of AEC conference-training-standards meetings (e.g., conventional explosives, plutonium, or pressure vessels) is so great as to suggest a central focal point for control, coordination and further develop-

ment of such opportunities for professional growth and internal standards.

Not surprisingly, line management responsibility from the first level of contractor's supervision to the General Manager of AEC, and thence on to the Commission and the Congress, is highly defined and responsive to both needs and opportunities. For example, the AEC's priority problem lists, called "Fire Safety and Operating Conditions" lists have received heavy management pressure to identify and correct risks (and do much of this from current operating budgets), an excellent example of management vigor in pursuit of safety!

The AEC program is an example of the best of present occupational safety practice, and has been adequate to earn for AEC many well-deserved awards. But, it does not generally require for occupational safety the forms of analysis and action utilized in "system safety" and exemplified in major space, weapons and reactor programs. Thus, for example, there are few non-nuclear requirements for life cycle analysis, documentation of analysis, hazard review milestones, change review, or trade-off analysis of additional countermeasures.

In addition, AEC and its contractors suffer from the same information system deficiencies identified in the aerospace and national safety information networks.

Three examples of system safety practice, two positive and one negative, can be given.

1. The AEC reactor safety program embodies system safety characteristics, although it has had its own special terminology rather than the jargon of the aerospace industries. Reactor safety uses Safety Analysis Reports and supporting documentation, change review, life cycle analysis and independent review.
2. Another positive example, "Safety Guidelines for High Energy Accelerator Facilities," (1967) reflects many system safety requirements -- trade-off criteria, life cycle analysis, periodic review, multiple safeguards, procedure and personnel requirements, monitoring, emergency plans, etc. This pamphlet provides principles which are not being applied to other areas of AEC work.
3. A negative example, AEC has a requirement for an appraisal of safety in the preliminary stages of new construction proposals. From a 1969 meeting of field safety directors it could be gleaned that the procedure was not working well. However, probably of greater significance is the low conceptual level embodied in the appraisals. For example, a proposal for a cafeteria addition said, "No new hazards will be created." Obviously this is almost the exact opposite of the life cycle analysis which might be started by answering the question, "How many accidents to employees or customers can be prevented during the life of this facility if design features are changed?"

Some research and development work undertaken by AEC contractors involves high energy and is work close to boundary conditions. Therefore, high orders of

system safety practice are, not only needed for safety, but may also make possible advanced research work.

AEC has more fully integrated staff organizations for the range of safety problems encountered than do some of its contractors. Where weapons, reactor or other aspects of safety are organizationally divided, there is not always full exchange of information on analytic techniques and competencies.

During this study there has been much evidence of applicability and need for fuller exchange between reactor, weapons, radiation and other safety programs. Indeed a system approach to occupational safety problems seems to offer considerable potential for improvement in all fields, including the augmented concern for proper waste management. All of the special kinds of accidents have common features.

Trials at Aerojet. Aerojet Nuclear Company, whose AEC contract provides for operation of experimental reactors at the National Reactor Testing Station, Idaho, was chosen as a site for trial of MORT techniques. Lest there be any impression that Aerojet was less than excellent prior to the 1971-72 year of the trials, it is well to cite some data (including data from predecessor companies, Phillips Petroleum and Idaho Nuclear):

Average employment, 1966-71 = 2,170.

ANSI Injury Rates:	1951-70	1966-70	1971	Chemical Industry
Frequency rate	0.70	0.81	0.48	4.01
Severity rate	124	63	16	433

The organization has never had a fatality.

Awards to the Phillips-INC-Aerojet succession (much the same staff) are numerous, including:

The Idaho championship! A 12-million man-hour no-lost-time injury awards, December 4, 1962 to January 14, 1966.

Idaho and AEC awards - 2 million man-hours, November 1966 to March 1967.

NSC Award of Honor for 1970.

Idaho award - million man-hours, ending October 1971.

The bus transportation system operated by Aerojet has earned driving and occupational injury awards.

Aerojet already had many features of the system which was evolving -- hazard analysis process, analytic capacity, procedure, reliability and quality assurance, monitoring, human factors studies and independent review.

NASA and NTSB. The publications and staff advice of the National Aeronautics and Space Administration, especially in system safety, and of the National Transportation Safety Board, in investigation, had major significance.

Disciplines. In addition to various occupational safety specialties, including fire and industrial hygiene, the work profited from publications and discussions with a wide range of other groups -- managers, university and other researchers, nuclear and system safety engineers, mathematicians, biophysicists and health physicists, information scientists, reliability and quality assurance engineers, and others.

Degree of Proof. By and large the system is an assemblage of individual ideas with varying degrees of proof. Many concepts are proposed safety applications of general theory developed by related sciences, e.g., behavior or organization.

An ordering of the degrees of support for a specific idea or component could be:

1. Scientific evidence:

- a. Safety application, e.g., human factors engineering.
- b. General theory (not specifically safety), e.g., acceptance of innovations.
- c. General safety theory generated from findings, e.g., Haddon's energy barrier notion.

2. Intermediate proofs:

These could include widespread, strong convictions of values, e.g., Job Safety Analysis in steel and other industries; literature search as a standard practice in science; or codes, standards, and regulations in safety law and practice.

3. Minimal proofs:

This would include some, a few, or a single closely related usage with some proof of value, e.g., trend analysis without controls or managerial opinion based on stated criteria, and includes some traditional approaches largely untested.

4. Logic or common sense.



to fill gaps.

5. Innovative hunch.

In MORT the emphasis has been to utilize ideas as far up in the hierarchy as possible, but at the same time, fulfill the logical requirements where necessary.

Processes and Results.

A foundation text developed in the first six months of the study endeavored to assemble and integrate the main factors found in the best industrial practices and in aerospace system safety. In addition, literature and experience with concepts of energy, energy barriers, error, change, sequence and risk were examined and developed, particularly as they related to a functional definition of accidents. Behavioral and organizational sciences were screened for relevant material. And the effort was to create an integrated whole.

The earliest focus was on accident investigation and reporting. It quickly became apparent that conventional, mass methods of report and analysis (ANSI and other) were sterile and unsuited to any superlative system, that a multiplicity of measurements were needed, and that, if safety program standards were only partially defined, the subsequent measurement of program failure would be vague and imprecise.

In the first exploratory phases at three research sites it was clear that traditional methods of investigating and reporting accidents could not be tinkered into useful measurements of a comprehensive program. A shocking absence of useful literature on methods of investigation had been noted earlier.

The result was development of the Management Oversight and Risk Tree (MORT). In addition to present best practice and system safety, MORT endeavored to integrate safety concepts into a coherent whole. Fundamental to the logic was a stated concept:

"Since management (specifically the Chief Executive Officer) has the legal and moral responsibility for safety, it follows that safety information and measurement programs should be primarily designed to answer the critical safety questions of management:

1. What are the nature and magnitude of the organization's accident potentials?
2. What has been done to reduce risk?
3. What is the long-term level of residual risk?
4. What additional measures to reduce risk have been considered and rejected on "practical" (investment/benefit/value grounds?)
5. Are the safety programs and systems actually operating as described in manuals and procedures?"

The format and logic of the Tree at that point (Monograph of April 27, 1971) were very much the product of the first text plus the particular accident/incident events investigated or reviewed. (Later Aerojet scientists were to push for tightening and clarifying the logic.)

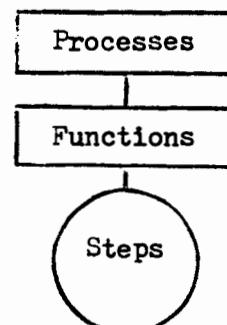
The exploratory phase also revealed many analytic methods of assuring reactor and weapon safety which deserved application in occupational safety.

MANAGEMENT OVERSIGHT & RISK TREE

MORT is simply a logic or decision tree which structures causal factors and/or preventive measures in an order which:

1. Makes explicit:

- a. The functions necessary to complete a process,
- b. The steps to fulfill a function,
- c. Text references to criteria to judge when a step is well done.



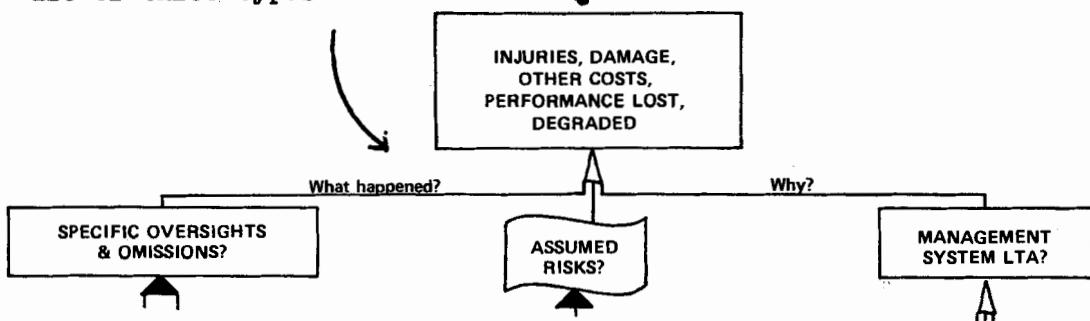
2. Provides relatively simple decision points, in analysis or review, albeit a lengthy list.

3. Enables an analyst or reviewer to detect omissions or defects in a process (or in the tree itself).

MORT began as an investigative tool, but has shown value in program appraisal and application.

The structure of MORT organizes the largely unstructured safety literature and practice.

Causes of adverse consequences are of three types:



LTA = Less than adequate

(At this point, a reader not familiar with the tree would probably be wise to quickly review at least the first page of the detailed diagrams in Chapter 16.)

The trials at Aerojet began with a series of "Safety Program Improvement Projects" (SPIPs), initially 25, and later 29, separable MORT concepts which were relevant to Aerojet problems.

The use of the SPIPs is discussed in the chapter on Transition. However, here it should be noted that the projects were parts of MORT system, but responsive to Aerojet's expressed needs. In that sense there was no overall trial of MORT as such, rather there was use of MORT parts to see how an excellent organization could further improve.

An illustration of the symbiotic relationship of Aerojet's systems and MORT is highly indicative. Aerojet's independent review system is superlative, and filled a gap in MORT. MORT, on the other hand, shows that independent review is no substitute for a defined upstream hazard analysis process, and can only be a check on the process. Thus, both Aerojet systems and MORT improved through interaction.

Aerojet also showed clearly the need for a multiplicity of measures of performance for different programs, and this led to the construction of the first "War Room" to display data on safety plans, results and problems.

In the long run, the most important contribution of Aerojet may have been to provide a situation in which the model for a general and idealized safety system, congruous with management methods, could develop from the embryo systems outlined in various of the author's publications from 1967 to 1971.

Dynamic Safety System. The model of this system (described in Chapter 11) uses the elements of MORT to construct a more positive, interacting, cyclic process akin to good management systems. In a sense the dynamic safety system is a positive view of the negative, failure-finding MORT process.

The trials have moved rapidly if one enumerates the specific developments, but slowly in test of the whole MORT system. Each concept had to be carefully incorporated in a real-life system and MORT is not just a system, but a "way of life," as one Aerojet scientist said.

What was expected from trials of MORT at Aerojet? -- very little in scientific evidence, and intermediate proof, except this: the trial is a single case, but more variables are controlled. Therefore, the single case,

plus prior evidence from other uses, might establish an intermediate proof or conviction.

As minimal proof, subjective opinion of managers or safety or technical personnel are the primary basis. This can be subdivided into several question:

1. Can the safety operation be performed, and how?
2. How costly is it?
3. Does it seem effective?
 - a. For safety?
 - b. Does the place seem to run better, with better performance, and fewer troubles?
 - c. Are there any trend or comparative data?

In short then, the primary results to be expected from the trial were minimal proof, but the differences from general safety development will be at least two:

1. Practicality:
 - a. Is it possible to use Information Search, Job Safety Analysis, Human Factors Review, NASA-structured analysis or review, review with criteria, etc., all in the same context?
 - b. Do total costs seem reasonable?
2. Effectiveness - in an already highly developed system:
 - a. Do results seem good for safety?
 - b. Do results seem good for general performance?

This might mean, using actual quotes from AEC and Aerojet personnel, that "accident investigation reports seem to be considerably better," or "the craftsmen laid more requirements on themselves in a job safety analysis than we would have dared to prescribe, and they enjoyed the work." Or, with respect to general performance, a safety-related effort (e.g., functional schematics, steps, and criteria) seems useful in general management. Or, general management doctrines are useful in safety (Juran's Control Cycle and Kepner-Tregoe's Problem Analysis) and in turn these contribute to overall management.

Aerojet executives have been careful to say that the trials do not yet provide a basis for endorsement of MORT, but have provided encouraging results and they believe it is "the way to go."

A four-day workshop for AEC headquarters and field safety personnel held at Aerojet helped improve organization, presentation, support and application of MORT.

Any final proof of MORT as a whole may be long-long-term, because it is a "way of life." Many, small tightly-controlled experiments, as well as overall applications of the synthesis, would be needed.

On the other hand, MORT is a synthesis of ideas and facts, and the possibility of another type of proof is emerging, namely from use of the entire system or synthesis. This, taken with the support for individual components, might lift MORT to the status of a tentative general theory and practice.

Indirect proof of usefulness of the overall MORT framework is frequently provided by the easy assimilating of new findings reported in current literature. This also emphasizes flexible and open-ended qualities predictive of further development.

Developmental work has been largely qualitative. Quantification has been feasible in only limited areas, for example, in numbers of causal factors revealed by MORT, in error and omission rates, and in exploring predictive measures. Certainly more data are needed, particularly for a wider range of organizations. However, many omissions of safety measures, e.g., failure to make an information search, human factors study, or independent review, create "uncertainties" which will likely remain difficult to quantify.

Organization of the Text.

In Part II of this report, What Produces Hazards? the concepts of energy barriers, error, change and sequence are developed. This leads to a new, more functional definition of accidents. The frequency-severity matrices which develop from energy relationships are defined and explored as management tools to focus on the vital sources. Basic risk management concepts are introduced.

These concepts require rather more exposition than would be feasible in presenting the MORT logic, and also form background for some of the structure of MORT.

In Part III, How to Reduce Hazards? methods of integrating system safety with present best practices, the value of visible analytic method to handle content or subject matter, and the congruous relationship of safety and performance are discussed.

A model of a general safety management system is developed and shown to be congruous with a variety of general management systems. This major proposition has been only partially tested, but stems from findings that certain accidents are more nearly escapees from managerial controls than conventional safety problems.

Part I and II results are then used to develop a set of general theses as to the nature of a safety program.

These concepts also help provide background for understanding the structure of MORT.

Part IV, MORT, describes the development of the Tree and the detailed analytic logic, as well as a discussion of values and problems.

The MORT diagrams of management systems provide the outline for the remainder of the text.

In Part V. management policy, implementation, and decision are discussed.

Part VI, the Hazard Analysis Process, includes human factors review and risk analysis, aspects of special importance.

Part VII covers Work Flow Processes and includes control over the upstream processes by which work ingredients -- things, people, procedures and supervision -- are developed. The important matters of employee motivation, participation and feedback are discussed.

Part VIII takes up Information Systems, beginning with design of monitoring plans which will produce the needed data (conventional accident reporting systems do not and cannot do this). Data reduction and control over fixes provide the ingredients for a management "War Room" which serves as the control center for safety. Local and national information network capabilities and deficiencies are also discussed.

Part VIII also discusses some techniques of measurement and assessment -- accident investigation, rate and incidence analysis, group cause analysis and program and control evaluation. These also provide exhibits for the War Room. It is common to assert that accident investigation is "first and fundamental," which is true. We come to the subject rather late, but we now know the kinds of information to seek.

Part IX discusses safety program review and describes the deplorable lack of program definition and data which not only make measurement difficult, but operate to shift blame to supervisors and operators rather than management and safety professionals.

Part X, Transition, discusses some experiences, particularly Aerojet's, in attempting the difficult transition to new, high levels of performance, the superlative, and suggests steps to be used.

Terms with special meaning and definition, the seemingly inescapable jargon, are listed in the Index with references to the pages which define the terms. Some terms are also included in the list of Abbreviations up front, again with page references to definitions.

Scope of Application.

At the outset of this study the scope was occupational safety, that is, employee injury, plant property damage and fire. It was suspected that improved methods would, however, be applicable to other kinds of accidents -- nuclear, radiation, industrial hygiene and waste management.

Since the author had no expertise in the latter areas, a practice was followed of awaiting views of others on MORT applicability in their fields of specialization.

One early MORT analysis was "High Level Spill at the Hilac" (see Appendix A-1), a radiation event being chosen simply because it was serious and there was a good report.

Later, considerable methodology was absorbed from the safety programs for nuclear weapons and nuclear reactors.

As the study proceeded, the nature of waste management accidents suggested that MORT was clearly applicable to the analysis of sudden system failures in waste control; that is, large, unplanned discharges are accidents in every sense. One example was a clear-cut failure to consider human factors and errors, certain to occur in time. Waste management literature and practice seem weak in this area.

MORT draws heavily on aerospace safety. On the other hand, those MORT elements not present or visible in aerospace safety almost certainly have applicability there, examples being: independent review, monitoring, and information systems.

During the past year, chemical and petroleum plants, pipelines, off-shore drilling, steel producing and general manufacturing are a few fields in which MORT concepts have been thought to be usable.

The findings and recommendations are based primarily upon studies of high energy research and development work, often approaching technological boundary conditions.

This study should be fully applicable to production work, since the amount and type of analysis is more easily justified for longer term production cycles than for more rapidly changing R & D cycles. Further, the number and size of controls necessary for relatively stable production are less than for R & D, and thus more easily justifiable.

Construction work, motor vehicle accidents and smaller plants are not now covered in MORT.

Over the years NSC's Construction Section has tried a variety of experi-

mental approaches -- one was directly tied to better planning (over and above the usual management, supervision, training, etc.). While these approaches are used by the better companies, and are rational and presumably beneficial for both costs and safety, they simply have not caught on in the industry. Therefore, until a pilot project demonstrates that MORT approaches can be used, it would probably be wise to rely heavily on codes, standards, and regulations forcefully and intensively applied, as in U. S. Corps of Engineers' experience which was extended into the Manhattan Project and carried on by AEC.

Motor vehicle accidents, the source of 18% of occupational fatalities, are well handled by the present best fleet safety practices (for example, NSC's Motor Fleet Safety Manual), which is much the present practice of AEC. However, the MORT methodology -- crash resistance, and shock absorption, selection, training, error reduction and control -- also reflects major aspects of the broad, national traffic safety program. Every fleet can profitably review its practices, e.g., in vehicle selection, to assure that the best practice is followed. Transportation of hazardous materials is, however, an activity clearly within the scope and methodology of MORT.

Smaller plants are unlikely to be able to afford the effort of acquiring and using a complex technology. On the other hand, smallness gives no immunity from hazards! A Danish executive described one small chemical plant as a "one accident" plant -- one accident and there is no plant! A chemical plant employing only seven people to operate an exothermic process became a \$750,000 loss, and this is not small! From a practical view a small plant would have to enlist outside expertise in proportion to energy and loss potentials. Meanwhile, further experience with MORT may reveal short-cuts for small plant application.

Research Work.

It seems clear that system concepts can be applied to large, high energy facilities. Proportionate application to smaller, lower energy facilities should present no insuperable problems.

If the kinds of work and degree of hazard are grossly categorized, the following broad characterizations of present research safety program strength and control seem defensible:

	Degree of Hazard		
	<u>Catastrophic</u>	<u>Critical</u>	<u>Marginal</u>
Fixed, Major Facilities	Good Control	Good Control	Weak Control
Other Research	Questionable	Weak	Weak
Support Functions	Good	Good	Fair

For the fixed, major research facilities, it is relatively easy to see a model safety plan:

1. Safeguard the facility itself.
- 2a. Put pressure on the experimenter to conform to safe practices.
- 2b. Help the experimenters with safe variances when experimental needs approach boundary conditions.
3. Have a system safety procedure (ala the Bevatron at Lawrence, see page).

For less permanent experimental set-ups, it is less easy to conceive a plan, but the essentials seem to rest on an initial basic review plan:

1. Basic experimenter's safety review. (A "positive tree" was developed at Sandia, see page .)
- 2a. Safety staff assist experimenters.
- 2b. Safety staff monitor potentials, changes, errors.
3. Documentation of review, of monitoring, of changes, etc., an auditable record, both for safety and for research effectiveness and validity.

There remain, however, many unusual facets. For example, at a university, a primary complication is the division of supervisory authority between faculty advisors (especially for graduate assistants) and the managers of more or less permanent research equipment. The faculty is generally weak in safety supervision; the latter force tends to be stronger, but highly variable.

There are special problems arising from:

- Research and development work
- Involving high energies
- At or near boundary conditions
- With frequent changes
- And narrow error tolerance limits.

It has been argued that accidents are an acceptable by-product of research in areas of advanced technology. The reverse seems true, witness the aerospace program. Safety is a necessary condition for work near boundary conditions. The planning and foresight needed for safety also give greater assurance of successful completion of valid research.

Much more needs to be done in research organizations to put safety in a context of long-term results, and the steps taken to assure experiment or test validity, with preservation of the research facility as an added bonus! During the study several accidents were reviewed wherein the changes and errors which caused the accidents also rendered the research data invalid!

Where Are We?

Assessment of MORT will, of course, require a lengthier period and independent evaluation. An objective, scientific, or modest attitude would suggest that appraisal wait. However, many of those who have used the system as it was being developed have urged that the positive case be stated now in order to begin the task of persuading others, particularly management, to take the time to understand MORT and initiate experimental trials.

The goals and criteria which guided the study provide a concise listing of some presumed advantages. In addition, experience and comment to date suggest other at least tentative evaluations.

MORT and associated systems seem to provide, at the least, a place to stand -- a foundation for planning further progress.

MORT Advantages and Disadvantages

Goal-oriented -- emphasizes safety's role in building high performance, and congruity with good management methods.

Comprehensive -- endeavors to cover all aspects of safety in all kinds of work -- a global scope!

But, this curtails depth of treatment of any facet, and also taxes experience and understanding.

Systematic -- integrates, organizes, and structures safety into functionally defined relationships and measurements.

But, creates a formidable amount of complex detail!

Flexible -- assimilates new ideas and concepts, which implies further development and change, and requires a user to define his premises and methods,

But, "cookbook" solutions are easier!

Innovative -- endeavors to use new technology and concepts and foster experiment, and to outline ways to gain acceptance of innovations,

But, there are pains in innovation, and dangers of disappointment.

Humanistic -- attempts to cope with the rich and exasperating human qualities of the people who operate the system, exposes their problems, and guides the services they need for effective, satisfying work,

But, this is the area about which we know the least, theories often conflict, and super-rationality may seem "unhuman."

Practical -- pieces of the system can be introduced for separate test.

-- effort can be equated to problem (but do not skip steps).

-- projects can be adapted to constraints and conditions.

-- man-power used in trials was not great.

-- concepts, standards of judgment, information search and analysis are cheap compared to hardware and accidents.

-- a few good data are cheaper than sterile masses of information.

-- MORT analyses are fast (with a little practice) and are always

faster than blind searches.
-- MORT solutions are cheaper than endless brush-fire fixes.

Effective -- the proofs or testimony for components are drawn from a wide range of present practices,

But, the degree of proof is less than adequate, often subjective, and qualitative, rather than objective and quantified. And, much of the logic of the connecting system framework has had only initial, exploratory trial.

However, every application has improved investigation and analysis. Nothing got worse!

Unpleasant!

Emphasis on management responsibility tests understanding, patience, determination, and maturity. The "jackass fallacy" -- blaming people -- is easier and more comfortable, even if less productive.

But, management leadership, vigor and competence are the real determinants of safety.

Risk analysis (and ultimate acceptance of evaluated risks) can be impolitic, as well as harrowing.

But, there is no riskless place. Risk analysis most often leads to risk reduction and the really dangerous situations are those unanalyzed!

When suggesting that advantages be emphasized, a scientist-manager who participated in the study said:

"An inexperienced person can become proficient in analysis simply by conscientiously following a set pattern of instructions. I believe that this is perhaps the most valuable feature of the whole MORT concept and should be emphasized. Opportunities to upgrade the capabilities of personnel in an entire component of a company without extensive training or personnel replacement are all but nonexistent. Yet properly used, this is exactly what MORT can do."

Unfinished Business

Further simplification and integration are needed. For example, the MORT Hazard Analysis Process (Chapter 23), the Framework for Analysis of Risk (Figure 21-3), and Aerojet's Configuration Control Tree (Exhibit 3) are similar in purpose and overlap in degree. However, the three methods are mutually complementary, and further trial is needed to develop a synthesis.

Proof and quantification are sorely needed and should be feasible, partly because so many variables have now been defined.

Broader scope of application and more expeditious transition to new methods can probably come only from expanded training and trials.

Most important, each accident, each failure, must be used as a basis for improving the system.



GETTING STARTED

Ingredients:

One accident, problem or program
One set of MORT diagrams
Red, green and blue pencils.

1. Color the bubbles (circles are basic problems).
Red -- appears deficient.
Green -- appears o.k.
Blue -- don't know.
2. For each blue bubble,
list the questions needing answers.
3. Consult the cookbook if definitions or criteria are needed.
4. Two-person dialogue greases the process.
5. Cooking time -- one hour; for tough problems, until done.
6. Serves everyone.

This page intentionally blank

II. WHAT PRODUCES HAZARDS

This Part includes discussion of certain accident concepts which combine to produce a new definition of an accident, more functional for preventive purposes.

II

The accident definition which evolves is:

1. An unwanted transfer of energy,
2. Because of lack of barriers and/or controls,
3. Producing injury to persons, property or process,
4. Preceded by sequences of planning and operational errors, which:
 - a. Failed to adjust to changes in physical or human factors,
 - b. And produced unsafe conditions and/or unsafe acts,
5. Arising out of the risk in an activity,
6. And interrupting or degrading the activity.

This page intentionally blank

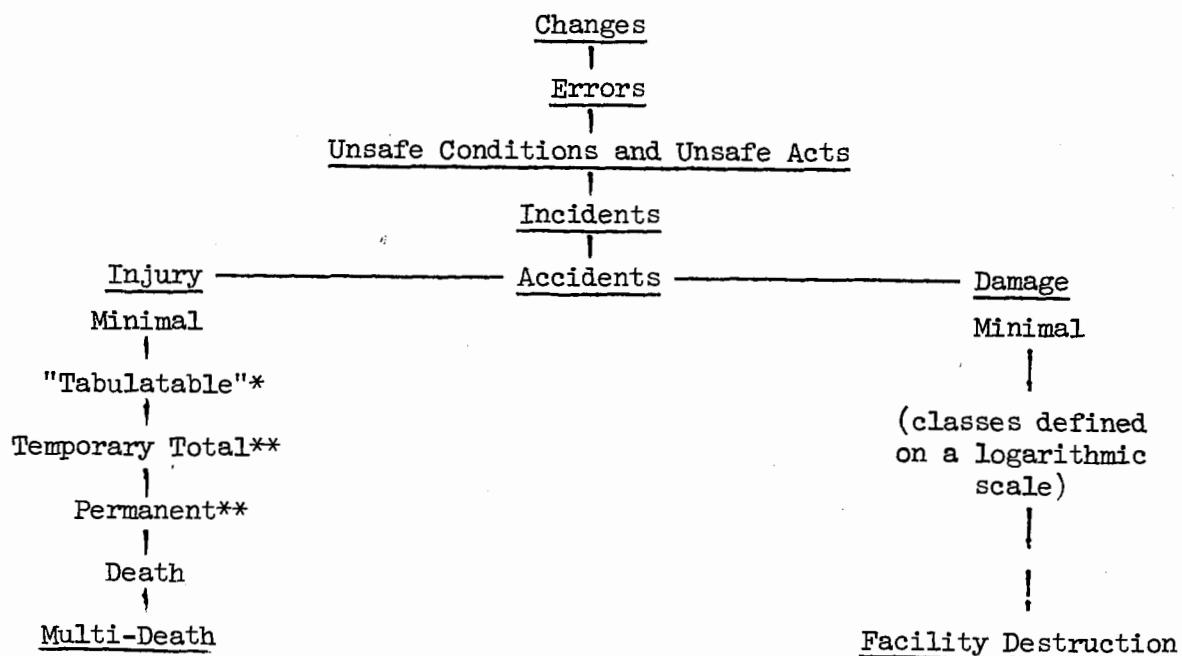
1. ACCIDENT/INCIDENT.

An incident, as we shall define the term, is similar to an accident but without injury or damage (element number 3 in the definition on page 25).

This Accident/Incident distinction is adopted from aerospace system safety practice. It seems to conform to common usage. (The phrase "Accident/Incident," however, is somewhat awkward, so the word accident is generally used in this text and construed as including both kinds of events where pertinent.)

It has been suggested that the term accident be defined to include a "not necessarily injurious or damaging event." (Tarrants, 1965.) The motivation behind the notion is sound -- such events are within the scope and concern of preventive effort. The "near miss" may have great import for safety. Tarrants did not use the concept of "unwanted transfer of energy," and thereby picked up some non-accident events. For example, an unwanted release of energy may occur in a non-injurious manner because of safe design. It would interrupt the activity as was anticipated, but hardly seems an accident; rather, the opposite! The event is an "incident."

Events of interest may be arranged in order of increasing concern, which is also the order of decreasing frequency:



* Definable in a variety of ways.

** May be broken into subclasses by severity.

The basic point that an accident is the unit event, and may produce multiple injuries and/or damage, would probably not need emphasis were it not that so

much occupational data uses the "injury" as the unit event. Classification of the seriousness of errors and accidents may thereby be distorted, and the magnitude of review and hazard reduction required for changes may be unnecessarily obscured. For example, in a frequency-severity matrix, the severity scale should reflect potentials for multi-injury and multi-death accidents, and all untoward impacts should be included in a single result.

If we are satisfied of the expedient need to tabulate injuries rather than accidents, the OSHA or ANSI injury definitions may be simple and usable to derive a control fact, but non-functional for damage accidents and for prevention purposes.

Functional aspects of our definition of an accident can be suggested:

1. Energy present in a task is associated with performance of the task (that is, usually cannot be prohibited), but must be controlled.
2. Excessive energy build-up is a change, or change releases the energy in an unwanted manner.
3. If an activity has been proceeding free of accidents, change in the system is "cause," or an antecedent of the problem.
4. If an activity is new, the activity itself is change.
5. Planning is, by inference, defined as anticipation of change, error, and potential energy release, and adverse consequences of such.
6. Risk is inherent in any activity.

In practice the usefulness of this definition will depend in part on the degree to which people can be constructively sensitized to energy control, to changes and appropriate counterchanges, and to risk analysis.

Hazard.

The stated definition of an accident suggests a definition of hazard as: the potential in an activity (or condition or circumstances) for an accident, particularly:

1. An unwanted transfer of energy,
2. Which can occur in random variations of normal operations or from changes in physical or human factors.

Among the hazards to be identified and controlled are those which result from interaction of two or more energy potentials.

Risk.

The stated definitions of accident and hazard, in turn, suggest a definition of risk:

1. The probability during a period of activity,

2. That a hazard,
3. Will result in accident,
4. With definable consequences.

The elements of definable probability and consequences are particularly significant. This definable characteristic leads to classification of risks as:

1. Assumed, calculated, analyzed -- before the accident. These are usually few in number.
2. Uncertainties, errors, oversights, omissions -- and sometimes hunches or guesses, not well known until after an accident. These are usually larger in number.

This page intentionally blank

2. ENERGY AND BARRIERS

Energy is the capacity to do work and is therefore an essential to performance. Energy use per capita has risen on an exponential curve.

The energy forms which produce injury and damage are:

Kinetic, chemical, thermal, electrical,
ionizing and non-ionizing radiation,
acoustic, biologic,

and by interfering with normal energy exchange:

exclusion of oxygen and exposure to elements.

A useful set of concepts of energy and barriers was developed by Gibson (1961) and Haddon (1966 and earlier). They made the point that an accident is an abnormal or unexpected release of energy. The concepts were utilized and improved by the U. S. Commission on Product Safety (1968-69).

The energy concept seems to have several values:

1. Simplicity and objectivity,
2. Suggests common approaches to a form of energy,
3. Suggests that hazard modes for a kind of energy may be more explicit than the terms now used in most accident statistics analyses,
4. Suggests that scaling of hazards (and preventive programs) may be more explicit for a given form of energy,
5. Provides a point of similarity to system analysis of energy transfers,
6. Sensitizes us to energy build-up, and to release mechanisms,
7. Reminds us to consider a product or situation for all kinds of energy,
8. Alerts us to sequences of interaction of various forms of energy.

The human body (or any given object) has tolerance levels or injury thresholds for each form of energy. Energies, particularly near or above thresholds, must be quantified to determine the magnitude of control required. A summary of the literature on energies and injury thresholds was prepared for the U. S. National Commission on Product Safety (Weiner, 1969). Factors common in injury production, in addition to magnitude, were duration or frequency of exposure, and concentration of forces. The magnitudes of tolerable forces, often expressed as exposure matrices, suggest greater emphasis on generic standards for energy transfer, rather than standards for specific situations, which can be inhibiting or narrow specifications.

McFarland (1967) said:

"... all accidental injuries (and damage) result, (1) from the application of specific forms of energy in amounts exceeding the resistance

of the tissues (or structures) upon which they impinge, or (2) when there is interference in the normal exchange of energy between the organism and the environment (e.g., as in suffocation by drowning).

Thus, the various forms of energy ... constitute the direct causes of injuries in accidents. Also, prevention of injuries can often be achieved by controlling the source of the energy, or the vehicles or carriers through which the energy reaches the body.

"While the specific types of energy which give rise to injuries are quite limited in number, the forms in which they abound and the variety of the vehicles or carriers of energy are innumerable. Man himself is constantly compounding this situation as he develops more powerful sources of energy and puts the various kinds of energy to new uses."

The nuclear energy projects utilize energies in great variety and magnitude. This suggests that energy-based accident concepts may have particular value for AEC.

A weakness in the "energy" concept is that most accidents fall in the kinetic category. This necessitates use of injury mode subclasses, such as: fall (1 or 2-level), nip, shear, cutting, and bodily motion. The concept seems, at this time, least useful in the substantial categories of strains, sprains, and falls on one level. Nevertheless, advantages cited seem increasingly clear. Useful studies in kinetic, chemical, electrical, radiation and biologic energies have been done.

Even for the broad grouping of accidents under kinetic energy, the meticulous tracing of energy flow has proven in this study to be a useful analytic method to make visible the number of practical potentials for interrupting energy flow, either in hazard analysis or in accident investigation. Process audit can also be guided by the meticulous energy trace and careful examination of potential energy interactions.

We continuously use energy magnitudes in everyday decisions, for example: allowing greater clearance for heavy, swiftly moving objects; admitting a cigarette lighter but frowning on a can of gasoline; handling flashlights, but using 110 volts only with controls, and avoiding "high" voltages; tolerating illegal "lady finger" firecrackers but avoiding a case of dynamite.

Three practical requirements force us to consider the feasibility of developing energy magnitude criteria and energy-exposure matrices to better express what we will tolerate or accept:

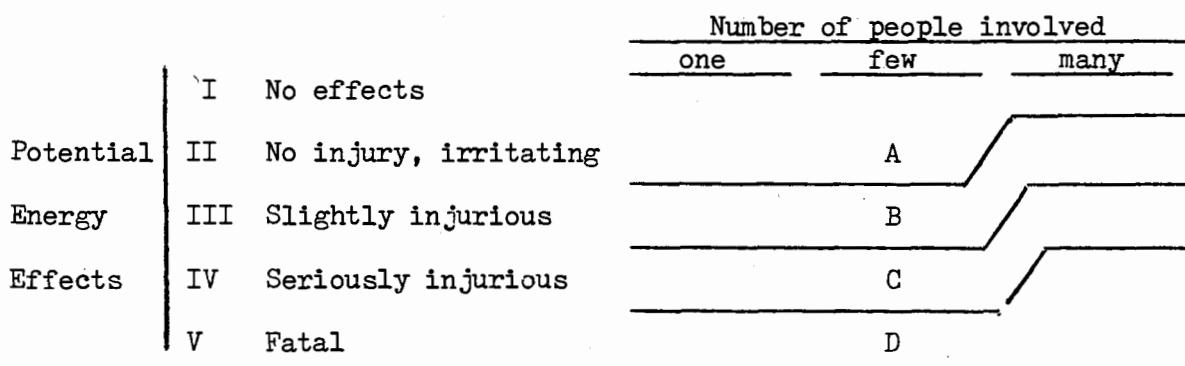
1. At least order-of-magnitude energy data are needed in systems analysis.
2. The cost of controlling energy sources will force us to choose between

controlling relatively large numbers of small energies or relatively small numbers of large energies.

3. Delegation of decisions regarding potential, harmful energy releases is a practical necessity, and decisions or feedback cannot be systematic without standards of judgment.

Thus, whether we are explicit or not, we are using a decision standard constructed somewhat as follows:

Figure 2-1. Risk Decision Standard.



We do appear to delegate decisions in area A to the operator level, in B to first level supervision, C to middle or senior management, and D reserve for top management. Shall we delegate more specifically, e.g., by specifying each level of each energy and each source? Or shall we attempt to define (whether in general or by specification) the permissible limits of delegated authority? The scaling mechanisms suggested for the Hazard Analysis Process and the development of improved energy scaling mechanisms are more fully discussed in Chapter 24.

Barriers.

Haddon apparently originated the concept that harmful effects of energy transfer are commonly handled by one or more of a succession of measures. As expanded in this study, the "barriers" are:

1. Limit the energy (or substitute a safer form),
2. Prevent the build up,
3. Prevent the release,
4. Provide for slow release,
5. Channel the release away - that is, separate in time or space,
6. Put a barrier on the energy source,
7. Put a barrier between the energy source and men or objects,
8. Put a barrier on the man or object - block or attenuate the energy,
9. Raise the injury or damage threshold,
10. Treat or repair,
11. Rehabilitate.

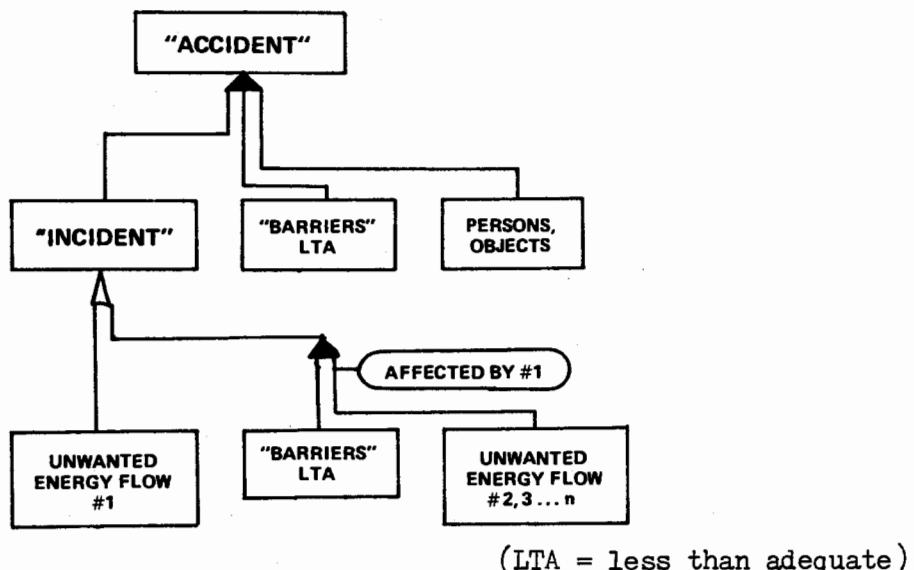
These concepts hold a variety of important implications for data collection and analysis, and for hazard reduction.

For ease of reference, the successive steps (1 to 9) have been called "energy barriers," but this connotes physical interventions. A procedure may be the means of separating in time or space, for example, with a procedure of firing explosives at the end of a shift (but these have been called "paper barriers"). Substituting a less harmful energy may be a way to "limit the energy" or "prevent the build-up," and we see many of these barriers in safety practice.

Haddon suggests that the earlier in the barrier sequence the preventive steps can interrupt the energy transfer, the better. He further suggests that the greater the potential damage, the earlier should be the interruption and multi-interruptions (redundancy) should be provided.

The portion of MORT analysis dealing with final results of energies and barriers is shown below.

Figure 2-2. Energy and Barrier Tree



One value in the barrier concept seems to be the way it provokes the imagination to see the varied possibilities for safety. For example, grinding wheel safety practices reflect several of these sequential steps: prevent excessive build-up, prevent release, put barriers on the machine, and put a barrier on the man.

A worksheet used in a training program is shown in Figure 2-3. The successive protective features for grinders are shown, plus a variety of other examples. The open space was used to get other illustrations from the class.

Figure 2-3. Examples of Barriers

Type	Grinders	Others
1. Limit energy	Speed size	Low voltage instruments Use safer solvents Limit quantities
2. Prevent build-up		Limit controls, fuses Use sharp tools Gas detectors Floor loading
3. Prevent release	Store Test Mount Tool Rest	Containment Insulation Toe boards Life line
4. Provide slow release		Rupture disc Safety valve Seat belts Shock absorption
5. Channel away (Separate)	Exhaust	Rope off area Aisle marking Electrical grounding Lock-outs, Inter-locks
6. On source	Guard	Sprinklers Filters Acoustic treatment
7. Between	Glass Shield	Rail on aisle Fire doors Welding shields
8. On Man or object	Goggles	Shoes, Hard hats Gloves, Respirators Heavy Protectors
9. Raise Threshold		Selection, calluses Acclimatize to heat or cold Damage resistant material
10. Ameliorate		Emergency showers Transfer to low radiation job Rescue Emergency medical care
11. Rehabili-tate		

Then the order of listing can be used to test the relative earliness in the sequence against effectiveness. The systematic use of successive barriers is clearly apparent from examination of fire prevention protection features.

A walk through the exhibit at the National Safety Congress will give colorful evidence of the variety and investment in barriers to harmful energy.

If Haddon's barrier concept were just a way of categorizing the many, many protective features in present safety practice, the scheme might be only an intellectual exercise. However, in this study, the meticulous application of the barrier hierarchy to specific energy transfer points has proven useful in stimulating ideas for use of tested methods and new, innovative methods of interrupting transfer. For example, in the high-explosive press accident (Appendix A-3), the barrier discipline applied to a meticulous energy trace raised the question as to why the press was given a fluid reservoir large enough to push the ram to an unwanted position. In other accidents the use of the method produced a "brainstorm" of ideas from young engineers, and some proved practical.

All too frequently two energies interact -- for example, a lift truck ruptures chemical apparatus. Such situations provide opportunity to consider two series of energy barriers, one set between the two energy sources, and one set between the energy and the people.

The energy concept suggests that safety is pre-planned energy management for high performance.

* * *

The energy source groups currently in use at Aerojet to develop the next generation of priority problem lists are:

- | | |
|-----------------------------------|-----------------------------------|
| 1. <u>Potential</u> | 3.3 Toxic |
| 1.1 Electrical | 3.4 Flammable |
| 1.2 Nuclear | |
| 1.3 Gravitational (mgh) | 4. <u>Thermal</u> |
| 1.4 Pressure vessel (pv) | |
| 1.5 Coiled Spring (kd) | 5. <u>Radiant</u> |
| 2. <u>Kinetic</u> | 5.1 Electromagnetic & Particulate |
| 2.1 Linear | 1-1 Radioactive |
| 2.2 Rotational | 1-2 X-Ray |
| 3. <u>Chemical and Biological</u> | 1-3 Light (laser) |
| 3.1 Corrosive | 1-4 Ultraviolet |
| 3.2 Explosive | 5.2 Acoustical |
| | 5.3 Thermal (radian) |

This grouping has seemed to be useful in three ways: (1) stimulating incident or situation reports, (2) scaling by magnitude, and (3) development of barrier and target information which in turn leads to probability and consequence scaling.

3. FREQUENCY-SEVERITY MATRICES AS A MANAGEMENT TOOL

This chapter sub-title could be: "What Produces What Amount of Hazard?" Harmful effects of most energy forms operate through distance-intensity matrices. These, in turn, are the genesis of frequency-severity matrices for harmful effects. The frequency-severity matrices, in turn, have implications for direction and allocation of resources for reductions in hazard, and perhaps most important, provide the basis for projecting the inexorable quality of disaster potentials, and thereby generate fuller understanding of the precept:

WHAT CAN HAPPEN, WILL HAPPEN, the only uncertainty is When!

Energy matrices, coupled with distribution of energy sources and people in space, produce matrices of injury frequency and severity by energy source or subtype, which are likely to be useful in at least two ways:

1. Consideration of the unique injury production matrices of different energy sources, and therefore, their unique negative effect on overall safety,
2. Longer term predictions of a spectrum of consequences, including serious outcomes, even though present experience may be short, variable and unreliable.

A matrix of major categories of work injuries can be approximated from National Safety Council and U. S. Public Health Service data on annual U.S. totals as shown in Figure 3-1. The estimate of medical and temporary partial injuries may not be accurate. The slope of the last two segments of the line approximates 45° which is the "line of balance" on a log-log chart. That is, the more severe injuries are decreasing in frequency at about the same rate as they increase in seriousness. Thus the projected aggregate impact of the last three groups is roughly equal, if days charged are a correct measure.

Figure 3-2 shows the similarities of broad industrial groups. There are differences, too -- note that the chemical industry record is more like construction than all industry in slope toward deaths. Other data (not pictured) show great similarity of AEC 10-year research data and similar data from NSC chemical labs, for example, permanent partials were 7.2% and 6.7% of disabling injuries, respectively. Other examples are included in Chapter 41.

Use of matrices to assess the spectrum of short and long term injury and

Figure 3-1. Major Categories of Work Injuries

- 38 -

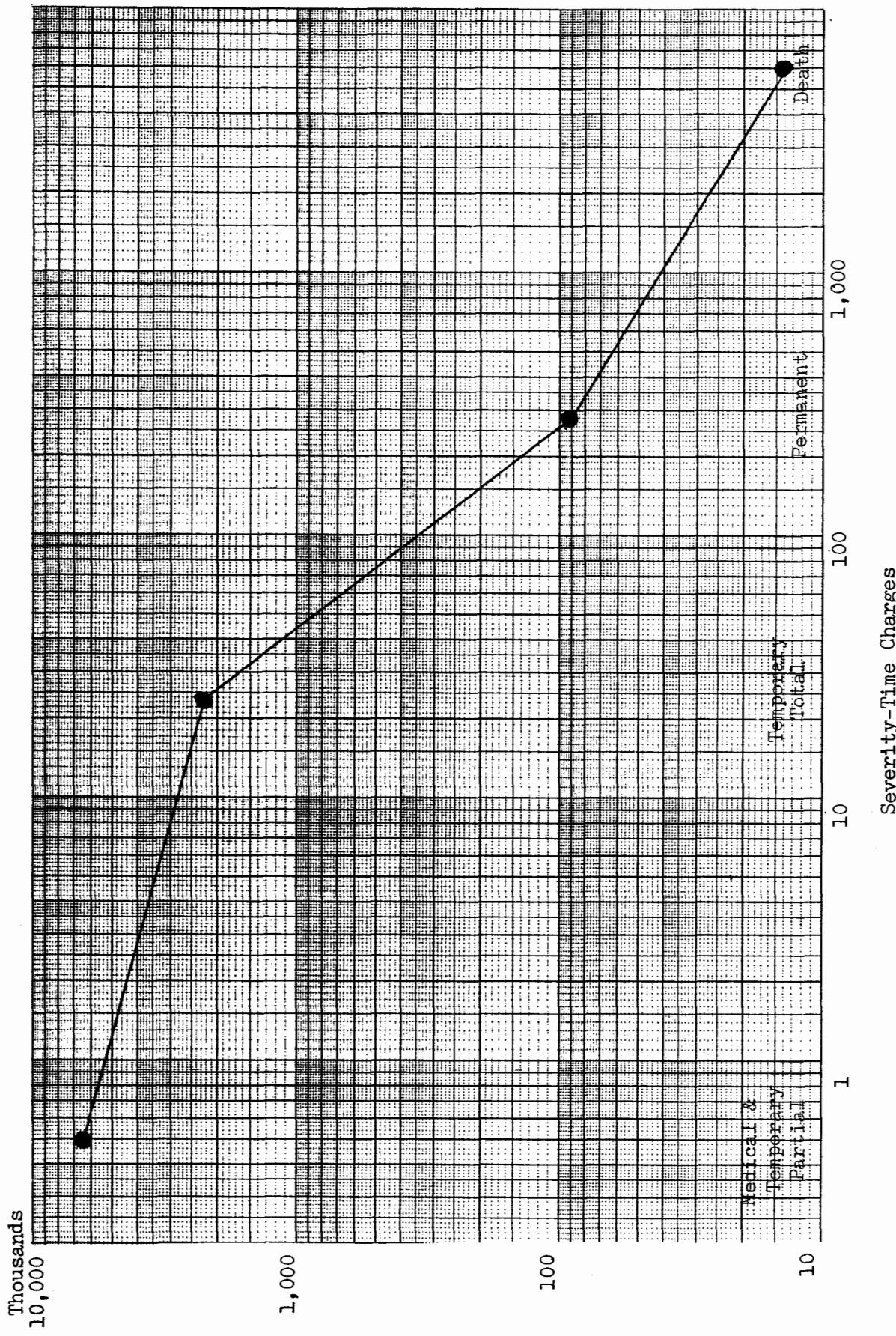
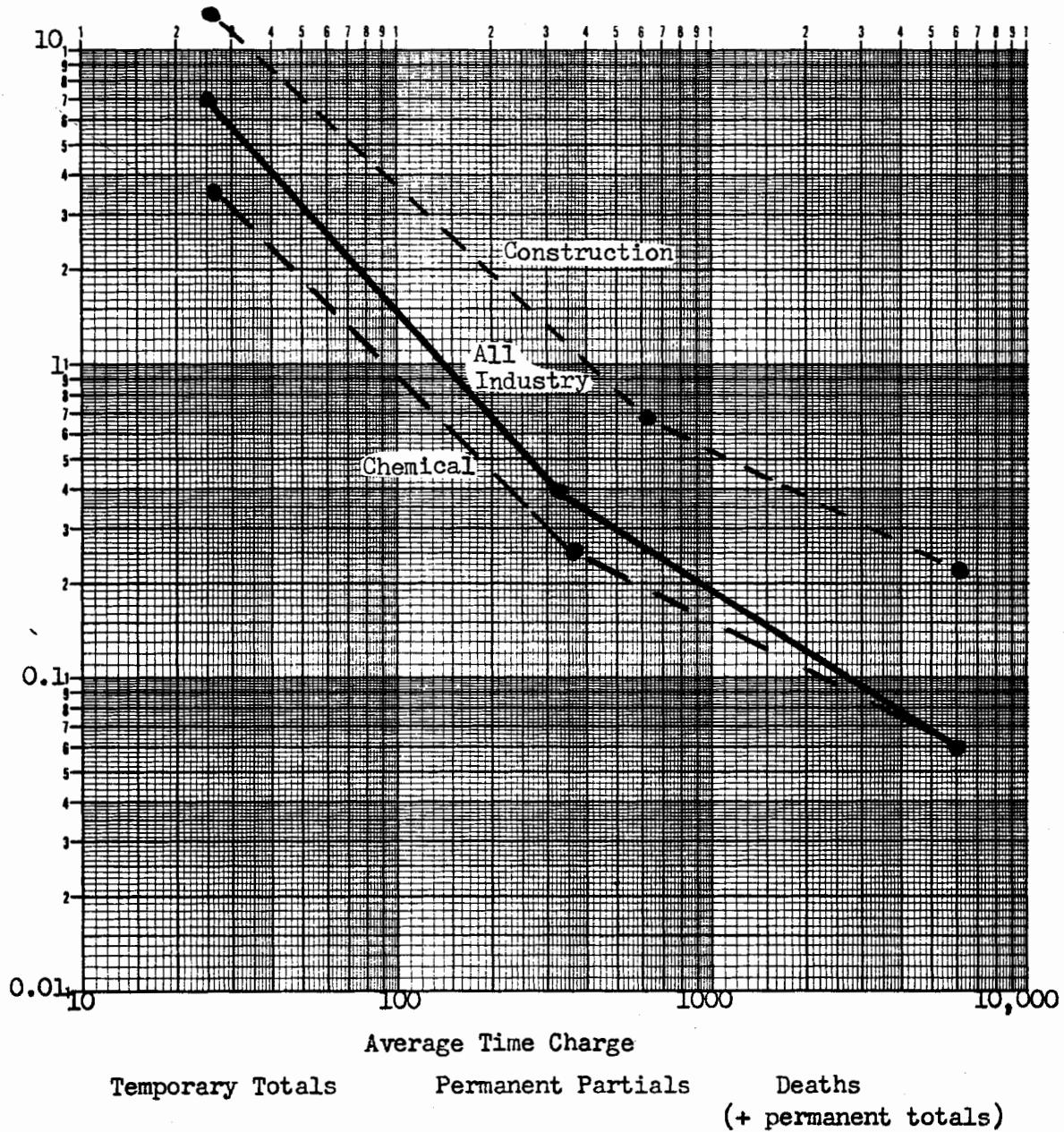


Figure 3-2

Frequency-Severity Matrix-Type Chart for
All Industries, Chemical and Construction Industries
Standard Classes of Disabling Injuries

1968

Frequency Rate*



* per million man-hours

damage potentials has advantages which seem to include:

1. A format is provided to explore the degree to which less severe categories are predictive of more severe categories, particularly for a type of energy or type of industry.
2. A continuum is established to which even more frequent error and change data, which also may be predictive, can be added.
3. The "sharp pencil" practices to lower injury classification of certain cases, which now plague standard occupational rates, have much less effect on inferences.
4. A format is provided whereby:
 - a. more severe temporaries and other events can be made visible,
 - b. multiple results of one accident (injuries and damage) can be reflected,
 - c. The ultimate long-term possibility (high or low) of disasters can be made visible if trend lines are extended to more serious results,
 - d. damage accidents and fires can be similarly plotted using an economic denominator to equate damage to injury, or vice versa.
5. Investment/benefit implications of emphasizing minor vs. major injuries are more clearly implied.

The matrices have been explored in some detail and at all three sites during this study. For a time it was felt they might be a primary management tool. However, at present their values seem to lie within the risk assessment problem discussed in Chapter 41, that is, one of several tools.

The matrix uses order-of-magnitude values of frequency and severity plotted on log-log paper. The slope or shape of the lines gives an important picture, not the relative heights of the lines. The matrices can be used for three purposes:

1. Visually projecting rare event possibilities, when organizational exposure is limited.
2. A line sloping at less than 45° is a very dangerous line - it may signal a disaster.
3. Management emphasis in terms of the Pareto Principle, the "vital few" or the "trivial many" can be assessed visually or mathematically.

Thus far, no substantial literature on the matrix approach has been located; the quickest way to find it may be to say it is sparse! A paper of F. R. Farmer, United Kingdom Atomic Energy Authority (1967), used such matrices in analyzing deployment of preventive effort. Occasionally a

log-log plot appears in a technical safety paper, but the method has not been given emphasis. (Surry, 1969, provides an example.)

The frequency-severity matrix when plotted on log-log paper commonly tends toward a more or less straight line. Farmer raised the question in nuclear radiation fields of whether preventive effort should be deployed:

1. Along the whole line,
2. On the high-frequency, low-severity portion,
3. Or, on the low-frequency, high-severity portion?

In this study, fire data plotted by severity was predictive of a disaster because the line was sloping at less than 45° , which is a "dangerous curve!"

For this and other reasons (e.g., managerial and public impact) the author tends to favor the third of Farmer's alternatives.

Pareto's law and the high cost of the "vital few" also favor the approach. Pearson (1969) and Peterson (1971), both with Employers' Insurance of Wausau, have urged such attention, as has their company. As a current example, the Bureau of Mines has announced a special drive on coal mine haulage deaths, now the leading cause.

The tricky job of safety management is to balance:

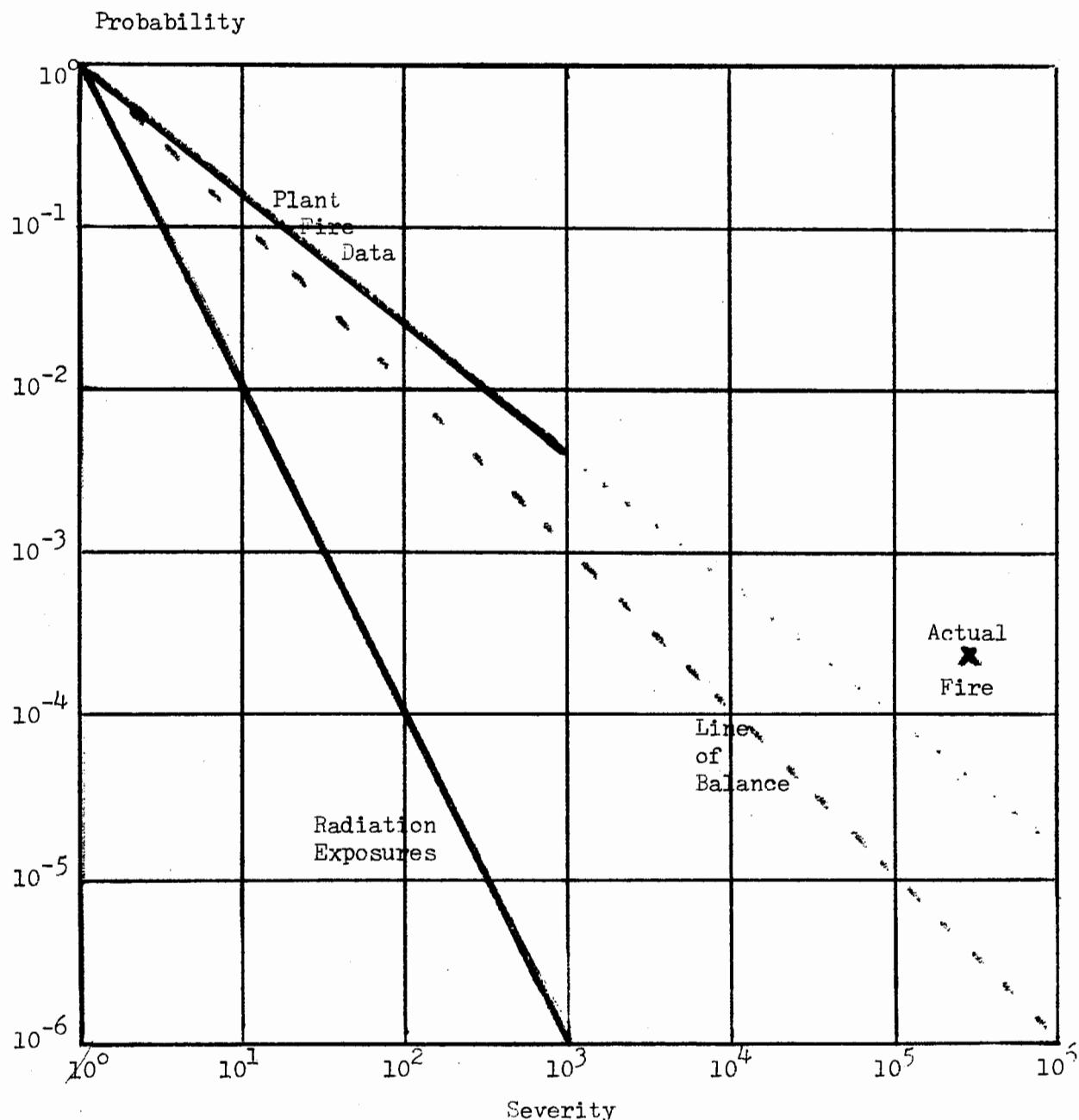
1. Review of every accident/incident (and use incident recall to gain more reports) for individual preventive value,
2. Give special attention to the "vital few."

Fire Matrices. During this study a special report was provided to AEC indicating that a "20-20 hindsight" analysis of events leading up to a major fire suggested that risk of major loss might have been detected by a routine form of analysis, namely, reporting of fires by the order-of-magnitude limits listed above. The matrix had an almost uncanny straight line pointing at the major fire. (Figure 3-3.)

Later in the study, at one site, very sparse data (few fires) suggested a similar signal. (Repeatedly, this study has been handicapped by the fact that AEC sites do not have enough accidents to make reliable projections -- a good problem!) When the sparse data were examined at this site, it was discovered that the few fires were a non-homogenous collection of events ranging from fires as ordinarily understood, to electrical failures, to a remote common-carrier fire involving equipment. However, it didn't take long to check out the false alert.

There is enough data to warrant a strong recommendation that AEC or any other large organization institute trial of an order-of-magnitude fire reporting

Figure 3-3
Divergent Slopes of Radiation and Fire Data



Note: Absolute values for radiation and fires are on different scales.

system, computerize the information, and ask the machine to give signals when the data warrant. AEC as a whole may be homogenous within the definitions applicable to predictive techniques. Individual sites could profitably watch fire matrices, but if a proper system of reporting is instituted, a headquarters computer could watch and assess the data equally well or better, and could send out signals to take a harder look at selected risks. (A related fire-predictive technique is cited in Chapter 41 as "Extreme Value Technology." The indications are that any large pool of fire information can profitably be organized to send out warnings.)

The matrix can also be executed as a table to extend probability and consequences to estimates which can then be aggregated; this can be done for days lost or dollar values, and for a year or ten years. The total or aggregate then represents the exposure.

<u>Events</u>	<u>Probability</u>	<u>Average Consequences</u>	<u>Extension</u>
by	_____	_____	_____
size	_____	_____	_____
groups	_____	_____	_____
Total			

When this has been done for fire data, the dollar value of disasters with low probability may emerge as a significant figure. The spectrum of consequences is useful in risk analysis.

Comparisons of Injury or Damage Sources. AEC's radiation exposure data show sharp decreases in exposure frequencies as exposures approach injury thresholds, the contrary of the above cited fire prediction. Thus, the data indicate the existing radiation protection system is not likely to produce larger numbers of serious injuries (except if the system is changed in an untoward manner).

The relative slopes of the fire and radiation lines are shown in Figure 3-3. No scales are shown on the log-log chart because the absolute data are non-comparable.

The historic safety precept, "prevent the minor injuries and you prevent the majors," seems, in some part, true for a type of accident in a given situation. However, heavy emphasis on an overall "frequency rate," which is essentially a rate for temporary total disabilities, or on rates for even less serious injuries, has perhaps done occupational safety as much harm as good since it fails to direct attention to the sources of the most severe accidents.

Heinrich (1959 and earlier) had drawn attention to the high ratio of unsafe acts and conditions to injuries, and the high ratio of minor to major injuries, and correctly urged attention to the numerous events. However, the principle seems to be misapplied if all accident sources are lumped together, because attention will be focussed on sources of minor injuries rather than major events.

As early as 1940 Grieve of the NSC staff raised the question of emphasis on minor injuries in the electric utility industry pointing out that minor injuries (tending to be bumps, bruises, minor cuts and dust in eyes) did not focus on causes of electric shock fatalities.

Thus the minor to major continuum has preventive values primarily within a specific type of accident. In this study "critical incident" (near miss) reports will be shown to be predictive of more serious incidents in ways in which the typical first aid cases are not.

The matrix is an aid to management of the vital few; it helps give visibility to the nature of problems, whereas the typical injury rates obscure meanings.

The programming implications of the matrix are further displayed in Figure 3-4. While we are anticipating later developments in the text, the values for safety management are sufficiently important to warrant early display.

The consequences of accident/incidents are classified by magnitude. Investigation of all of these has value for designing cures.

The limitation on minor injuries is that they are largely predictive of minor injuries.

The value in incident reports is that they may be predictive of major events.

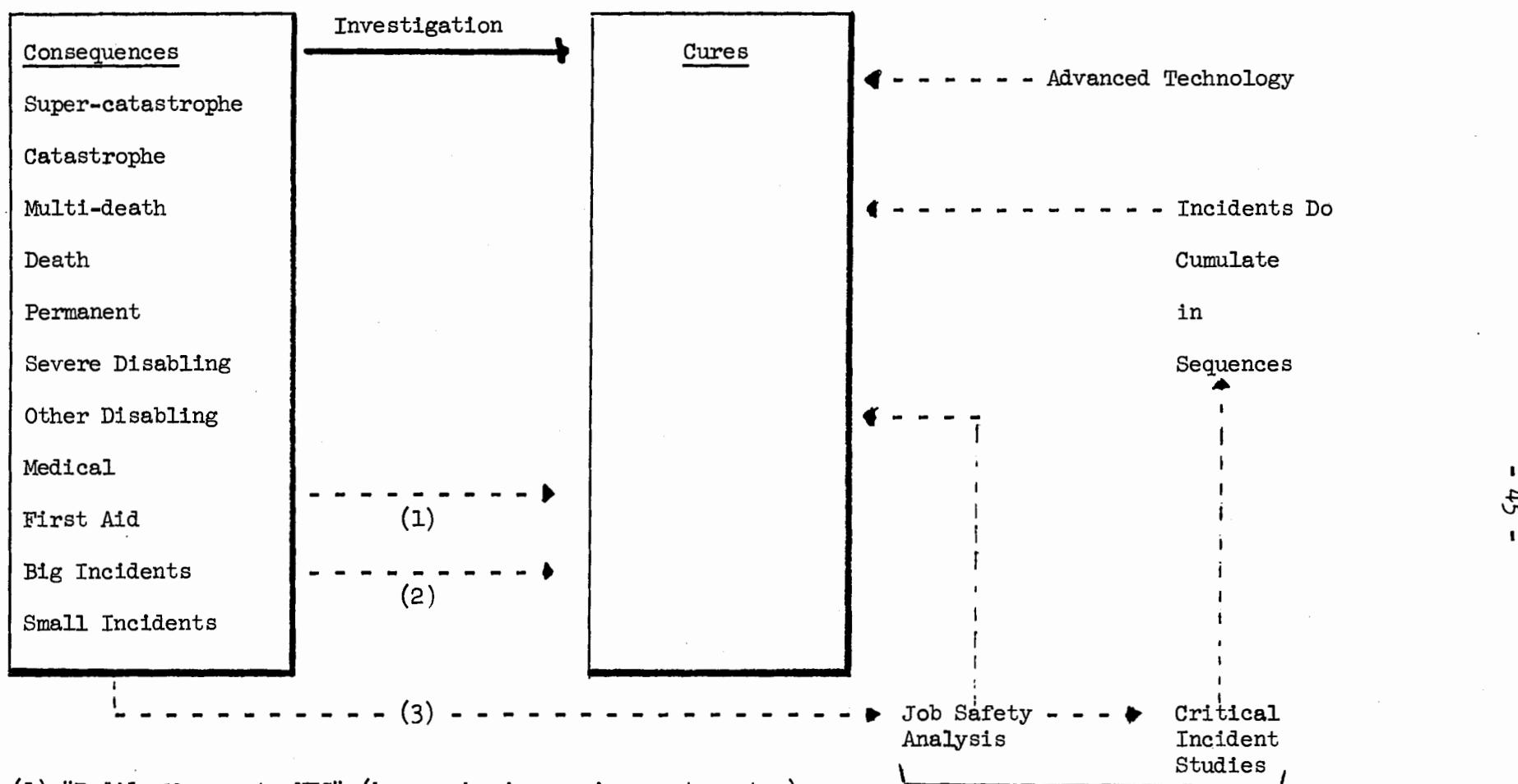
Two order-of-magnitude concepts were developed by DOD to form a matrix useful in decisions in system safety. The categories were first:

"Probable"	$< 10^4$ hours (or other units)
"Reasonably probable"	$< 10^5$ hours
"Remote"	$< 10^7$ hours
"Extremely remote"	$> 10^7$ hours

and second:

"Safe"	=	= failure results in no major damage, not functional damage, nor contributes to injury or damage.
"Marginal"	=	without major damage or injury.
"Critical"	=	injury, damage substantial.
"Catastrophic"	=	loss of the system, death, or multiple injury.

Figure 3-4. Preventive Implications of Matrix.



(1) "Bodily Movement, NEC" (bumps, bruises, minor cuts, etc.) may be largely predictive of minor injuries, but they should all be screened individually; group study if problem warrants.

(2) Big Incidents will be known to Management.

(3) Job Safety Analysis and Critical Incident studies are the two best methods of finding small events predictive of large events.

A matrix constructed with these terms, Figure 3-5, becomes a decision aid.

Figure 3-5. Risk Tolerance Matrix

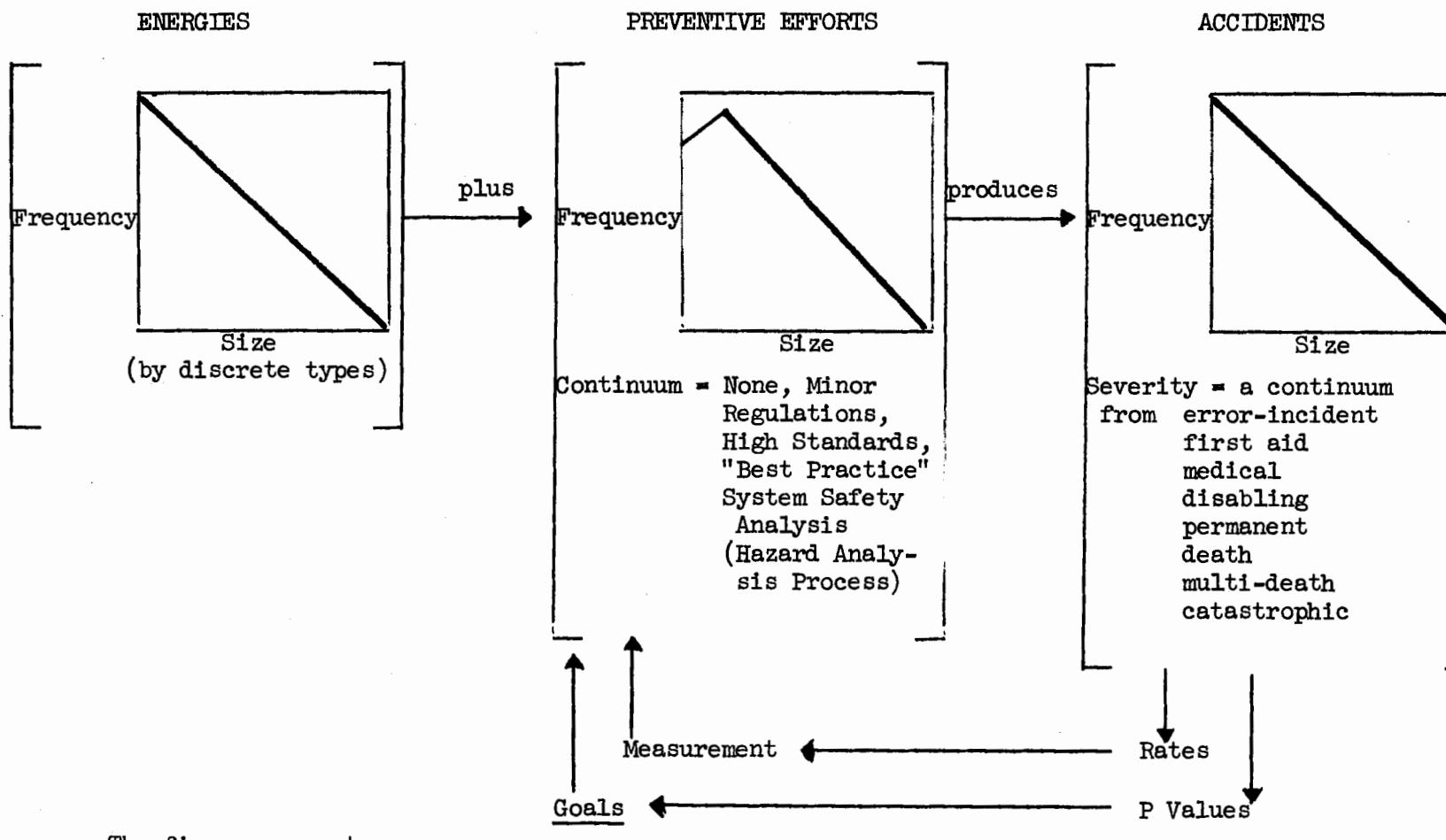
	Safe	Marginal	Critical	Catastrophic
Probable				
Remotely Probable				
Remote				
Extremely Remote				

Tolerable? Tolerance Cannot
Level? Tolerate?

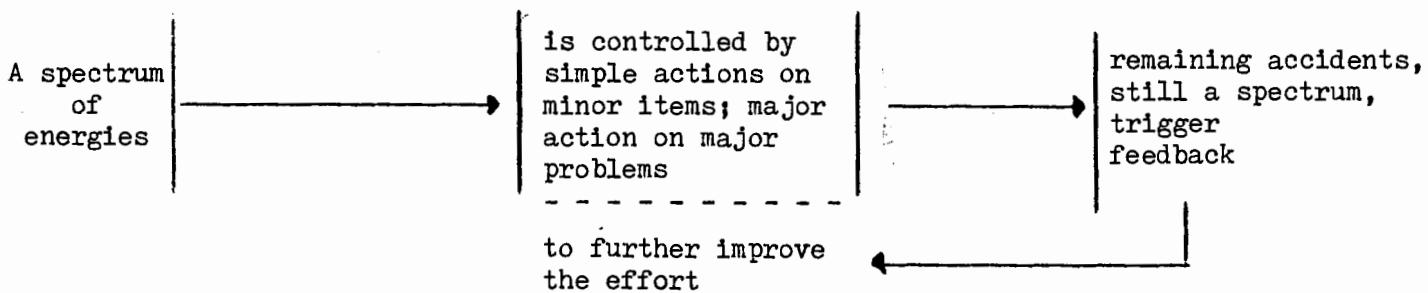
Categories of situations to be handled at a given level of management can be defined. In system safety the direction and magnitude of preventive effort can be guided.

As this study progressed, the notion of potential significance of a series of scalings of energy, preventive effort, and injury based on frequency-size matrices emerged. Such a series presents some promise of unifying rather divergent views of accident and safety problems. A present effort to portray such a series of relations is in Figure 3-6.

Figure 3-6. Energy, Prevention and Accident Matrices.



The figure suggests:



This page intentionally blank

4. ERROR AS ACCIDENT CAUSE

Accidents have been characterized as members of the broader family of human error by Altman, Chapanis, Christensen, Rigby and Swain, and we shall lean heavily on them to develop a concept of value in establishing mechanisms of accident occurrence and explaining causation. Errors are easier to study and literature on error reduction can be tapped.

Peters (1966) defined error as:

"Any significant deviation from a previously established, required, or expected standard of human performance, that results in unwanted or undesirable time delay, difficulty, problem, trouble, incident, malfunction or failure."

Rigby (1970) described error in the following terms:

"Both people and what they do are very complex. In treating complexity, it has become customary to presume that performance will vary but that variability is not important so long as it is within certain limits. When those limits are exceeded, we speak of deficiencies -- of defects, failures, accidents, and errors. Thus, in the most general and most practical sense, a human error is any member of a set of human actions that exceeds some limit of acceptability. An error is only an out-of-tolerance action, and the most important ingredients in any discussion of error are definitions for both the set of actions and the tolerance limits that define errors for those actions. (emphasis added)

"Every human action is an opportunity for error. An action may be a visible act, such as a control movement, an internal process, such as reading, or even lack of activity, such as waiting or omitting a procedural step."

Chapanis begins one paper with this case history:

"... a shocked nation read that six infants had died ... because they had been fed formulas prepared with salt instead of sugar. The error was traced to a practical nurse who had inadvertently filled a sugar container with salt from one of two identical, shiny, 20-gallon containers standing side by side under a low shelf, in dim light, in the hospital's main kitchen. A small paper tag pasted to the lid of one container bore the word 'Sugar' in plain handwriting. The tag on the other lid was torn, but one could make out the letters 'S.lt' on the fragments that remained. As one hospital board member put it, 'Maybe that girl did mistake salt for sugar, but if so, we set her up for it just as surely as if we'd set a trap.'"

This tragic case suggests many preventive steps, but the one not acceptable as "solution" is to tell nurses to "read labels more carefully." Yet the solutions we see today on many accident reports are equally superficial and inadequate. Better answers may lie in color or shape coding cans, or separation of supplies, rather than simple solutions!

Further, Chapanis says:

"When a system fails it does not fail for any one reason. It usually fails because the kinds of people who are trying to operate the system, with the amount of training they have had, are not able to cope with the way the system is designed, following procedures they are supposed to follow, in the environment in which the system has to operate."

Some other examples of Chapannis's observations are:

1. "Many situations are error provocative."
2. "Given a population of human beings with known characteristics, it is possible to design tools, appliances, and equipment that best match their capacities, limitations and weaknesses."
3. "The improvement in system performance that can be realized from the redesign of equipment is usually greater than the gains that can be realized from the selection and training of personnel."
4. "For purposes of man-machine systems design there is no essential difference between an error and an accident. The important thing is that both an error and an accident identify a troublesome situation."
5. "The advantages of analyzing error-provocative situations are:
 - a. It is easier to collect data on errors and near-misses than on accidents.
 - b. Errors occur much more frequently than do accidents. This means, in short, that more data are available.
 - c. Even more important than the first two points is that error-provocative situations provide one with clues about what one can do to prevent errors, or accidents, before they occur.
 - d. The study of errors and near-misses usually reveals all those situations that result in accidents plus many situations that could potentially result in accidents but that have not yet done so. In short, by studying error-provocative situations we can uncover dangerous or unsafe designs even before an accident has had a chance to occur. This, in fact, is one of the keys to designing safety into a system before it is built.
 - e. If we accept that the essential difference between an error and an accident is largely a matter of chance, it follows that any measure based on accidents alone, such as number of disabling injuries, injury frequency rates, injury severity rates, number of first aid cases, claim rates, and so on, is contaminated by a large proportion of pure error variability. In statistical terms the reliability of any measure is inversely related to the amount of random, or pure error, variance that contributes to it. It is likely that the reason so many studies of accident causation turn up with such marginally low relationships is the unstable, or unreliable nature of the accident measure itself."
6. "Design characteristics that increase the probability of error include a job, situation, or system which:
 - a. Violates operator expectations,
 - b. Requires performance beyond what an operator can deliver,
 - c. Induces fatigue,
 - d. Provides inadequate facilities or information for the operator,
 - e. Is unnecessarily difficult or unpleasant, or
 - f. Is unnecessarily dangerous."

To Chapanis we are also indebted for the following:

"To say that an operator was inattentive, careless, or impulsive is merely to say that he is human.

"The evidence is clear that people make more errors with some devices than they do with others. ... A good systems engineer can usually build a nearly infallible system out of components that individually may be no more reliable than a human being. The human factors engineer believes that with sufficient ingenuity nearly infallible systems can be built even if one of the components is a human being."

Altman makes the following points:

1. Fragmentary error data are more likely to be useful than fragmentary reliability or safety data.
2. Error analysis is a factor in task analysis.
3. Value in error analysis comes in design and evaluation of error-reducing techniques.
4. Errors can be classed according to detectability, revocability, and consequences - with obvious implications for kinds of preventive action.
5. Error analysis leads often to re-design, automation, and use of human factors engineering.
6. Error analysis also leads to monitoring, (a) to intercept and ameliorate, and (b) to provide feedback to operator.

In routine industrial and product situations, quantitative data may not be immediately available, but qualitative use can be made of the logic and practice of error reduction, even while data collection is being implemented.

Accident studies are, more and more, utilizing concepts of error and error-reduction (American Institutes of Research, 1965). One occupational study reported unsafe acts as due to human error, and referred to them as "microscale mistakes." (Phillips, 1965.)

Swain (1969) argues persuasively that:

"... a means of increasing occupational safety is one which recognizes that most human initiated accidents are due to the features in a work situation which define what the worker must do and how he must do it the situation approach, emphasizes structuring or restructuring the work situation to prevent accidents from occurring. Use of this approach requires that management recognize its responsibility (1) to provide the worker with a safety-prone work situation and (2) to forego the temptation to place the burden of accident prevention on the individual worker."

It is worth noting that Swain's observation applies equally to general performance, and supports a safety relation.

An error reduction program in NSC service shipments in 1948 provided the author with interesting insight on error-accident comparability.

The error report form contained propaganda: "Errors are like accidents. They must be investigated to be prevented." All preventive steps were parallel to NSC safety procedures. Investigations showed a close parallel between errors and accidents. The same kinds of improvements -- equipment, training, procedure, supervision -- greatly reduced errors.

One significant value in human error analysis is the possibility of objectively describing the behavior involved (by contrast with the terms "unsafe conditions" and "unsafe acts" commonly used in safety).

The analytic and classification schemes utilized by Altman, Chapanis and Rigby also suggest the objective nature of error study.

It is useful to remind ourselves of the essentiality of standards of judgment in any error-free, reliable control process. An error consists of an improper action or omission where a standard of judgment exists. For example, in a volume on driver behavior (Insurance Institute for Highway Safety, 1968) two models of driver functions are given in more or less detail -- one neglects criteria for judgment, the other suggests it by a word, but is thereafter silent on such implications as ignorance of defensive driving criteria.

Rigby (1970) said that "tolerance limits" define errors, as follows:

1. "Barrier limits physically prevent or limit unacceptable performance (e.g., retainers, stops, or highway dividers)."
2. "Fixed limits are clearly and permanently established (e.g., lines on a target or street detents on switchs)."
3. "Empirical limits can be checked by measurement or sampling during or after performance (e.g., hole diameters)."
4. "Reference limits can be compared with the output in time of doubt (e.g., samples of good and bad solder joints)."
5. "Caution limits are reinforced by warnings, signs, or other indications (not always available at the time of the action)."
6. "Conventional limits are instilled by training or custom, but may not be otherwise reinforced in the work situation."
7. "Forensic limits are subject to debate and are often defined only after the fact by a hearing or other consensus."

"The above are in order of decreasing effectiveness. Unfortunately, this order is the inverse of frequency. There are seldom well-defined limits on human performance, and where one aspect of performance is defined others are not. Yet, errors are fewer to the degree that workers understand and can work within relevant tolerance limits."

Note that his first tolerance limit provides a point of connection with the Barrier idea discussed earlier!

Note also that his last two limits are the weakest -- custom, and debate after the accident. Yet these ineffective limits are very often seen in accident investigations. If investigations define the tolerance limits in force at the time of the accidents, we will get such statistics as:

xx% of the error limits were in custom,

xx% of the error limits were in debate!

The asking of questions about error definitions in accidents would be

amusing, if it were not so serious. Further, when these same error tolerance limits are applied to examination of managerial factors -- design, risk analysis, safety services and implementation -- the answers are even more alarming. Major elements of the safety program have weak and inadequate definition, and managerial errors and omissions result.

A note of optimism can be injected from the observation that people -- managerial, technical or craft -- often are doing better jobs than are specified when following their training, custom or innate intelligence. Therefore, any move to decrease vague or unspecified error tolerance limits must not fail to get and incorporate the best of present practice.

Surry (1968) conceptualized twelve points in information processing and reaction which, as in actual accident sequences, show numerous opportunities for intervention or improvement, and suggest system analysis needs (Figure 4-1). Her model may be a key to analysis of employee, supervisor, or management decisions in those kinds of emergency situations which emerge more slowly, and if not redirected, develop into major accidents/incidents. Even in accidents which develop with great speed, Surry's sequences provide useful guides for data to be sought in accident investigation. The nature of warning information (e.g., a proposed change in a hazardous material package) may be fairly subtle. From a management view, we could expand the term "physiological response" to include "managerial response."

We shall be tracing management errors as well as operator errors. Therefore we have the interesting possibility that more facts on rationalization prior to management error may be available and may give greater insight. We shall also examine supervisor actions in emergencies and shall find almost no literature on emergency problem solving standards at the point of need. Surry's concept may structure this difficult aspect of supervision.

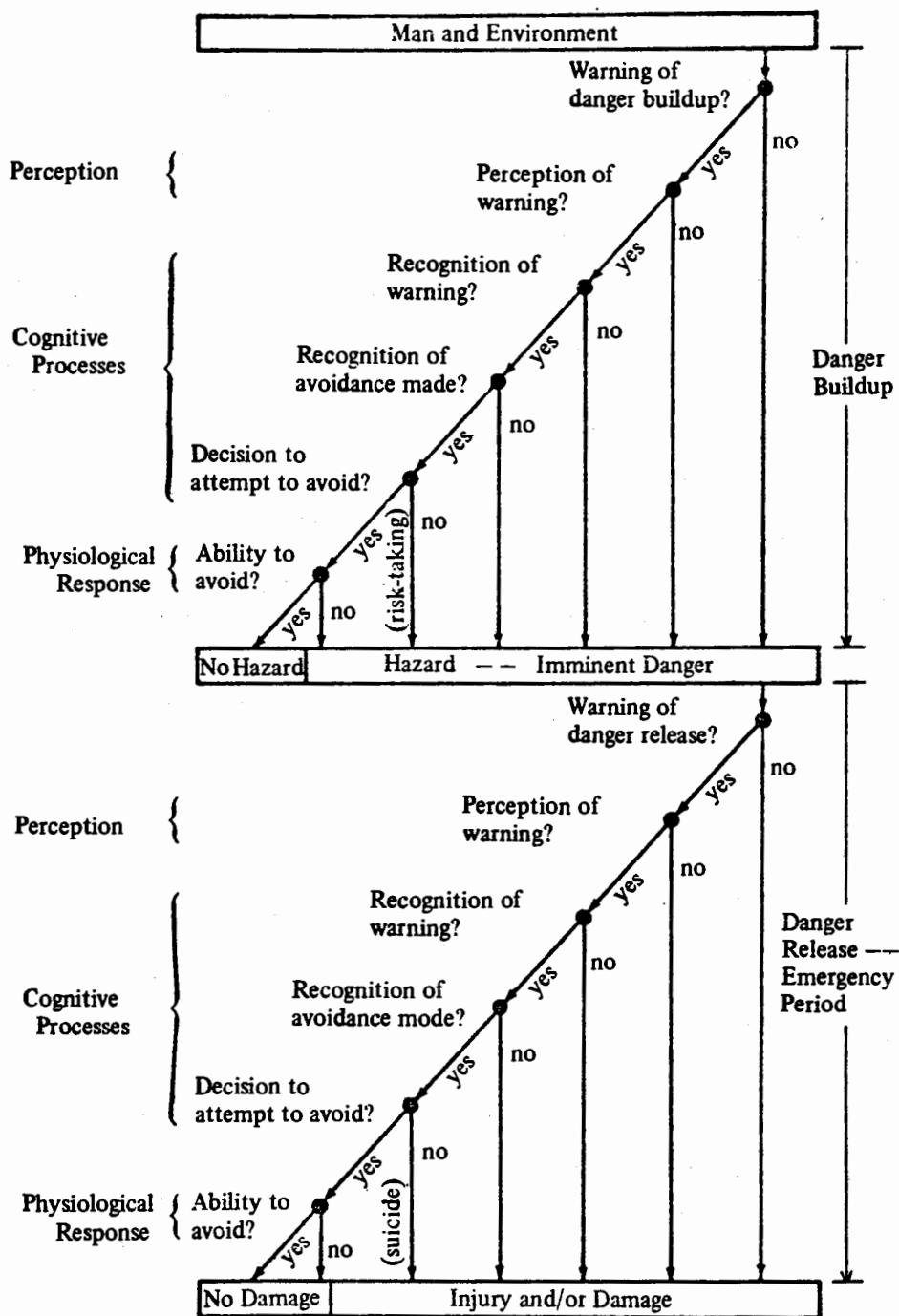
Among the apparently usable ideas from error analysis is the "false hypothesis" (Davis, 1958) or "unwarranted inference." Davis used "preoccupation" and "emergency mechanisms" as other concepts to explain errors.

In considering the unwarranted inference, at least for management and planners, we can make at least a few distinctions in processes as illustrated in Figure 4-2, top of page 55.

Personal risk acceptance and avoidance have had little study in work situations. We can consider and measure failures in perception and reaction in terms of their objective probabilities. Human factors design and training can adjust the task load and improve both skills and their assessment. But the decision to act or not act is based on a subjective estimate of task require-

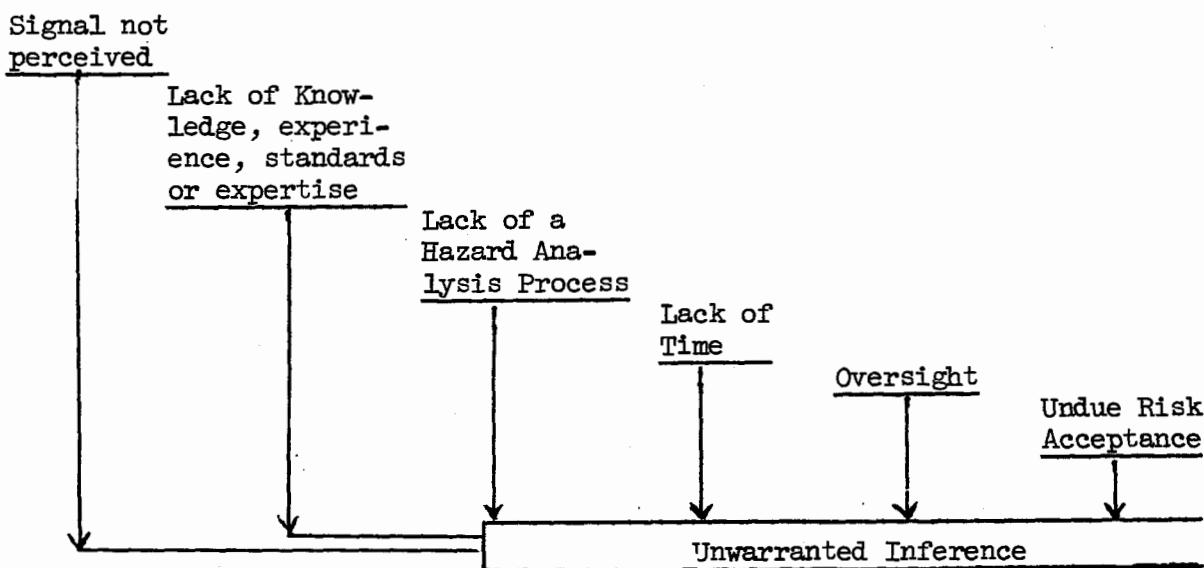
11302
11302

Figure 4-1. A Decision Model of the Accident Process.



Surry, 1968.

Figure 4-2. Decision Premises in Unwarranted Inferences.



ments, skill capability, and values of success, failure, or inaction. These remaining value factors are dependent on attitudes, life experience, social-management pressures, psychological factors, and biographical aspects, according to Rockwell (1968) who found the "high risker" underestimates the risk requirements and overestimates his capabilities. Rockwell also found that the "high risker" tends to seek less information in an experiment involving a psychomotor task. (If this be true for management tasks, and experience suggests it probably is, safety has an additional obstacle.)

Rockwell has counseled the design of systems which maintain alertness without danger. Jones (1970) has urged that sufficient safety decisions remain in a task to heighten skill and decision capabilities. These are difficult goals and in partial conflict with error reduction.

The laboratory studies of non-industrial risk situations may provide some help, but are not easily transferred to practical industrial use. Consequently, they have been held over to Chapter 7, The Role of Risk Management, where the more structured managerial situation may provide a better background for assessing their usefulness.

Most literature on human error, as well as risk, is concerned with personal errors. In this study we shall also examine managerial, supervisory and staff errors, defined as omissions or oversights in a specified hazard reduction method or process. We have seen in this study that some designers are more error-prone than others (for example, in failure to check field conditions until too late). When standards for performing such work are vague (as they usually are), the

designer's error potential is obviously greater than that of the individual operator since the designer's work affects many people and situations.

The emotional overtones of the term "error" are a matter of some concern. Perhaps a variety of terms should be explored. For example, Webster says "mistake implies misconception or inadvertence and is seldom a harsh term."

Rigby counseled as follows:

"We can deal more effectively with human error if we deal with it openly and objectively as a natural and inevitable function of human variability. The term 'human error' should connote no more sense of blame or other emotion than the term 'component failure.' It is merely a way of describing probable events. Emotion only obscures understanding, and it is as wasteful to spend one's time blaming and finger-pointing in human affairs as it is to curse a broken part."

In any event, each error at an operational level must be viewed as stemming from one or more planning or design errors at higher levels. And at whatever level in the organization, human factors review is intended to increase the success rate of all the people who operate the system.

Although human factors review sometimes seems mechanistic in its approach, its purpose is intensely humanistic. Reduction of the causes of failures at any level in the system is not only a contribution to safety, but also a moral obligation to serve associates with the information and methods needed for success.

We shall return to discussion of error reduction in Human Factors Review, and shall also draw on Swain's observations on error data collection in attempting to design an improved accident data system. (Chapter 26.)

However, the latter effort has not produced a general safety data system since meaningful error data has come largely from error rate samples with task specific definitions.

Unsafe Conditions and Unsafe Acts.

These categories of errors are extensively used in accident data collection. However, the fact remains that concepts of unsafe conditions and unsafe acts are usually simplistic and definitions are variable from place to place.

A decision as to what is "unsafe" is subjective and dependent on the sophistication of the classifier. For example, many "unsafe acts" have been cured by human factors engineers, and were probably, in retrospect, "unsafe conditions." Seemingly, the greater the lack of knowledge by the classifier, the larger the "unsafe act" category, and the smaller the "unsafe condition" category.

One study (source will not be cited!) concluded:

"A total of 80% of all the office accidents were caused by unsafe acts and nearly 75% were judged to be solely the fault of the employee to whom the accident occurred."

Christensen (1972) referred to carefully compiled Air Force data showing 60% pure or partial error as dubious data since the role of design error in causing pilot error remains unknown until studied intensively.

During the OSHA hearings, testimony was presented to the effect that 85% of work accidents were due to human factors, only 15% due to physical factors. Such numbers are nonsense! At one research site the author encountered great reluctance to produce such data stored in a computer because the data were known to be so highly colored by the classifier.

Tarrants (1963) did find that two investigators of comparable background obtained comparable results in a "critical incident" study. And he gives suggestions of making such classifications more useful. Tarrants properly argues that reliable error data are needed to judge performance, but attaining comparability is difficult and less subjective use of critical incident data is possible and valuable.

The terms "unsafe condition" and "unsafe act" may be with us for some time, and may be useful if properly defined.

We can define an "unsafe act" as an operational (employee) error. Most accidents appear to have one such error, and may have two or more, the first in the sequence often being an operational error which creates an "unsafe condition."

All work accidents have a sequence of planning (management) errors (or assumed risks) which allowed the "unsafe condition" and the "unsafe act" to develop. The number of such planning errors detected will depend on the thoroughness and sophistication of the analyst. But, if we utilize a defined Hazard Analysis Process, especially a process with human factors review, we are more likely to detect a large number of sequential errors.

This page intentionally blank

5. THE ROLE OF CHANGE IN ACCIDENTS

The role of change in accidents, and more important, the significance and usefulness of change-based preventive and analytic methods, has emerged with increasing clarity during the past ten years.

Historically, the change or revision record on engineering drawings has been both a basis for review and a fertile source of clues as to causal factors in the event of trouble. But accident histories show clearly that a more thorough and searching review method is needed if changes, particularly unwanted side-effects, are to be controlled.

Prior to World War II the role of "change work," such as maintenance, construction and research, was recognized for its effects on plant accident experience. Moves into new, inherently safer facilities were usually accompanied by temporarily increased accident rates. However, practical use of such observations in terms of preventive counterchange was far from clear.

A specific change-based analytic technique has been cited in system safety analysis.

In system safety parlance, a change in "form, fit or function" of a part has signalled review of components and subsystems (including interfaces) upwards in the design review channel until no change is demonstrated. Interestingly, in discussing organizational behavior in general, and the hierarchy of subsystems, Seiler (1967) observes that change in a part has a vastly greater effect on a sub-unit, and counsels analysis of effects on the sub-unit before considering the totality. So, whether hardware or people are changed, any change should be reviewed on up the system until no change can be demonstrated.

In any organization there are readily available data on certain classes of changes: new employees, transfers, work orders (classed by size), and new projects (classed by size). All such sources should be systematically canvassed and then current data can be helpful in guiding safety attention. Accident rates can be related to these indices of increased hazard.

An illustration of change, and sequence of change may be helpful. Here is a case history and a puzzle:

Before Changes -- a large chemical plant had operated uneventfully for years.

Change 1 -- The plant was replaced by a larger, more efficient plant.

Change 2 -- The first plant was decommissioned and partially disassembled.

Change 3 -- The new plant didn't produce as well as expected (at first).

Change 4 -- Demand for product grew more than expected.

Change 5 -- Put the old plant back in production.

Can you write the scenario as to what happened? (Try! The answer is in a foot-note on page 62, but try before you peek!)

In another episode on a lesser level, involving a three-stage compressor developing 3,000 psi for a research experiment, a lower pressure was drawn off to actuate a house circuit for pressure-actuated tools. All went well.

Change 1 -- The 3,000 psi compressor was no longer needed and was not active.

Error 1 -- The equipment was seen by an outside pressure vessel expert who made some recommendations if the equipment was ever used. The equipment was not tagged, marked or made inoperative.

Change 2 -- After $1\frac{1}{2}$ years of non-use and non-maintenance,

Change 3 -- A mechanic decided to activate the compressor to use a wrench to remove a few bolts - a rather massive case of overuse of energy!

Error 2 -- The project engineer in charge of the work conducted no perceptible pre-job safety analysis.

Change 4 -- The mechanic started the compressor and it shortly blew up, narrowly missing a one or two fatality accident.

Levens (1970) alluded to change as stress on a system previously in a state of dynamic equilibrium, and spoke of stress as anything which disturbs the normal (planned) functioning. Thus change is an element in hazard identification.

Regarding the role of change, Altman (1970) said:

"We explored briefly before the need in error analysis to allow for changing conditions. The rapidly changing requirements and conditions of modern industry have implications for learning and accidents. Indeed, training for safety might sometimes be almost easy were it not for contingencies and change."

In a broader sense, changes in employment or economic conditions may have similar effects. Tuz and DeGrazia (1967) found:

"..... there seems to exist a rather significant relationship between cyclical fluctuations in economic variables and changes in accident frequency of manufacturing concerns when these accident rates are suppressed to low levels."

An analysis of routine accident reports from a number of corporations to detect the role of change yielded two types of results:

1. Most reports were grossly deficient in identifying changes that contributed to the series of events that resulted in the accident -- report

forms did not ask the pertinent questions.

2. Where reports were, by chance, complete in the narrative section, the number of changes was so great it was amazing they didn't kill everybody!

A similar finding for routine reports was made in the AEC study.

An interesting commentary on the relation of change and danger is made by McKie in "The Company of Animals" (1966):

"... jungle man has an acute awareness of surroundings, that is, a sense he has not lost or has resurrected, ... atrophied or dormant in most of us, which warns him not only of direct danger, but also of changes in the patterns of jungle life - changes which could be a prelude to danger."

The sensitivity to impending or probable change may be a key component in the work of a good, experienced manager or safety professional, which has sometimes been described as having an "almost intuitive" quality. In an accident in experimental equipment operating near technological boundaries (Figure 5-1), which the field safety engineer would have difficulty understanding or analyzing for hazard, there were numerous changes, performance problems and failures, and a lengthy period of overtime work associated with "high energy" heaters. The latter signals of stresses and energy could probably have been detected by an observer alerted to their significance. Thus, one aspect of the work of a field safety engineer seems susceptible to more precise and useful definition. (See Figure IX-2, page 453 for an application.)

In discussing sensitivity to change with a manager, he argued that his people were sensitive as the result of several incidents, but this is an expensive method of training and will atrophy with time. So training or other sensitizing methods are needed.

An exploration in supervisor training for sensitivity to change employing some simple forms and questions was undertaken in this study, but the trial was largely unsuccessful.

At Lawrence, a group of maintenance and job shop foremen were given a "Change Docket" with two blank columns headed "Changes" and "Counterchanges." This was also given to their supervisor. The instructions were to enter in the first column any "significant changes which probably need thought and attention" and in the second column the preventive counterchanges needed. Two examples were provided. The first, for a foreman, listed such things as a new press, a new material, a new employee, a rush order requiring overtime, a person who was angry, an outbreak of first aid cases, a quality (reject) problem, and the supervisor's planned absence for personal reasons. The second sheet, for the organization president, listed an increase in product liability suits, a marketing V. P. killed in an off-the-job traffic accident, "competent, responsible people are not available in needed numbers, and turnover is high," "supervision is deteriorating and here, too, turnover is rising." On both sheets some possible preventive counterchanges were shown. Whether because changes were too numerous in their work, or because

a new approach not well understood in management levels could not be easily used, the men involved produced little that was helpful to them.

In the closing interviews it was apparent that the four-week trial had contributed little, if anything, to change sensitivity. One foreman reported that his absence due to sickness had struck him as a potentially harmful change. All are strongly oriented to the practical content of their work, rather than abstract concepts. And this is probably as it should be.

Since line supervision in much of Lawrence's research operations is divided between the Division staffs and the faculty who direct the graduate assistants, trials in a normal line production organization were not possible.

Another trial and perhaps other approaches seem warranted when the change concept is more fully developed in managerial and safety staffs.

Lawrence did, however, have two safety operations keyed to the role of change:

In a large building containing numerous chemical laboratories, a corps of health physics technicians, constantly moving about monitoring for radiation hazards, had been trained and sensitized to note changes and differences and to promptly report them to a chemical safety engineer for field review.

Five members of a chemical divisional safety committee (a scientist, business manager, two lab supervisors, and a maintenance machinist), after four weeks' trial, felt they were already sensitive to change and that it was, indeed, their primary concern!

In neither group did the change concept appear to enhance sensitivity to potential hazards. Both groups, the health physics monitors particularly, felt that they were already sensitive to and acting on changes.

What is the practical significance of this Change idea? The answers seem to be:

1. Systems fraught with changes usually generate additional hazards (e.g., research, construction and maintenance, or transfers to new jobs). We can be sensitive to the nature of "change work."
2. We can be sensitive to change situations -- transfers, new machines, new materials, new operations, modifications, shut-down, start up, etc.
3. We can strive to augment the essential feedback to detect those changes that could contribute to accident sequences.
4. Sensitivity to change (and the possible need for an offsetting counter-change) is a mark of excellence for a manager, supervisor, or safety

Answer to episode, page 60.

Change 5 -- Put the old plant back in production.

Change 6 -- Restore necessary operating controls to get back in production as quickly as possible.

Error -- Lack of formal review for hazard analysis and/or operational readiness.

Change 7 -- Some redundant safety controls were not reactivated.

Change 8 -- The plant exploded, killing six men.

professional. We can explore training methods to sensitize supervisors to detect and react to significant change.

5. In systems theory, review and counterchange theoretically follow every "significant" change.
6. We have some new ideas as to what to seek in accident investigation.
7. If a major problem has obscure cause, or if we want to dig out underlying causes, we have available a relatively sophisticated method to search for that change which is cause.
8. On the negative side, change is continuous and many changes apparent in accident reports simply amount to truisms. We have much to learn to sort wheat and chaff in our perception of changes, and our subsequent preventive counterchanges.

The point has been made that an accident is after the fact, post-mortem or "tombstone," and that error (unsafe condition and unsafe act) is before-the-fact of an accident. It seems further true that "change" is before-the-fact of error. Therefore, a managerial system should be based on change identified and counterchange.

Changes are myriad. If change is to be a useful criterion for systematic safety action, we shall be forced to construct standards of judgment as to kinds of changes to be handled at various levels according to whether energy management standards are available, or new information is needed.

Change-Based Analytic Methods

In 1967 the author said:

"A basic theory and a body of experience indicate Change to be Cause of a Problem. Some case histories and sporadic experiences indicate the basic theory may be a major contribution to concepts of accident causation and may provide a foundation for improved methods of accident investigation and prevention."

Findings in this study confirm and expand on the earlier belief. The basic thesis is:

For any system in operation which has been going on satisfactorily (i.e., up to some standard), Changes associated with energies and errors are Causal Factors of a Problem.

This provocative thesis, which has considerable potential for safety, was developed in Rand studies for the Air Force. The concepts were made explicit in a text book, "The Rational Manager" (Kepner-Tregoe, 1965) and a one-week training course* which has been widely used in business for control of quality and other aspects of work. Interestingly, a large proportion of the examples used in the training course were accidents.

* Conducted by Kepner-Tregoe, Inc., Princeton, New Jersey

An example was cited by a safety engineer who was a member of NSC:

A car manufacturer had serious quality control problems on an assembly line. The Kepner-Tregoe cause analysis method traced cause to weekly transfers of employees on a seniority basis to fill vacancies, and the proof was sufficient to persuade the union to accept monthly transfers.

The improvement in quality was as expected. An unanticipated dividend was a decrease in accidents. That is, change was the cause of both problems, poor quality and accidents.

This case is especially valuable because of its implications about the congruous character of control of work for quality and accident prevention.

The above case also illustrates a common contrast between Kepner-Tregoe methods and those apparently needed for accident analysis and control--the contrast of single cause analysis with multi-factoral analysis. Single cause analysis has great efficiency where it is adequate. Experience before and during this study shows that numerous changes, coupled with failures of successions of energy control features interact with latent, more or less continuous errors. Thus the change-based analysis and control methods used in safety should reflect the multiple, sequential realities rather than rely on possibly simplistic detection-correction of a single causative change.

In 1966 the Kepner-Tregoe problem analysis method came to the attention of the author. Several of us on the NSC staff enrolled in the training classes. The training has been applied in NSC systems analysis courses, and has played an important part in this study. In the Aerojet trials the Kepner-Tregoe text had substantial usage and was beneficial. But the best advice for any large organization is to enroll at least two staff members in the training course, and then, after trials, consider organizationwide usage on all manner of problems.

Grizzly Bears. The author's first effort to use Kepner-Tregoe analysis was in assisting the National Park Service to analyze the two grizzly bear fatalities in Glacier Park in 1967. Some of the experiences in that work seemed unique at the time, but they have been confirmed in subsequent analyses of occupational accidents and therefore the accidents and analytic methods are worth summarizing briefly:

1. From press reports it seemed that cause was obscure.
2. A standard with 57 years experience to validate it was: "Grizzly bears do not seriously chew on people in sleeping bags at night."
3. The Deviation - two girls in sleeping bags were killed by two bears in a single night. Chance? One in a trillion. The Kepner-Tregoe method says, "Something in the park has changed."

4. Upon arrival at Glacier Park the author was briefed for $1\frac{1}{2}$ hours and then read transcripts of witness statements. In about five hours all the facts or probable facts of the two accidents were concisely displayed in an orderly way and showed the changes which were likely causes. (No experimental verification is possible in such episodes, so if we are to do something, our preventive action must be based on circumstantial evidence.)
5. The analytic method was not fully satisfied, in that it should display a reportable change in one bear (the other had grown old). When a research biologist saw the information needed, he instantly supplied it -- a fresh five inch cut on a foot of the bear. (If you know what information to seek, it is often readily available.)
6. The basic cause -- a steady increase in hikers on the trails and their garbage by late summer of 1967 likely was producing exponential adverse effects on the bears' habit of avoiding man. There were other factors (e.g., menstrual cycles), and the method was also helpful in disposing of possible causes not having circumstantial support (e.g., a dog with one party).
7. The elements of a solution:
 - a. Revised doctrine on garbage (take it out).
 - b. Concise doctrine for visitor behavior (leaflet).
 - c. Better monitoring systems for bears and people. Ranger patrols and employee reports of bear sightings.
 - d. A trigger mechanism -- close the trail at the first report of a bear which is not avoiding man.

Many of these early ideas will be seen in more fully developed form in MORT, especially the multi-factorial aspect. A further example of multiplicity of factors is reflected in another example developed during this study.

In an experimental heater accident (Figure 5-1) the "IS" was a semi-scale heater. The "IS NOT" most closely resembling the "IS" was a predecessor quarter-scale heater. The distinctions and changes could then be listed, and they were the technologic roots of the accident. In charting this accident, the Figure shows a left hand tab was added for "managerial controls" and it was then evident that distinctions and changes in these had occurred which allowed the technical problems to cumulate and escalate. Other stresses, such as lengthy overtime, and the trigger event (closing a circuit breaker without checking for cause) could also be neatly displayed.

The Change-Based Accident Analysis (Figure 5-2) provides for examination of 25 potential factors, but even that number is not fully definitive, and the analyst should not hesitate to add to the list as the actual event dictates.

In the columnar spaces the characteristics of accident situation are specified as precisely as possible:

1. Present situation
2. Prior situation (or most nearly comparable situation)

Figure 5-1
Problem Analysis Worksheet
Semiscale Heater Accident

Heater element fails, and other elements fail in rapid sequence.

	IS	is NOT	DISTINCTIVE	CHANGE
WHAT? Project	Semiscale 65 kw load Elements brazed in place in San Diego Reused old power circuitry 32 elements on a circuit	Quarterscale 10 kw Insert method used in $\frac{1}{4}$ scale? Designed for task 120	Larger Handling, protection more difficult Harder to fill and construct Closer to technical boundaries Protracted failures in development. Lower reliability More handling, less control Not easily replaceable. Less costly, quicker If 1 fails, load rises 3% rather than .8% If 2 fail, 6%, not 1.6% If 3 fail, 9%, not 2.4% Etc., etc. in escalation, immediately.	(thermocouple welds failed) 1 element likely to fail Tighter budget and schedule?
Protection	Single-failure Manual controls	Double-failure Automated	Cheaper; less safety F/ can escalate w/in reaction time.	
WHEN?	After protracted failures After days of 17 hours	Going well Normal	Protracted stress on people Nearing deadline Acute stress and fatigue	Any change in schedule? Error-provocative situation.
Trigger:	1 element fails Supv. told technician to reset breaker	Checking for cause	"Engrs. & Sci. do this"	Failures escalate rapidly
Managerial Controls	Ad hoc engr. & devel. group Project w/o independent review Procedure w/NOS personnel safety review Essentiality III 2 Special Reviews of R&E operations d/n detect NOS surveillance d/n detect AEC surveillance and appraisal d/n detect After repeated reports to management Risks assumed at intermediate level	Established engr. div. Present review system (installed later) Review of hardware envelope I or II Review of analytics nor audit against criteria Surveillance plan w/criteria Surveillance plan w/criteria w/o reports w/formal analysis	Not structured, audited, w/o internal review, etc. "Faster,cheaper,more convenient" w/o critique, by technically competent peers w/o envelope, can't detect R&QA does not monitor automatically. Cannot detect impending deviations. Management could assist, guide, correct Decisions might have been different	Change from $\frac{1}{4}$ scale? Is this a change or normal?

NB: Prepared to show analytic technique and a possible way of displaying factors.
 Facts represent the consultant's understanding of the Board's findings. The conclusions are his own.
 It is precisely because AEC systems are highly structured that gaps can be detected.

NOS = Safety
 R & QA = Reliability and Essentiality

Figure 5-2
Change-Based Accident Analysis Worksheet

Subject _____

Factors	Present Situation?	Prior, Comparable?	Differences?	Changes?
<u>What</u> Object(s) Energy Defects Protective devices				
<u>Where</u> On the object In the process Place				
<u>When</u> In time In the process				
<u>Who</u> Operator Fellow worker Supervisor Others				
<u>Task</u> Goal Procedure Quality				
<u>Working Conditions</u> Environmental Overtime Schedule Delays				
<u>Trigger Event</u>				
<u>Managerial Controls</u> Control chain Hazard analysis Monitoring Risk review				

3. Differences between 1 and 2

4. Changes in the differences, or resulting from the differences.

In a complex, protracted event, the author found a time-ordered arrangement helped display the sequences. One of the Glacier Park grizzly bear fatalities in 1967 was of this nature.

In an analysis of two dropped loads by one crane, the number of columns was doubled to distinguish events 1 and 2, and then look for common features or distinctions.

In seeking relevant distinctions it is productive to compare the present problem in terms of the same object the day before, the week before, the month before, the year before. (At first, the questions: How is this changed from the hour before, etc., seem a little silly. But, when the changes and distinctions emerge they often prove to be serious.) In most cases there has been change(s) which is cause.

Change-Based analysis is useful in three stages of a problem:

1. Knowing what additional facts are needed. Very often the relevant facts are quickly available if their need is pin-pointed, and this is much more efficient than a half-blind search for "more information."
2. Finding obscure cause. At the initial stages who knows what the causal factors are? Therefore, the use of the format as a convenient way of summarizing findings and information needs as investigation progresses is recommended. For this purpose it is usually well to rule up a 17"x23" sheet on which to organize cryptic notes.
3. Presenting findings in a concise, precise and well-organized way.

Consequently, the use of the format, at least as a worksheet, for any serious accident or problem is wise.

Aerojet has had extremely high standards for formal change review, especially for modifications and experiment insertions in reactors. As criteria were upgraded, a specific requirement to "define differences from previous tests" was added, partly as the result of a change-induced accident probably detectable by the analytics in Figure 5-1. This can be done in a meaningful way by simply changing the right hand column heading on the Change-Based Accident Analysis Worksheet (Figure 5-2) to "Preventive Counterchanges" and thus produce a "potential problem analysis worksheet related to changes" with a capacity for detecting unwanted side effects of improvement or unplanned changes.

Figure 5-3. Potential Problem Analysis Worksheet for Changes

Specify the change(s) in this project as compared with the most recent, and most comparable past projects.

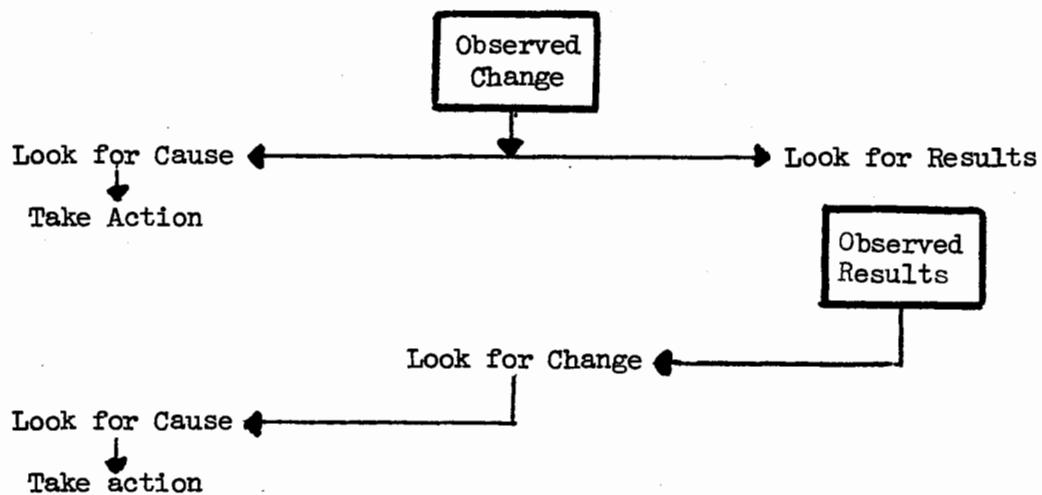
<u>What?</u>	<u>Present Proposal</u>	<u>Prior</u>	<u>Differences</u>	<u>PREVENTIVE COUNTERCHANGE</u>
<u>Project?</u>				
<u>Technology?</u>				
<u>Who?</u>				
<u>Where?</u>	Extended list as pertinent from Fig. 5-2			
<u>When?</u>				
<u>Managerial Controls?</u>				
<u>Extent?</u>				

A NTSB (1971) report on risk concepts stressed the increased levels of risk which resulted from inadequate analysis of changes in methods of transporting hazardous materials.

Reference to the role of change will be found throughout the text, often taking the form of questions about specific changes.

In safety program planning, a series of schematics has been developed to show action implications of change.

Figure 5-4. Action Implications of Change



Classification of Changes.

In a presentation developed some time before the NSC staff began to give study to the phenomena of change, Roy Benson, Manager of NSC's Industrial Department, had produced a display of "thought starters" on preventive changes.

Figure 5-5. Some Kinds of Counterchange

<u>MODIFY</u>	<u>REARRANGE</u>	<u>REVERSE</u>	<u>REDUCE</u>
Color	Sequence	Order	Omit
Shape	Pace	Direction	Shorten
Sound	Components		Split
Odor	Schedule		Condense
Motion	Pattern		
Meaning			
Light			
<u>ADOPT</u>	<u>SUBSTITUTE</u>	<u>COMBINE</u>	
Outright	Ingredients	Blend	
Related	Power	Units	
	Process	Assortments	
	Approach	Ensembles	

It seems likely that this also is one first approximation of a taxonomy of changes which cause accidents. That is, to take the first illustration in the Figure: a new object is introduced and superficially is the same as its predecessor; safety characteristics are different, but both are the same color; an accident results; solution - change color. In a powder-powered tool accident, a tube extension was left in from a previous use and not detected. If it had been colored red, the change might have been detected. (Interlocking with the shield would be better, but more expensive.)

No complete taxonomy of changes has been discovered thus far in the AEC study, but some facets emerge with increasing clarity. For example:

1. Planned vs. Unplanned.

- a. Planned - require scaled Hazard Analysis Process (HAP), and affirmative safety action.
- b. Unplanned - first, detect by monitoring. When detected, (2) make immediate correction when necessary, and (3) require scaled HAP.

2. Actual vs. Potential or Possible

- a. Actual change is detected by reports and observations.
- b. Potential or possible change requires analysis.

3. Time - deterioration of a process over time, interaction with other changes.

4. Technological - the new projects and processes, particularly near technological boundaries.
5. Personal - the many variables which affect performance capability.
6. Sociological - closely related to personal changes, but of broader significance.
7. Organizational - shifts in unit responsibilities may leave interface gaps, particularly when HAP was ill-defined, but done by custom by some people.
8. Operational - changes in procedures without safety review.
9. MACRO vs. MICRO

- a. MACRO - overall organization data, e.g., new employees, transfers and other operating data suggesting needs for preventive countermeasures.
- b. MICRO - particular events, as classified by such a system as MORT, but then through MORT leading back to MACRO changes needed, such as management implementation.

A useful subdivision of micro-events might be early detection and counteraction, e.g., a plan to promote a supervisor and then promote his assistant. What does this change imply?

The use of MORT analysis, thus far, has been largely on a clinical, case-by-case basis. A moderate number of case histories have been accumulated. But a review of the cases to develop a tight classification or taxonomy of changes useful in preventive work has not been done and remains a project for the future. On the other hand, findings have been incorporated in MORT analysis as rapidly as they appeared, so we are not wholly without answers to such questions as:

1. Do types of change relevant to accidents give characteristic advance signals? Many of them definitely do give signals.
2. Do types of changes point to types of countermeasures? Here the indications are that regulations may be a first level answer, but hazard analysis, including human factors review, is usually needed.

Research needs would seem to include study of clusters of accidents by type of change.

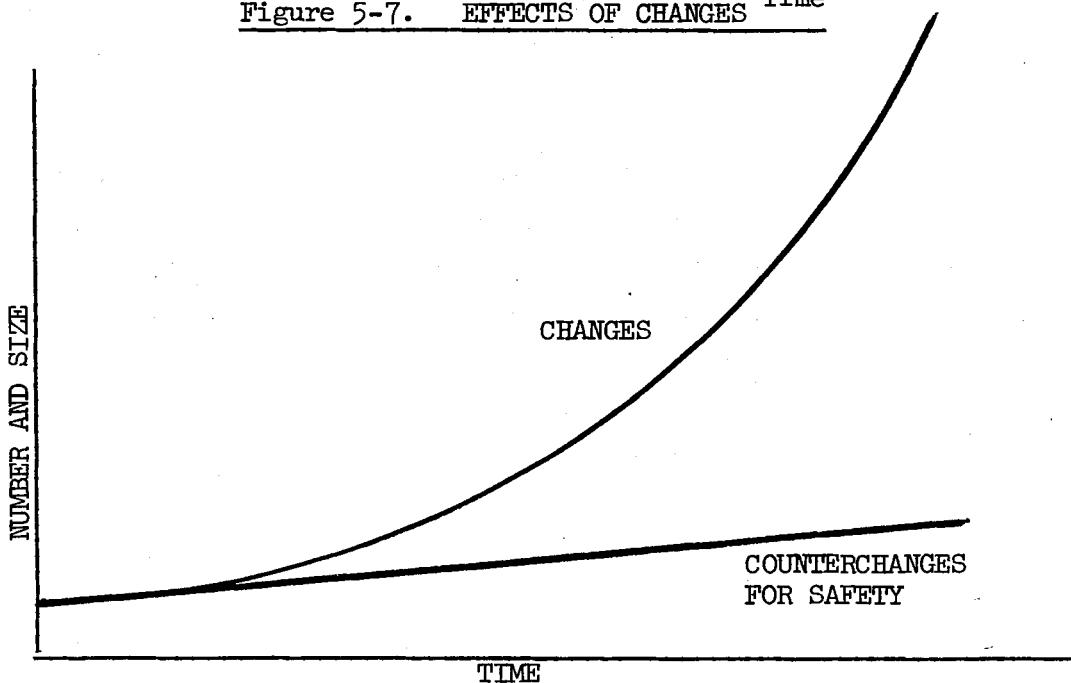
Some Awesome Changes. Beginning as far back as the 5th century B.C. with Heraclitus and Parmenides, and extending through such men as Disraeli, the role of change in society has been debated and discussed. However, the current

literature increasingly refers to the directional and exponential nature of change in modern society. For example, Gregory (1967) describes the exponential increase in the tempo of change and describes problems as "children of change." Another commentator used the acronym ROCOROC to describe increases in "the rate of change of the rate of change." Wood (1967) begins a discussion with the phrase, "As we ride the tiger of exponential change ..." Very apt for safety, and we can call the tiger ROCOROC! (See special bibliography at end of book.

Directional means that change most often keeps on going, and doesn't change back. If you are hoping for a return to some "good old days," forget it! In safety, this means more technological challenges, not fewer.

Exponential means that changes interact to compound the effects on accident exposure. Larger railroad cars or trucks are filled with more exotic material and go faster on roads with more traffic. New materials and advanced technological equipment must often be operated with less skilled and less motivated personnel. Thus exposure to accidents tends to move as E^2 , E^4 , E^6 , or E^8 . The implications for the kind and amount of control which will be needed are clear in Figure 5-7 which takes a rather pessimistic view of our current rate of safety progress.

Figure 5-7. EFFECTS OF CHANGES ^{Time}



It is not difficult to see plant siting criteria as involving

- (1) potential growth in plant size (and in any of its adverse effects)
- (2) probable growth in nearby plants,
- (3) growth in traffic and residential density, and
- (4) growth in public concern.

Thus future impact is a function of E^4 , and should be reflected in current precautions and adjustments.

Toffler (1970) has described acceleration of change as an "elemental force" and said we must control the rate of change or suffer an adaptational breakdown -- "future shock." Without choosing sides on this issue, the effort in this text will be to outline some techniques whereby we might avoid the impending breakdown by effective adaptation.

The view that ecologic threats to man are serious, and becoming more so, is pervasive in the press and on the air. Any injury rate upturn may be just one more evidence of systemic troubles poorly understood and inadequately coped with. There are reasons for believing that more cogent and successful methods of coping with threats in the relatively controlled environment of employment may have the added value of suggesting rationale, method, scale and pace needed in broader spheres.

The Change-Based methods (plus the grizzly bear episode) greatly aided the author's early work on models of general safety systems. For the NSC Boards and Conferences meeting in October 1967 a presentation entitled [Effects of Changes]^{time} showed the role of exponential change. Figures 5-8 and 5-9, taken from that presentation, show the sequential role of change-error-accident, and the general system shows the early seeds of the general system evolved in this study -- that is, information and analytic processes feeding into a dynamic performance-oriented system.

Interestingly, when the above presentation was given to the 7th National Park Service Management Safety Planning Conference, coupled with the results of the grizzly bear cases, several senior executives said the system appeared to be a good way to manage the parks in general. So far as we know, this was the first time any safety system was seen by management people as a general management method for accomplishing anything. (1967.)

Ecosystem? A portion of the change literature listed in the special bibliography is concerned with the role of change in ecosystems. In this sense Glacier Park, the Chicago Metropolitan Area, or an industrial establishment can all be managed as ecosystems. A working familiarity with the change literature would supply insights helpful to the safety professional.

In the presentation to NSC the author said this:

"Unfortunately from the study of natural ecology, we have time in an exponential position in our equation. And that is an awesome place to put time."

Figure 5-8. Sequential Role of Change-Error-Accident

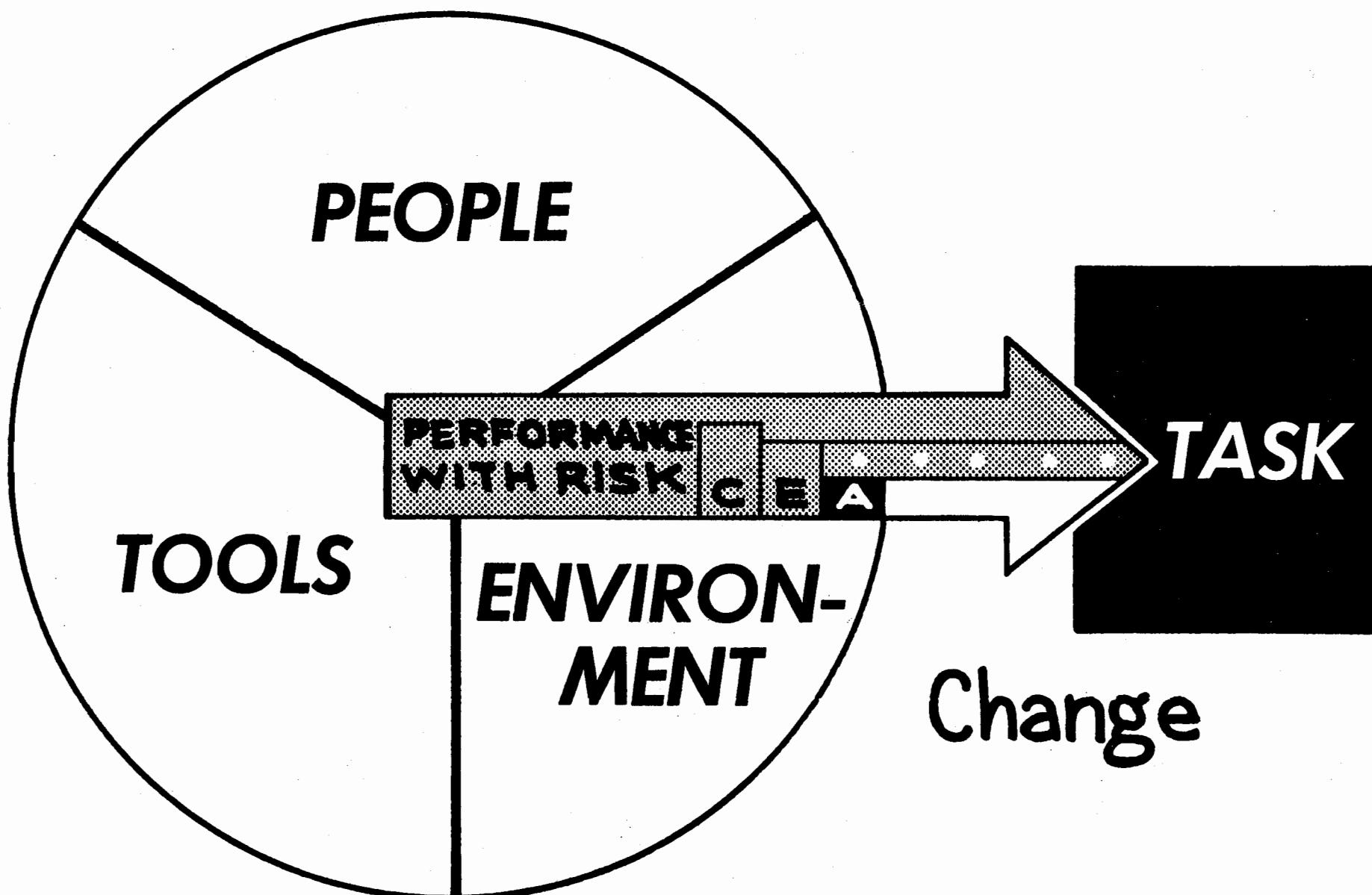
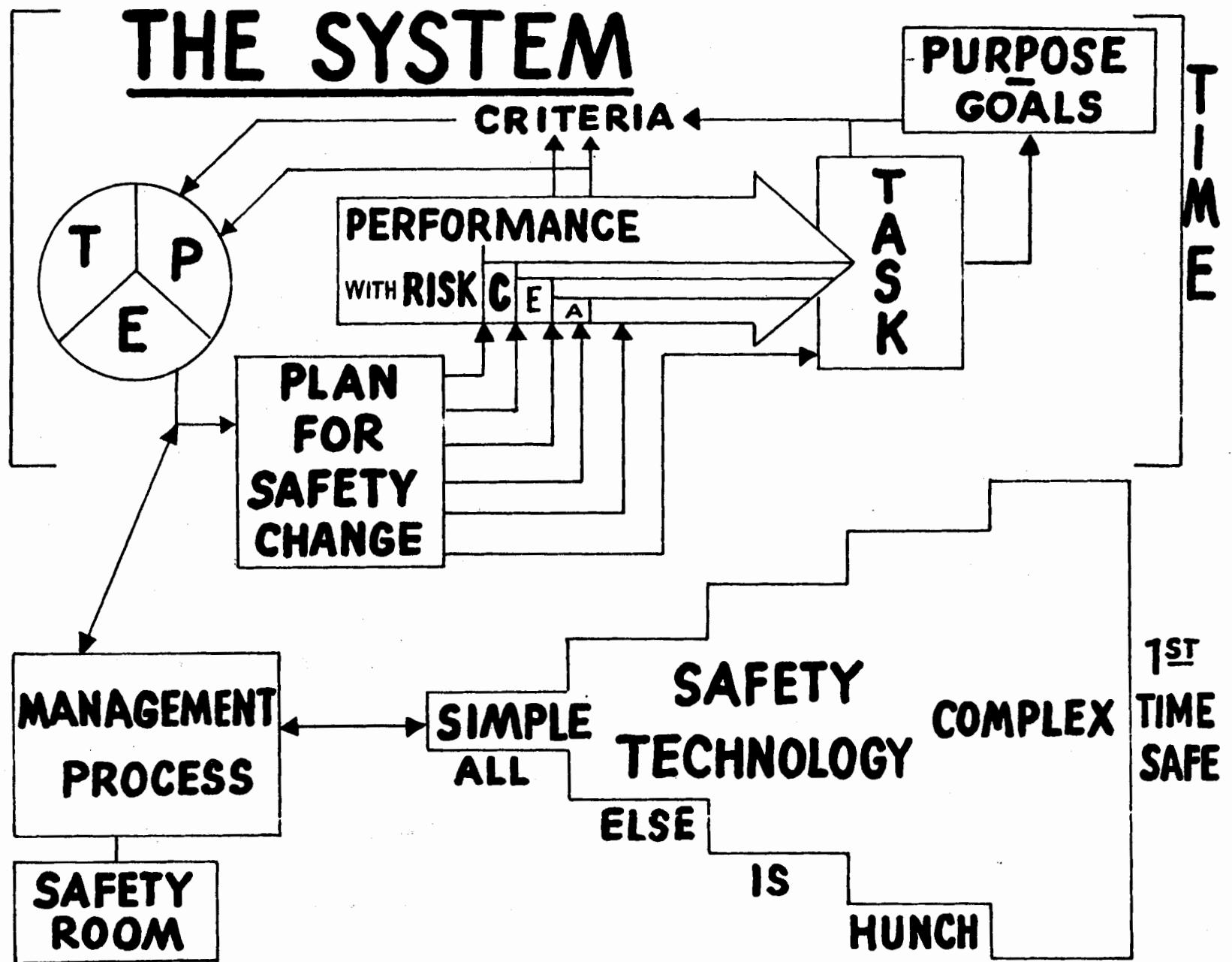


Figure 5-9. General System



It means that between two periods of time, one decade versus the next decade, that when you put a "2" in an equation, the problems of change get four times as big, and this, I am sorry to say, is what I think is happening to the world right now. We are dealing with the exponential change in our problems.

"Fortunately, I think we are also dealing with an exponential change in our capacities to deal with problems. This is what all of the hardware and software is about. So it would seem to me we have to see ourselves faced with a sharply rising set of problems, such as hit us in motor vehicle safety the last few years. If we expect to stay alive in the world, either as users or as the National Safety Council, we must tap exploding problem-solving technology, and use it to our own advantage.

"The forces of change are sweeping across the world. We must mount counter-changes for safety and scale them with equivalent force. Man has proven capacity to adapt to many aspects of past change, including safe handling of growing energy resources. But the pace of change clearly indicates the urgency of finding better methods of dealing with accelerating effects of change.

"This is a general safety method, but looks preliminarily as if it may also be a general method for accomplishing anything at all."

We are here concerned with the role of change in accidents. However, we should not be unperceptive as to the role of change in the organization as a whole. Congruence between general management and safety management may, indeed, begin with this perception of relevant, significant change, and the need for preventive counterchange.

The organizational manager is or should be concerned with changes and potential changes in (1) economic, political, and social factors which affect his organization; (2) technology, his and that of others; (3) physical, human, and ultimately financial resources of his organization; and then, of course, (4) markets for raw materials and products; and (5) alternative developmental potentials, e.g., his competitors or obsolescence.

It is not difficult to perceive how the general manager's concerns for items (1), (2), (3) and (5) above can and will be reflected in specific concerns of the safety manager.

It would be nice if the safety manager had an explicit method, philosophy or practice whereby the general manager could easily see the safety manager as a potent source of analytic and planning capability attuned to the organization's problems and difficulties in coping with change.

What remains to be demonstrated is the degree to which a safety effort oriented to change could assist the general manager in solving organization problems. We have had some encouraging experiences at Aerojet: for example, we have used change analysis techniques which seem simple and effective on specific projects. Broader safety-related changes or potential changes in the organization as a whole remain to be examined.

Systems analysis methods provide the capability for an exponential increase in preventive power attuned to the rate of change, provided that analysis and research are proportionate to changes and problems. A major thesis of this text is that a synthesis of safety practice is needed to "ride the tiger of exponential change."

This page intentionally blank

6. SEQUENCES IN ACCIDENT CAUSATION

Accidents are usually multi-factorial and develop through relatively lengthy sequences of changes and errors. There are strong indications that for the most serious events in a relatively well controlled work environment, the sequences are often themselves numerous, and in series and parallel. This complexity also means there were many opportunities to intervene or interrupt the sequences.

Schulzinger (1956) after a twenty-year study of 35,000 accidents offered two provocative descriptions of sequences:

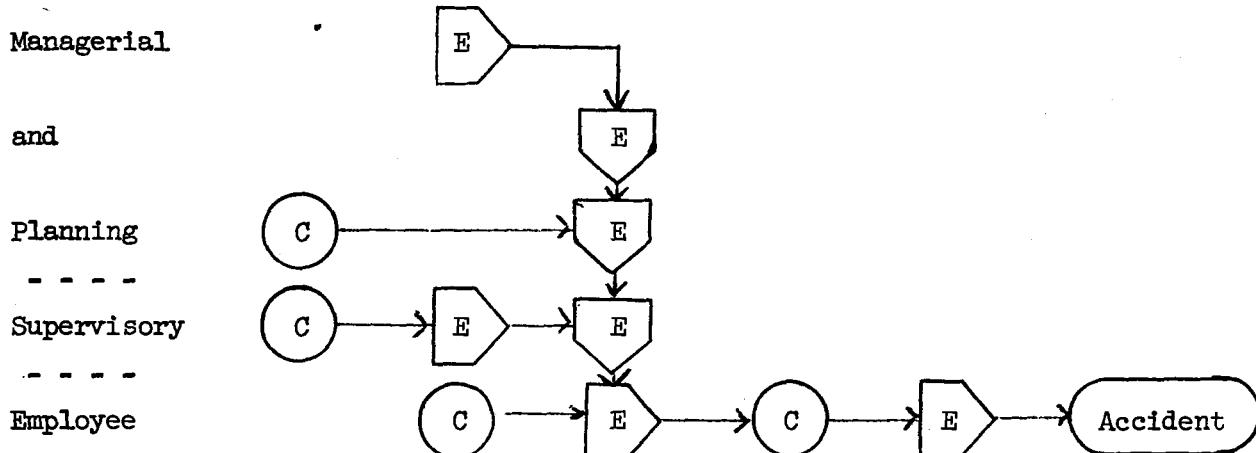
1. "a dynamic, variable constellation of signs, symptoms and circumstances which together determine or influence the occurrence of an accident."
2. "a synthesis of environmental, psychological, physiological, characterological, and temporal factors."

MORT analysis of serious accidents typically shows on the order of 25 specific factors and 15 systemic failures, many of them linked in causal or temporal sequences.

Levens (1970), in Search I, pointed out that, while not as desirable as preventive design, the hazard sequence offers multiple opportunities for interruptions by corrective or protective action.

One accident report showed cross-linked sequences of errors and changes which could be diagrammed as follows:

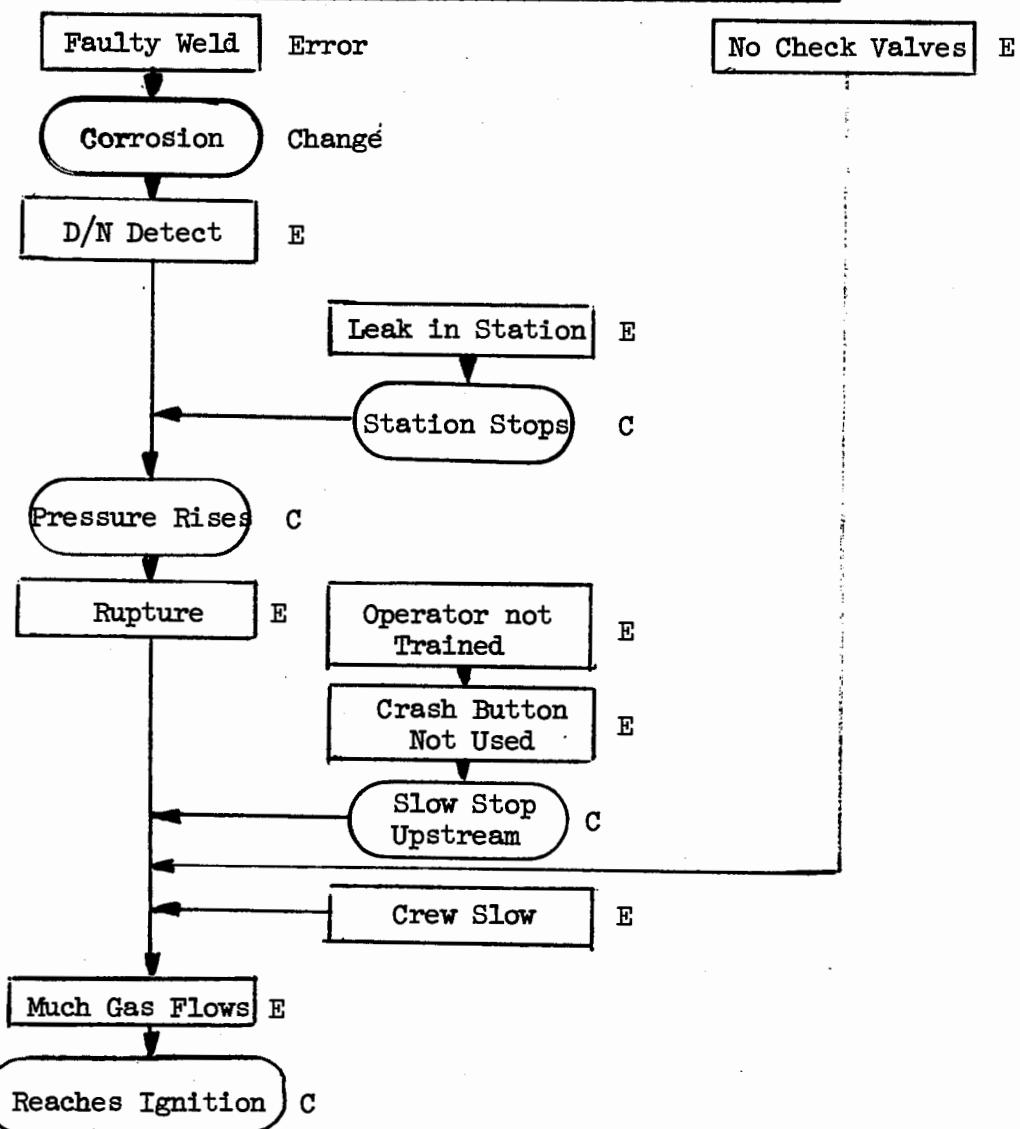
Figure 6-1. Sequences of Errors and Changes



Safety texts have used a row of falling dominoes as a model illustrating the accident sequence. This may be such a gross simplification as to limit understanding.

A recent pipeline accident report by the National Transportation Safety Board (NTSB) provides the basis for another sequential analysis (1972):

Figure 6-2. Gas Pipeline Accident Sequence



Reading the reports of major investigations of NTSB is very illuminating. Substantial numbers of recommendations for interrupting sequences are normal. Similarly, the major investigation reports prepared under AEC procedures commonly show lengthy sequences of causal factors, an average of sixteen per case for one sample.

Review of individual reports shows surprisingly frequent two and three person (or two department) involvements in serious accidents. This could arise from the fact that good organizations have successfully handled the simpler potentials. In any event, it seems essential that accident investigation methods and summaries give appropriate visibility to the complex

realities, rather than simplistic, one-at-a-time, categorical labels of conditions and acts.

Among the apparent sources of complexity revealed in accidents, is the non-routine operating mode. Trials and tests, maintenance and inspection, change over or repair, starting or stopping, special jobs, trouble shooting and incipient problems (rather than normal routine operations), appear with startling frequency in thorough investigations. From the preventive view, this suggests that the Hazard Analysis Process consider non-routine operations and specify needed controls. Failure to see or heed signs of impending trouble, and failure to pause or stop for diagnosis/correction are frequent. Thus HAP should give careful thought to signals and appropriate action.

The use of conditional probabilities (a measurement technique finding value in medicine) has been suggested by Edwards (NSC Symposium, 1970) as a method of hazard analysis for lengthy sequences.

Since this study has focussed on organizations which have suppressed accidents to extremely low levels, the possibility that simpler failures have been most affected must be considered. In organizations with higher incidence rates, simpler failures (and simple preventive measures) may be more common. This possibility can be assessed against the following logic:

1. Simple failures most affected (?)

Even simple failures have some sequences.

2. Complex failures least affected?

a. Minor consequences -- costs may limit investigation/correction.

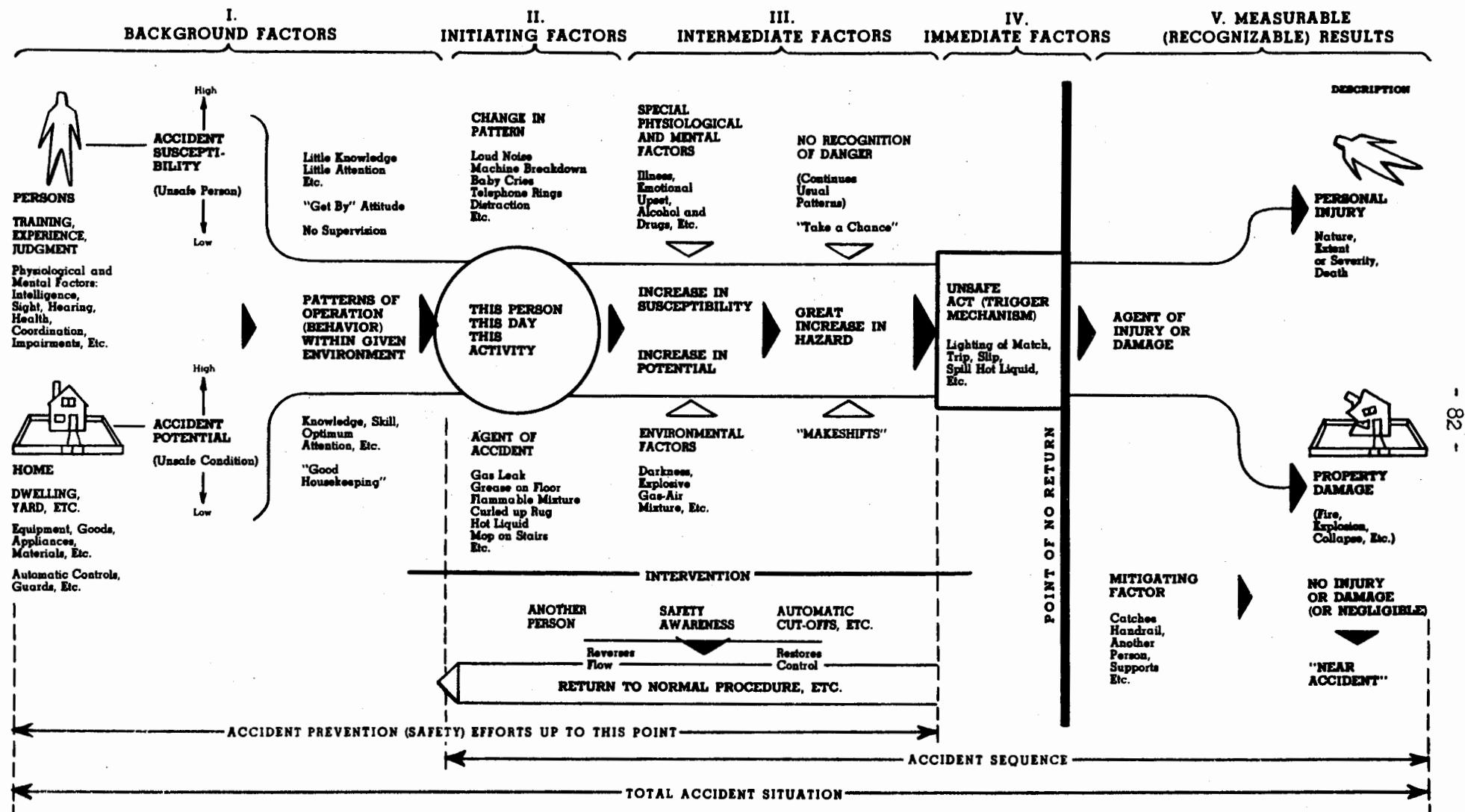
b. Major consequences -- searching study and redundant preventive measures warranted.

One of the most useful attempts to show the multi-factorial background of an accident was the "Dynamics of Home Accidents" developed by NSC's Home Safety Conference in the mid-50's. (Figure 6-3.) Unfortunately, no parallel occupational diagram has been developed. However, the model would be appropriate for a self-employed person, except that it fails to recognize the role of purpose, goal and performance, which should be stressed in all models of safety systems. The typical industrial situation also emphasizes managerial planning and supervisory control and intervention.

Examination of occupational accident case histories suggests that the accident's antecedents often develop in a number of sequences involving physical, procedural and personal elements. Because the occupational setting is more highly structured and controlled, we can look for the sequences of

Figure 6-3.

The Dynamics of Home Accidents



events which affected or changed the separate elements:

Management
Planning and design
Work environment (including arrangement and signals)
Machine (including tools, and equipment and signals)
Material
Supervision
Task procedure
Worker
Fellow worker (or other third party)

Frequently we find that a number of sequences were developing over a period of time before the culminating interaction. Events in retrospect were on a "collision course."

Thus if we superimpose the home accident model on the above factors, we begin to have a truer picture of the complexity. We have seen cases where the personal background factors of the designer and planner, the supervisor, and his supervisor all contributed. For example, commenting on a serious incident generated in part by an anomaly in hardware, i.e., a failure to match up, the division manager said, "The plan was written by my worst project engineer and the job was being done on the graveyard shift by my worst maintenance foreman with my weakest building supervisor. Four other persons were involved, and three of them made mistakes."

Having spoken of lengthy sequences, a word of caution may be in order. In either analysis or prevention we are wise to order our thinking in terms of "closeness" to the point of accident. That is, we begin with the accident and work back. Although background situations, if improved, may affect hosts of accidents, there are grave dangers in working on "problems in general." Particularly in trying to deal with the exasperating human factor, we must begin with behavior, rather than beginning with the often vague antecedent concepts of attitude, responsibility, education, or motivation.

An NTSB representative has said:

"Our basic criterion for determining cause-effect relationships of a practical nature vis-a-vis 'problems in general' is to identify them with real-world remedial action. Safety-wise, it becomes useless to cite broad conclusions, and you often do not realize this until you try to write constructive recommendations."

This page intentionally blank

7. THE ROLE OF RISK MANAGEMENT

Risk is an inescapable factor in any human activity.

The management of risk (either for an organization, an individual, or the public at large) should be assessed quantitatively insofar as knowledge permits. There is nothing wrong with the notion of "calculated risk," except the common finding that it wasn't really calculated! Efforts to calculate risk seem to have a beneficial result in added effort to improve planning, design and controls--in short, less risk.

Statements that there should be "zero risk," i.e., no accidents, seem laudable and inspiring on the surface. They may work harm indirectly by warping understanding of risk, hazard review and risk reduction techniques (as well as causing cover up). Evaluation of risk is almost impossible if "zero accidents" (or "zero defects") is the announced goal.

* * *

Risk taking behavior has had a modest amount of study, but this has been largely on individual or small group behavior and in abstract, laboratory situations. This has meant, vis-a-vis real life work, simplification and isolation of variables, weak incentives, use of students rather than managers, supervisors and craftsmen, and lack of the rich information, analytic and social context of occupational safety decisions. Experiments allow little room to change the situation (e.g., by hazard removal). Risk research choices are usually presented as simple Yes-No alternatives. Both the number of choices and the lack of modified or combination strategies is likely to be artificial.

Further, as in most behavioral sciences, there is substantial difference of opinions and findings.

The occupational risk taking situation is substantially more complex, but also more structured, more analytic and rational, more keyed to longer-term experience, and probably more easily improved. Consequently, it seems most practical to proceed in three steps:

1. Define the general format of the occupational risk taking situation.
2. Examine a selection of behavioral science findings for possible usefulness in:
 - a. Managerial risk assessment
 - b. Personal risk assessment (remembering that managers are people too!)
3. Then define the basic elements of suggested organizational risk assessment plans.

The Occupational Situation. The key elements of occupational risk assessment (as contrasted with personal or laboratory decisions) seem to be:

1. The nature of accident related factors is likely to be better understood--the roles of safeguarding, engineering, training, supervision, energy, error and change.
2. Information is, or can be, better in a number of aspects, fewer uncertainties:
 - a. risk identification,
 - b. risk analysis, including probabilities and consequences.
 - c. longer-term, broader experience, and reference to experience of others,
 - d. pilot tests where needed.
3. Decision methods can be better:
 - a. Criteria, including long-term and social or public concerns, can be more explicit.
 - b. Review is better.
 - c. Responsibility and accountability are more clearly defined.
4. The nature of the decision is usually different:
 - a. The situation and outcome are always modifiable by hazard removal.
 - b. The choice of alternatives will most frequently enhance safety, particularly if the alternatives are at least three:
 - (1) Continue unchanged (in some cases the safe alternative),
 - (2) Modify moderately (including single-failure fixes; fail-safe and cut-off points),
 - (3) Make major improvements (redesign, system study, redundant protection).

In some places, these key elements may be goals, rather than present practices! If so, the immediate work should be toward these goals.

It is not necessary to discuss each of the above elements in detail--the remainder of the text is largely in these areas. However, a few selected observations may help to visualize risk assessment in ways which will make the behavioral science findings more meaningful:

Much of system safety analysis is intended to reduce risk of failure, but it will also increase information on the objective probability of failure.

Management risk decisions should consider the number of accidents estimated as likely over the life cycle of an operation. For example, ten machines may be likely to produce four serious injuries over their life cycle if not better guarded. Or, a design goal, such as, injury probability per man hour of 1×10^{-4} , can be stated. Thus, it may be easier to convince management of an inexorable quality in future outcomes, given time. Objective probabilities from analysis will likely be given greater weight than in an unstructured personal situation. However, Carter (1972) reports some of the problems, as well as successes, in corporate attempts to use probabilistic methods in risk analysis.

An Air Force study (1968) was summarized as follows: "Arguments for an acceptable individual risk criterion, to be applied against any particular hazardous operation, are developed. A 'one-in-a-million' (0.000,001) fatality probability is selected as one which is consonant with those normal hazards experienced in routine, day to day living, the recommendation is made for Air Force adaptation of a 0.000,001 individual risk criterion for guidance in the application of safety programs."

Outside experts in risk evaluation (e.g., for fire risk or industrial hygiene) may be used, both for their competence and because they may have more precise notions of probabilities for long-term exposures.

Senior executives commonly have the skill of asking a series of questions to determine the amount and quality of analysis behind a proposal and thereby measure residual risk.

A declined risk by management may not be "inaction producing degradation;" the project may be sent back for more risk reduction. However, supercaution always has the potential for degrading task performance. "A man sits as many risks as he runs." (Thoreau.)

Risk Taking Behavior.

General risk research, essentially non-industrial, shows scholarly views in two groups represented by reviews entitled:

1. "Emerging Technologies for Making Decisions"--Edwards, Lindeman and Phillips (1965).

Models (usually mathematical) represent decisions in terms of expected probabilities and values, both rational and subjective.

Edward's models seem relevant to the type of hazard and risk analysis methods seen as necessary in this text.

2. "Risk Taking as a Function of the Situation, the Person, and the Group"--Kogan and Wallach (1967).

Decisions show differences in various situations and individuals, not explainable by the models of the first group. Most of us have seen considerable differences in risk attitudes among individuals, groups, and organizations.

Since both schools of thought seem to offer usable ideas for safety, perhaps we need not choose sides in the argument.

Ward Edwards was a member of the group at the NSC Symposium whose results are included as Appendix M. The group's views are consistent with Edwards'--indeed he contributed major points, particularly the sections, "Diagnosis" and "Effectiveness of Program."

Kogan and Wallach report findings which should be helpful.

Situational influences include:

1. When skill (rather than chance) affects outcome, riskier alternatives are selected.
2. More information is sought when consequences are severe, and less when information is consistent or costly. Seeking moderate, rather than maximum, information, a realistic choice, is indicated. (Individual

differences in information seeking are more heavily determined by personal traits, dispositions toward risk or conservatism.)

3. Deterrent values of costs of failure exceed values of success in decisions.

Personal variables include:

1. Consistent differences of individual inclination toward high, moderate and low risk alternatives.
2. No provable male-female differences across the life span, but a tendency toward conservatism with aging.
3. Higher social status seems to produce conservatism in decisions, but more participation in risk-involved decisions.
4. Highly motivated achievers indicate preferences for calculated, moderate risks.
5. Beliefs that individuals control their environment foster riskier choices.
6. Intelligence understandably affects correctness of decisions, but shows no stable connection with risk tendencies.
7. Maximal motivational disturbance seems associated with greater consistency of choice, risky or conservative, and less adaptation to environment or failure. Minimal motivational disturbance was related to rationality of choices and adaptability to environment, rather than consistent risk postures. (Note these are extreme fractions of a general population.)

Group influences on risk-taking may be of two types with rather subtle distinction:

1. The correctness (freedom from error) of a decision, e.g., from greater informational or interdisciplinary attributes, or judiciousness.
2. The risk-taking aspect, and particularly the group's influence on shift toward conservatism or risk.

The first aspect, not truly risk-taking, seems primary in the common use of groups in organizations, and also tends to initiate acceptance of decisions. Certainly in safety a review agency not inclusive of relevant disciplines will result in oversight or error--that is, poor analysis.

For the risk-taking aspect, there is some simple evidence for averaging toward a central risk value, and for conservatism. However, these may only operate against extreme individual positions and against extreme risks. Kogan and Wallach report the "risky shift phenomenon."

"The effect of group discussion to a consensus on the dilemmas-of-choice procedure is to increase the level of risk that persons are disposed to take."

A "risky shift" phenomenon is not necessarily bad--undue conservatism may be equally dangerous. Thus, the net effect of group influences could be construed to give greater wisdom, fewer extremes, and a selective disposition toward risk (progress?).

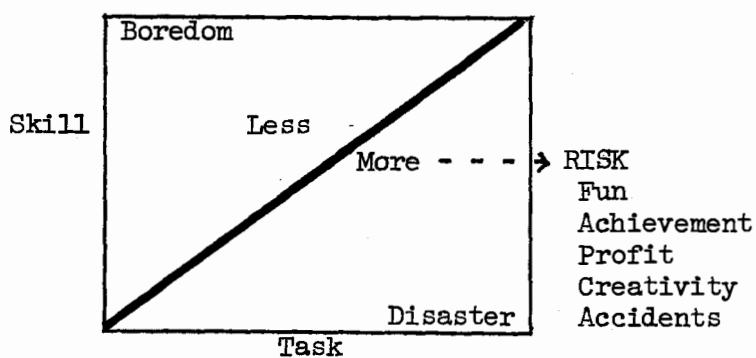
Since this text places considerable emphasis on groups and participation, it seems worthwhile to suggest the influences which are likely to work to produce greater safety, for example, in a Job Safety Analysis task involving senior craftsmen:

1. Safety becomes a focal goal.
2. Skill and knowledge of participants become socially important.
3. Information on risks is augmented.
4. Analysis reveals causal factors, contingencies and control techniques.
5. Modification of the situation--hardware, procedure, arrangement, or personnel--is feasible.
6. Acceptance of higher standards is fostered by peer development.
7. Performance (other than safety) may be sought, perhaps unconsciously. If so, a "risky shift" with compensating safeguards or controls may enhance safety and performance.

There remain some anomalies between risky personal behavior and expressed demands for safety which are frequently noted, and affect public and industrial relations. Risk acceptance is substantially higher for activities under our control than for activities not under our control, according to Starr (1969). This suggests the possibility that the employer-employee relationship can temper unduly risky tendencies of both employer and employee.

There also remains an ambivalent quality in risk, difficult to define, but impossible to ignore. That is, achievement, growing skill and pride, invention and innovation, and fun and creativity--perhaps "progress" however defined--often lie on the "no" or risky side. If risk were as simple as matching capabilities with requirements, we would have a Yes-No decision. But high capabilities with low requirements = boredom, just as low capabilities with high requirements = disaster. Consider skiing as an example in a pictogram reflecting levels of skill and task challenge!

Figure 7-1. Risk in General



Organizational Risk Assessment Plans

Risk evaluation provisions of NASA's manual (1970) express basic management and analytic responsibilities:

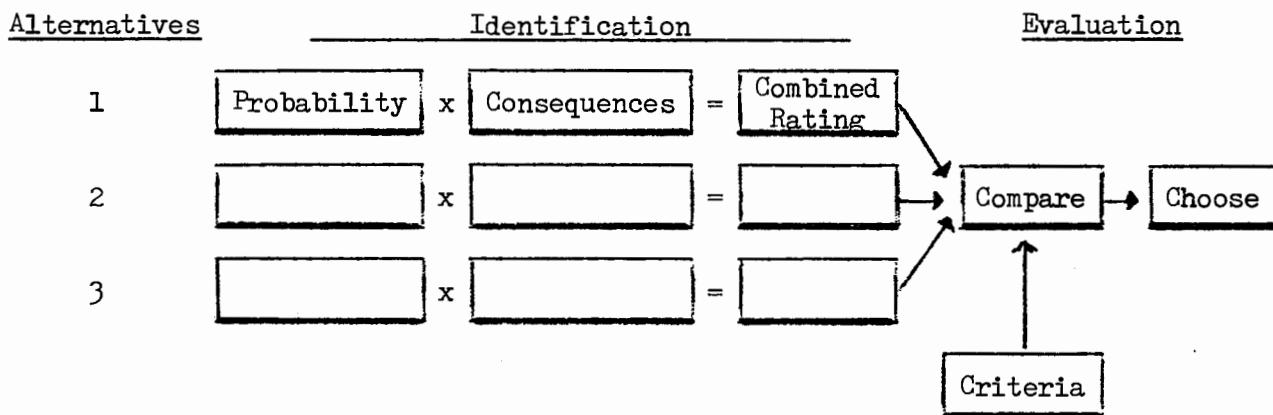
"The program manager ... must assume certain risks that are attendant to the design, manufacture, test, and operation of the hardware system to effectively accomplish the mission for which the system was developed. The acceptance of these risks should be based on thorough visibility as to the nature of hazards and risks that are in existence and the options and alternatives to the acceptance of the risks.

"The decision on whether to assume a risk is clearly a program management responsibility. This decision is no better than the quality of the risk data that serves as a basis for the decision. Accordingly, the development of hazard and risk data should be assigned as a responsibility to professionals whose training and orientation cause them to search out and find the hazards in the system before these hazards manifest themselves ..." in terms of injury, damage or destruction.

The basic elements of sound risk assessment are:

1. A choice of alternatives,
2. Identification of hazards, and the probability and consequences of accidents,
3. Comparison of the likely outcomes against criteria.

Figure 7-2. Basic Elements of Risk Assessment



Criteria or values include not only the organization's safety goals, but also cost, schedule, reliability and quality and other internal criteria, plus employee and public concerns and constraints.

Progress has been made in risk quantification for systems safety, and it is believed that quantified risk reduction goals can increasingly be used as criteria in designs and plans.

A Risk Assessment System and a Framework for Analysis of Risks are described in Chapter 21 as a major aspect of management's implementation of safety.

Residual Risks.

Residual risks can be classified as follows:

- I. Assumed risks--specific, named events, analyzed, and where possible, calculated, and accepted by management after evaluation.
- II. Other
 - A. Unevaluated--hazard known, not analyzed.
 - B. Unrecognized--hazard not known to management.
 - 1. Known and accepted at lower levels.
 - 2. Not known.
 - C. Uncertainties--omissions of major facets of the Hazard Analysis Process, such as information search, human factors review, test and qualification, or Job Safety Analysis.

In MORT analysis, the three "other" groups are treated as oversights, omissions and errors. Data collection is needed, but events thus far examined indicate:

Unevaluated and unrecognized hazards, and uncertainties in the analytic-decision process are frequent and conspicuous in serious events--more so than assumed risks.

This page intentionally blank

III. HOW TO REDUCE HAZARDS

The major elements of the best occupational safety practice and system safety are briefly described and compared to show how they may be integrated with mutual improvement. (Details are combined into the MORT system of analysis and evaluation.)

The new approaches are:

1. Separately usable parts of a complex system,
2. Simple, when separated,
3. Cheap, if scaled to the size of a problem.

III

The new approaches give greater emphasis to:

1. Method, rather than content,
2. Visibility for the analytic process, rather than just conclusions.

Most important, in this Part we develop a model of a safety system congruous with a goal-oriented high performance system, and show the new model to also be congruous with a variety of general management methods.

The concepts in Parts II and III lead to a statement of general safety program theses.

This page intentionally blank

8. INTEGRATING SYSTEM SAFETY WITH PRESENT BEST PRACTICES

A clearly articulated concept and method for reducing hazards is essential in knowing what to look for in accident investigation or in evaluating safety programs. Very high level ideals for hazard reduction procedures help measure program performance in good organizations and help establish future program goals -- for example, is new plant construction preceded by thorough life cycle analysis in early, conceptual stages?

We could categorize three concepts of high-level hazard reduction processes:

Level IV - the best occupational practice (far above I, Sub-minimal; and II, Regulations; or III, Voluntary Standards).

Level V - A "practical" combination of two concepts, IV and VI, above and below.

Level VI - the best of nuclear and aerospace system safety practice, a so-called "gold-plated" effort.

Five significant characteristics of the highest degree of safety effort (nuclear or aerospace) seem to be:

1. Modern analytic methods, beginning at conceptual stages.
2. Directed research programs to fill information gaps.
3. Substantial investment in hardware (priority over software).
4. Considerable investment in software (personnel selection, training, simulation).
5. Monitoring (observation, feedback).

These programs were expensive, government-funded, and the objective was "First Time Safe."

However, only a change in amount, or degree, or cost (based on what we are willing to invest according to economic and social criteria) would be necessary to apply these effective techniques to any activity.

The type or kind of safety work should not change, simply the amount.

In system design we see the operation of two aspects of safety:

1. Standards - for example, for daily exposure to radiation, controls, redundancy, limitation of effects of severe accidents.
2. Non-standard design and planning - to control other contingencies.

Also, we see the role of these two aspects:

1. Minimum allowable performance,
2. Maximum desired performance.

In steel and other industries, as an example of best business practice, we see a high degree of control at the work site:

Job Safety Analysis
Job Instruction Training
Safety Observation Plan.

Also, somewhat apart, but first in their hierarchy: a strong program of engineering and environment control. These are strong and praiseworthy, but even their cost might be felt to be "uneconomic" by other companies.

Having praised the leading industry programs, we can proceed to find out where even they fall short. The difference from system approaches may be in some measure degree or quantity. There is something more, however, all along the line. There is also a qualitative difference in sophistication, scope, innovation, and most certainly in the scientific or research orientation.

System safety, on the other hand, suffers from the discontinuities of project orientation and, when seen as costly, may be eliminated rather than using the on-going industrial approach.

A synthesis seems to be an ultimate requirement if we are to adequately examine accidents and performance against a unified standard of comparison, rather than two yardsticks. But before attempting in MORT analysis what is seemingly the first synthesis, it is probably well to at least roughly compare the two levels of practice, and thereby establish some outline for integrating the two. The notations are obviously cryptic, rather than fully descriptive.

	<u>Present Best Practice</u>	<u>System Safety</u>
<u>General Orientation</u>	Continuous Operational System given	Project or mission Pre-operational System designed
<u>Who?</u>		
Management Role	"Vigorous" Policy and administration well established	Not different Contractual requirements Budget allocations for analysis
Supervision	Accountable Trained	Not different
Special staff (non-safety)	Safety responsibility - sometimes unclear, or none	Accountable for quality of analysis for delegated functions
Safety staff	Consultant	Same Information responsibility and specific analytic duties well defined
	Much "program administra- tive detail"	Probably less

<u>How?</u>	<u>Present Best Practice</u>	<u>System Safety</u>
Process design	Standards emphasized	Analysis emphasized (Standards inadequate)
Research	Neglected	Emphasized to answer questions
Data Collection and Analysis	Stereotyped, simplistic, and not very useful	Emphasized to answer questions
Review	Before plans are used	At inception, at prescribed review points, and at change.
Design Scope	Not clear Much reliance on "retrofit"	Life cycle emphasis Inputs assume "fit" - criteria established.
Techniques	Primarily "content" e.g., manuals	Primarily "methods" System Safety Analysis Human Factors Engineering
Procedures	General rules promulgated JSA, often designed on job, after work begins	Prepared in Design and Development stages, more emphasis on early preparation
Selection	Medical exams and some selection	Strongly oriented to requirements and human factors
Training	JIT	Methods and aids created in Development stage
Motivation	Meetings, committees, propaganda, human relations emphasized Participation usually sought	More personal, professional
Discipline	Where necessary	Probably no different
Maintenance	Preventive	Maintainability designed
Monitoring	Inspections Safety observation plans	Methods and schedules developed in design More emphasis on monitoring

Occupational practice tends to be operational for a system as given, and may therefore be only expedient. System safety is pre-operational for the life cycle of a system to be created.

Jerry Lederer, NASA safety director, has called the old approaches "tombstone safety." (NASA, 1971.)

Mackenzie (1968) has said that:

"Stripped to the naked bones, system safety is oriented to 'hardware systems' while industrial safety is more in the direction of a people-directed activity."

Miller (NASA, 1971) used the military standard definition of system safety as:

"The optimum degree of hazard elimination and/or control within the constraints of operational effectiveness, time and cost, attained through the specific application of management, scientific and engineering principles throughout all phases of a system life cycle."

This brief comparison does not do justice to either process, but will be qualified and expanded in the details of MORT.

The early text also included the following brief summary of the synthesis:
In both the best occupational safety practice and the best system safety practice, the Who? of hazard reduction is identical:

1. Management is vigorous in pursuit of safety through managerial excellence, because of humane and economic concern, and because hazard reduction is congruous with reliable control of work and performance.
 2. Line supervision is accountable for performance with safety, is trained and motivated, and assisted as necessary.
 3. Staff. A specialized safety staff serves as consultant, advisor, expeditor, designer of hazard reduction programs, and monitor and evaluator of the effectiveness of the programs.
Other staff units have assigned safety functions consistent with their objectives.
 4. Employees are trained and motivated.

System safety is project oriented, whereas the typical occupational program is properly continuous. The sequential order of hazard reduction steps in occupational practice and systems practice are not so different that they cannot be integrated, if hazard reduction is viewed as a Hazard Analysis Process or cycle triggered by planned changes or deviations. This concept facilitates the progressive adoption of the superior system safety analytic techniques in change projects which upgrade the effectiveness of present business practice.

A primary focus of this study has been how to apply project-oriented, system safety techniques to on-going work, such as business or AEC. There are indications that aerospace, the originator of system safety techniques, may also need to examine how its agencies can utilize the "best practices" of business and AEC to handle its on-going, non-project activities.

Elements of an Ideal Hazard Reduction Program

with concern for human factors through:

- D. Full use of Human Factors Engineering
- E. Procedures - including anticipation of changes and emergencies, as in Job Safety Analysis
- F. Personnel selection
- G. Personnel training, for example, Job Instruction Training
- H. Motivation
 - 1. "Innovation Diffusion" processes to produce wanted changes
 - 2. Participation, group and social influences to build acceptance and morale.
 - 3. Human relations programs to help the individual
 - 4. Communications to support the program.

5. Residual Risks - estimated at three points in the Sequence:

- A. After Hardware (A-D)
- B. After Procedures (E)
- C. At the end of the Sequence

Re-cycle Sequence if Risk is unacceptable.

6. Monitoring

- A. Supervision, inspection, sampling, measurement, appraisal
- B. To detect Deviations: Changes, Errors, Incidents, Accidents
- C. Thus providing Hazard Analysis Triggers to reactivate the whole reduction cycle.

The Life Cycle phases of concern in any system are:

- 1. Conception
- 2. Definition, Requirements
- 3. Design, Development (including procedures, training plans)
- 4. Construction, or Manufacture, and Installation
- 5. Operation
- 6. Maintenance
- 7. Disposal

← Safety starts here,

← continues to here.

Hardware -- technical factors represented by adequate engineering have historically and correctly been the preferred solutions. Although investment-benefit calculations could raise questions about this strategy, the physical and technical factors can be dealt with in greater certainty than the less stable and less understood human factors. Further, a visibly good record on hardware improvement is felt to be a precondition for motivating the people in the system. Thus, hardware has precedence in the reduction sequence.

Brief History of System Safety.

The U. S. Air Force pioneered many concepts and techniques of system safety analysis. One landmark was the work done on the Minuteman inter-continental ballistic missile. The probability of an inadvertent launch of a missile was a very small number. But when you multiplied the small probability per day by twenty years and a thousand missiles you got a probability of an entirely dif-

ferent magnitude -- an unsatisfactory magnitude for the "life cycle of the system."

Bell Telephone Laboratories developed in 1962, and Boeing then applied, the "Fault Tree" analysis technique, which measures probabilities of various undesired events, and thus tells where preventive measures would yield the greatest additional safety.

Two important principles were involved - first, calculate or estimate failure probabilities, and second, do this for the "life cycle" of the operation.

At the same time systems in weaponry were becoming too complex and expensive to permit continuing the older reliance on test and retroactive improvement. Analytic detection of failure potentials in advance became a necessity.

The man-in-space program has employed many system safety techniques from its inception. A high degree of protection for astronauts (and others) was attained.

The Apollo V fire which took the lives of three astronauts showed that all human efforts are fallible and led to, not only a reexamination and improvement of the particular situation involved, but also brought about a reorganization and strengthening of the space agency's safety organization for manned space flight programs.

Apollo XIII also showed fallibility, but also in a positive manner, dramatically showed the emergency values in redundancy, procedures, training and decision mechanisms.

The nuclear and manned space flight programs involve an essentially new idea: First Time Safe. The missions are simply not ones which can be accomplished on the "old fashioned" premise that things are "pretty good" or "very good," and we'll investigate the ashes of our failures (a Fly-Fix-Fly routine). The job is simply impossible if done by conventional methods.

AEC has employed systematic analysis of the "maximum credible catastrophe" to assay the design of atomic reactors, and emphasizes a control principle of independent review. Also, the AEC program for control of routine radiation hazards exemplifies not only design and procedures, but also the important principle of monitoring.

Today system safety requirements in military procurement are spelled out in detail. Increasingly, companies with aerospace experience are applying the techniques to non-military projects; however, transfer is far from automatic unless the purchasers specify that system safety is a requirement.

Systems safety analysis has not only improved our technological capacities, but also has begun to raise public expectations as to what is possible in product, transportation and occupational safety. Therefore, any corporate future

holds both the threat and the promise that system safety procedures must be applied (see, for example, Hayes 1971).

System safety analysis is as much a logical process as a mathematical process. Therefore, there can be no excuse for failure to begin using the concepts, even though the research necessary for exact numbers and the time and professional talent available for the analysis may both be inadequate.

Currie (1968) has provided a useful general discussion of system safety, a more detailed history of its evolution, and an extensive bibliography.

The term "system safety" as used in the aerospace industries was an aspect of system engineering, which was usually a separable project or contract approach, and system safety was sometimes a separate contract. This gives rise to some semantic problems, in that system safety, as thus applied, is an early, finite phase in a project, rather than the on-going management effort characteristic of occupational safety. A system safety effort, despite its considerable virtues, was seemingly somewhat set apart from the ultimate on-going operations.

Safety professionals have had difficulty in seeing how and where they could use system safety techniques. Further, the contract organizational form seemed to divorce system safety from the ultimate operational activities, even though the system safety tasks included operational requirements.

Further complicating understanding of system safety by safety professionals was the substantial expense and new, sometimes complex, analytic techniques developed by system safety. Neither of these is a requirement for using a systems approach, but the difference between the simple logic of the effort, and the quantity of the effort was not clear.

We use the terms "system safety" and "system safety analysis" to refer specifically to the kinds of developments which took place in the aerospace industries (and in reactor development, but not by the same name). We use the term "safety system" to describe the kind of on-going development which now appears needed in occupational safety. This has several important implications for safety systems:

1. Improved safety systems assimilate past programs (if they are effective).
2. Improved safety systems can be built by successive additions of practical, effective system elements (rather than leaping full-blown from a large expense appropriation and a finite contract format),
3. Improved safety systems can be built from ideas which are no more than moderately difficult or complex. (System safety analytic techniques, e.g., the fault tree, are covered in texts even now being published.)
4. Congruity with on-going management methods can be shown.

Adopting New Methods.

Whether viewed as system safety or the MORT system, the apparent complex new methods stimulates "instant objections" as to imagined difficulty or cost. Therefore a number of suggestions are in order.

Separability. Evaluate and try the methods one at a time. They are usable separately. At Aerojet two safety professionals began using a total of five concepts after just a one-hour familiarization briefing on MORT.

An overall safety program could probably not be reorganized or upgraded to MORT standards in one fell swoop. Rather, a program can be gradually strengthened over time.

Simplicity? The MORT process is an attempt to define a safety system in as much detail as possible. Big hazards or big accidents deserve big review.

However, if the simple essentials of any method are to be used in scaled down form, these essentials must be visible. In addition, the basic hazard review logic in big and little matters should not vary, only the amount of study, and amount spent on hazard reduction.

The positive logic tree developed by some chemists after a gold powder explosion in 1966 (Figure 9-1) is a good illustration. There is a great deal more we can say about "hazards evaluation," or review of changes, and independent review. Nevertheless, the diagram is a good portrait of a basic process for self-analysis by chemists.

Initially we can focus on building a fuller understanding of the safety process at management and supervisor levels, and among scientific and technical staffs. As we progress we can, hopefully, make the process simple and usable at craft, operator and other employee levels, both to pre-plan for safety and to know when help is needed.

Costs? With some frequency, the concepts of system safety have been rejected as expensive and justifiable only when "gold plating" is warranted. This is unjustified. Ideas and logic are not expensive. If quantity of effort is scaled to size of problem, and method of logic retained, cost is manageable and flexible.

The biggest cost is in the mental effort and initiative of trying new techniques.

In the long run, the cost of any safety program, whether conventional or system safety, is small compared to total investment and small compared to the cost of one big accident. Further, system methods will enhance the whole management process and can pay big dividends in general performance.

9. METHOD vs. CONTENT

An examination of occupational safety literature reveals that description of methods of analyzing risks, or reviewing for hazards, or investigating accidents is sparse. The bulk of the material describes specific, topical treatment of particular hazards, and takes the form of standards or recommendations for given situations--this we shall call content.

System safety, on the other hand, stresses analytic methods and processes.

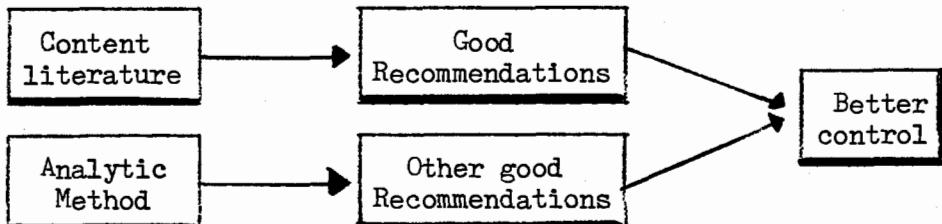
A more balanced emphasis on method vs. content offers a redundant examination of hazard:

1. The specific technology of a hazard's control can be reviewed,
2. The process of analysis can be reviewed.

This kind of redundant examination is an articulated and well-developed facet of the independent review system for nuclear weapons, and is also evolving in the nuclear criticality review system at the National Reactor Testing Station.

The ideal of duality in method vs. content is carried over into the staff organization of the nuclear weapons safety group which has two small, highly competent staffs for the two aspects, namely, analysts and weapons experts.

Since method is valuable precisely because it produces specific recommendations for situations, some perhaps not found in content, it is worth examining the two processes:



The redundancy of using both method and content (or technology) reviews is believed to be a major avenue to attainment of higher safety goals.

When a project comes before a review panel, the designer can be asked, "Did you perform the analysis?" If the answer is, "No," the review meeting is over!

Some of the distinctions are:

Method

Information Processing
Process of Analysis
Research
System
Search

Content

Technology
Standards and Codes
Recommendations
Components and specifics
Finite

Sometimes the distinction seems to be:

Theory

Sometimes this
works
very well,

Practice

And this
does not work
well enough.

An exploration of this view of analytic method with supervisors of chemical laboratories, for example, elicited instant understanding; that is, they saw the potentials for improved control if they could, not only monitor a chemist's technical plans, but also have agreed upon criteria for evaluating the chemist's self-review process (Figure 9-1). The methodology outlined in this "Positive Tree" is a shortened hazard analysis process.

"Brains" are an ingredient in a successful organization, but not as an alternative to method. Method is a means of enhancing the brain-power the organization possesses, hopefully a large supply. Accidents in "brainy" organizations not having visible safety method, for example in some R & D organizations, argue against reliance on brains alone.

A great amount of useful methodology is seemingly already in existence in a large complex organization, but is obscured by subject matter. A conscious search-out is required to bring the experience and wisdom to light. Sometimes it needs better articulation, but then it is available to add to a synthesis of good practice.

Method, when identified, is not infrequently the seemingly intuitive practice of good managers or good engineers. For example, an R & QA audit of Aerojet's Engineering Division found that a variety of sound methods were being used by the staff even though not specified in divisional procedures. The weakness in the intuitive, unspecified approach is, of course, its variability over time and among people.

Method is also an efficient guide to what information to seek. Needed information is very often readily available if the proper question is pinpointed.

Safety professionals typically put more emphasis on rules and procedures, and less on analytic method, than do managers and scientists. Thus a facet of professional growth in safety probably lies in greater use of method--analytic or managerial.

Once a review or analysis method is articulated as a standard practice, two key questions are fair, and often revealing:

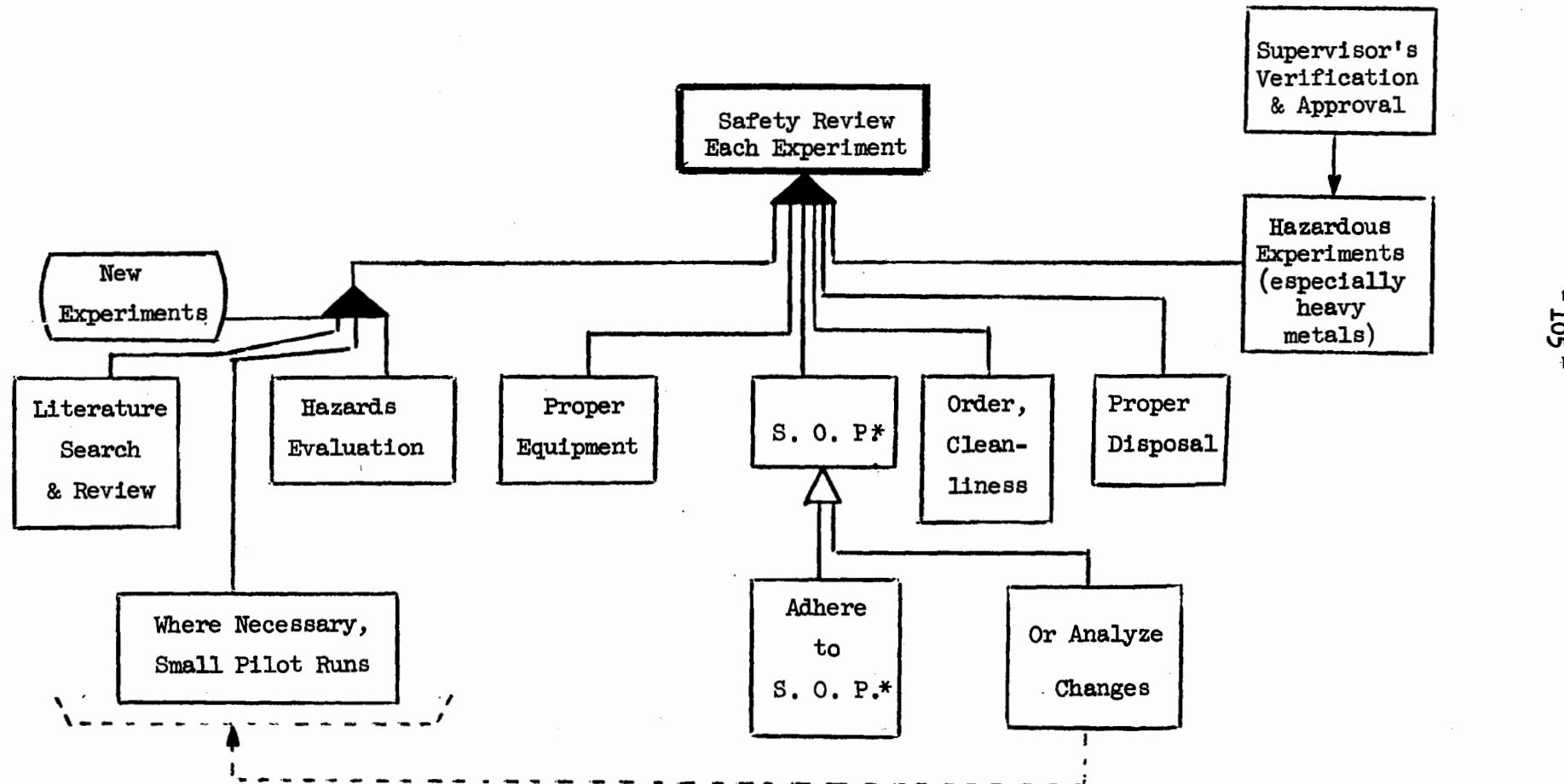
WHERE ARE YOU IN THE PROCESS?

WHERE SHOULD YOU BE ?

Figure 9-1.

POSITIVE TREE

Recommendations after
Gold Powder Explosion, 1966



* Safe Operating Procedure

These questions are featured on wall charts prepared for the Aerojet trials--
posters for safety engineers!

From asking these questions, a dictum evolved:

FOLLOW THE PROCESS

Following an analytic process has great efficiency and flexibility. If you know where you are in a process, you can take off on excursions and side trips:

Seek special information,
Use opportunities to leap ahead,
Try a solution,
Go back and verify an early step,
Or, even try another method.

When you have finished the excursion you can always return to the process, and know where you are.

10. SAFETY, EFFICIENCY AND PERFORMANCE ARE CONGRUOUS

As early as 1922, a study (American Engineering Council, 1928) showed that rising productivity was accompanied by decreasing accident rates, and vice versa. However, there is no way of knowing whether this was cause-and effect, or arose from common causes.

More recently studies have associated low accident rates with such performance criteria as profitability or low scrap and rework costs, labor and shop costs, etc., but the validity of the studies has been in doubt.

A past president of the American Society of Safety Engineers, John V. Grimaldi, has given considerable study to the role of management in safety. A paper which drew in part on British experience is particularly helpful (1965). This includes the view:

"There is good evidence that a close relationship exists between management effectiveness and safety performance. We find that when management operates its enterprise with taut controls, the measurable elements that contribute to business success may be noticeably improved."

However, Rockwell (1959) reported that high productivity was associated with high unsafe act ratios in one study of a small number of workers.

Notwithstanding some proof, belief in the congruity of safety and efficiency rests primarily on inferences from management views, from consideration of what hazard review reveals about other, non-safety causes of disruption, or malfunction, or error, and from personal experiences and case histories. The author's convictions go back to wartime experiences on the atomic bomb project, for which it was reported:

"The project's directors were aware of the close relationship between safety and efficiency, and there are many project stories graphically illustrating the fact that a job safely done is more quickly and certainly done." (Johnson, 1945.)

Successful business managers, in policy and personal statements, have said, "Safety and efficient operation are one and the same thing."

Logical relations between errors and accidents, as well as planning and performance, support the idea that safety and performance are two facets of the same management process.

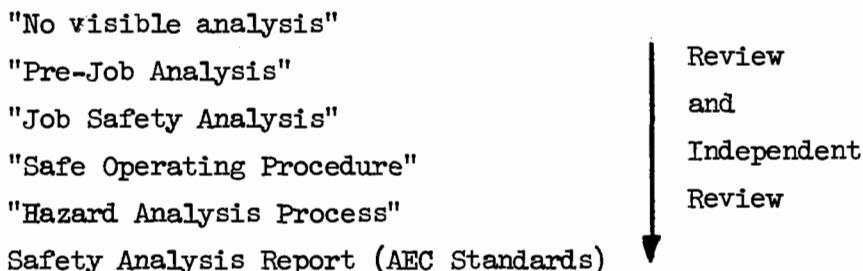
The hypothesis that accidents are congruent with errors, and safety with good management, may be key to further progress in two ways: (1)shaping development of safety procedures and methods, and (2) justifying additional

safety investments at the design and development phase of the system. Safety programs in the best organizations may be approaching a point of diminishing returns, unless the proof or conviction of collateral performance benefits is usable.

The overall role of larger energies in building higher performance indicates that control is needed to attain performance. If parallel progressions are shown:



then an equivalent progression of amount of safety controls can be shown:



Thus, the quantity and quality of analysis and safety control increases proportionate to the energy control and management needed for high performance. (See Figure 10-1).

Three cases analyzed in this study are interesting:

B1P1 A safety coordinator's review of a proposed experiment produced the suggestion that an alternate, easier-to-control source of radiation be used. This made possible the more rapid, trouble-free completion of the research.

A piece of experimental equipment yielded invalid test results for a long period because of an error-provocative design which finally produced a serious accident.

Experimental equipment destroyed by electricity showed, in the opinion of the investigating board, a likelihood that the research data which might have been produced would have been invalid for reasons related to the accident.

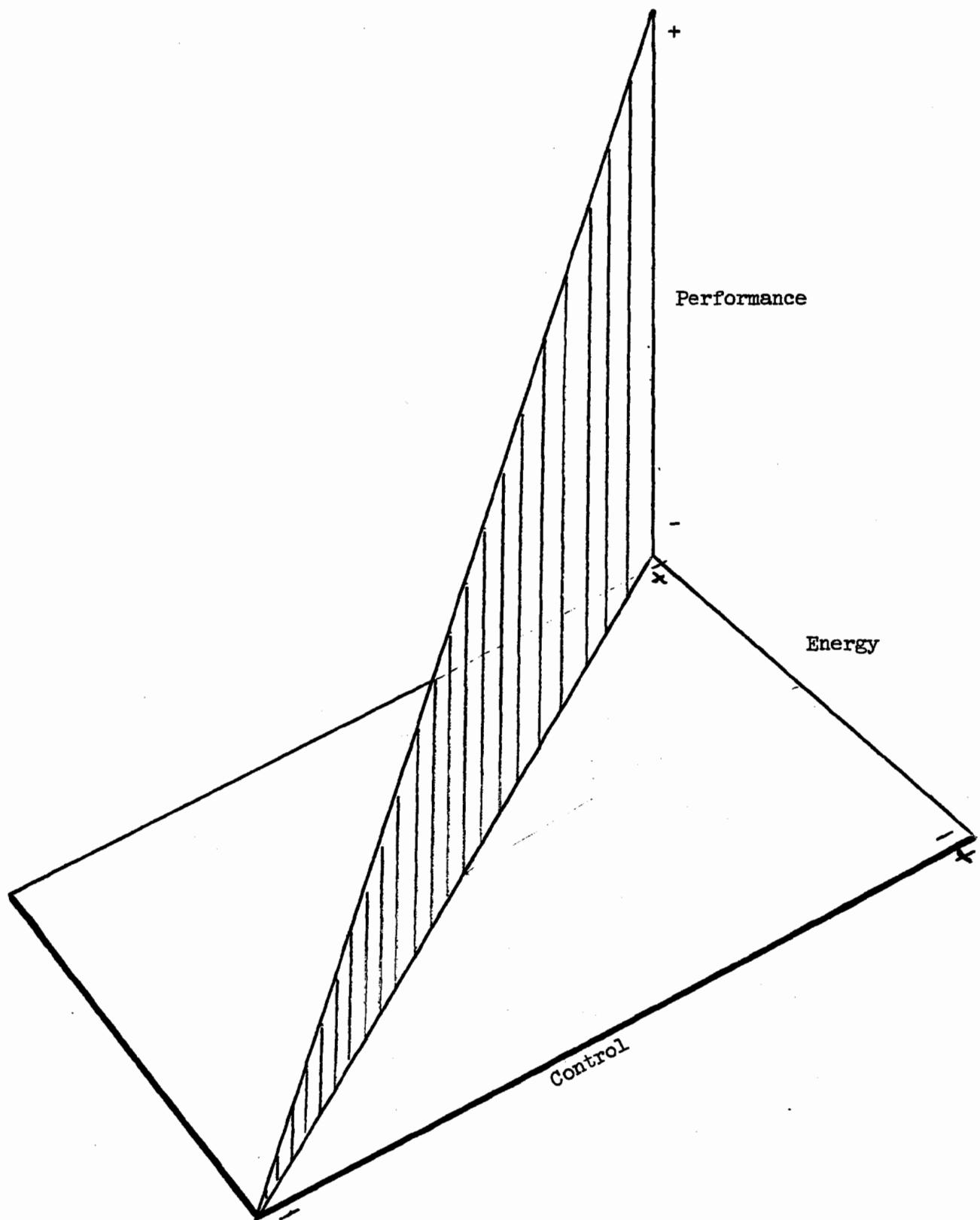
Special efforts should be made to compile extensive files of such cases to counteract the negative views of safety all too common in scientific circles, and sometimes in managerial circles.

The Right Way.

Injury and damage accidents can be viewed as special classes in the larger family of mistakes.

Some years ago a staff group within NSC undertook to define the steps in an accident prevention methodology in a document which was ultimately captioned

Figure 10-1. Performance Depends on Controlled Energy



"The Right Way is the Safe Way." (Johnson, 1962).

As the staff document emerged, General George Stewart, who was then serving as Executive Vice President of NSC, said, "That's it! That is precisely how we completed a winter exercise involving transportation of 20,000 military personnel to the Arctic and safely returned them at the end of maneuvers without killing anybody."

The steps in The Right Way can be quickly enumerated (more detail is available in the reference or from the National Safety Council):

1. Define your objective - state what you want to do.
2. Identify hazards - for example, read the instructions!
3. Prepare a sound plan - what can happen will happen!
4. Fix responsibilities - who is in charge of planning, inspections, training, supervision?
5. Seek good facilities - plants, roads, parks, etc.
6. Use proper equipment - easy to use safely and minimizing injury potential.
7. Build knowledge and skill - use training!
8. Supervise performance - firmly, skillfully, create adequate checks.
9. Learn from experience - study accident causes.
10. Evaluate progress - results count.

This methodology is not simply an accident prevention methodology. It is a systematic approach to accomplishing anything! It should not then surprise you that accident prevention can be a very revealing measure of people.

(A duPont president, Lammott Copeland, said a speech to this point was the "first adult speech on safety" he'd heard!)

One plant manager (also duPont) has said that accident prevention is his sharpest and keenest tool in developing an organization which can attain the corporate objective and that, aside from humanitarian or cost considerations directly associated with accidents, it is impossible to conceive of an efficient plant which is operated unsafely.

"Safety in Action," the National Safety Council's basic policy statement (1949) sums the matter very nicely:

The Council's Creed

Safety is positive. It is doing things the right way.
It is interest in the welfare of others.

It is a contribution to good living, to good government and respect for law and order, to efficient production, and to the well-being of every individual.

11. A SAFETY SYSTEM AS A GENERAL MANAGEMENT SYSTEM

During the Aerojet trials, there have been several major conceptual developments:

1. A basic model of a "Safety System Congruous with a High Performance System" was substantially improved.
2. The basic model of the safety system was developed to show congruity with typical general management methods.
3. The general management methods of Juran (1964) and Kepner-Tregoe (1965) were shown to be very helpful, not only in accident investigation and monitoring, but also in various other phases of the safety process, such as hazard analysis or implementation.
4. Certain incidents at Aerojet were as much escapes from management control as safety engineering problems.
5. It seemed that clearer, articulated concepts of tested management methods, and more frequent common use of such methods, might have beneficial results in the organization as a whole, as well as for safety.

Thus, the model for the general safety system and its supporting models of general management practices seem to hold great promise for upgrading safety work in a manner congruous with general management, and the prior lack of such models seems fundamental to insight and understanding of safety and other problems. The relations of the safety organization to the remainder of the organization could be much improved by common understanding and use of good management methods.

The early stages of this study included a modest search for models of productive processes to which safety models might be affixed. The search was largely unsuccessful - there are seemingly few such models. An exception was Thurston's "Concept of a Production System" (1963), a three-dimensional model of a flow process; however, this promising model did not appear as a general model of a safety process - iterative cycles based on feedback were absent. It is to be hoped that a search for general models of production systems will be continued and that safety can be shown as an aspect of such a system models.

The approach which evolved was primarily based on aerospace system and safety concepts, modified so as to be relatable to an on-going organization, rather than, or in addition to, a specific project.

System Concepts.

"A system is an orderly arrangement of components which are interrelated and which act and interact to perform some task or function in a particular environment." (Recht, 1965.)

Systems have purpose - they are mission, task or performance oriented. But there are always constraints of budget, schedule, performance, and legal and social pressures or values.

Systems are kept in a dynamic state of equilibrium by means of feedback

loops of information and control - devices as old as the earth, but re-invented by man for modern technological purposes. Methods of managerial control of enterprises are predicated on design and use of feedback loops for all essential aspects of the organization. (Juran, 1964) Thus, systems are tied together with communications networks.

Safety is, then, a management subsystem in an organization and can be visualized and described as (1) a hazard analysis process, (2) with feedback loops in organization operations to provide management with information on hazard reduction, and (3) feedback loops to inform management as to deviations from performance goals.

(If a reader has difficulty using system ideas, he may wish to review Appendix B, "A Few Useful System Concepts" before proceeding.)

Accidents occur when systems deviate from plans. Failures, errors, and degradations in performance are similar unwanted deviations. When a part of a system is altered or fails, the system changes, and may then produce an accident.

Why are we interested in systems notions about occupational safety? Because, if safety is a subsystem in a larger system, it behooves us to understand the larger system, and to construct a safety subsystem which is at least consistent, hopefully is congruous* and mutually reinforcing, and ideally, helps the larger system accomplish its goals.

A good safety process holds great potential for helping an organization reduce all manner of errors, malfunctions, deviations and failures. If this potential is to be seen, and used to support the safety process, that process must be visibly presented as a program congruous with management for high performance.

Safety professionals commonly complain that management or supervision or employees are not "sold on safety." This may reveal more about safety professionals and their program ideas than it does about the others! Top managers, on the other hand, complain that safety professionals do not understand organizational goals, and typically are not promotable upward in the organization.

If a safety professional operates without useful concepts of how his safety system correlates with a larger system, his effectiveness is greatly inhibited, his many opportunities for developing his management skills may be largely wasted, his diagnostic skills may not be used to solve general problems,

* Congruous: "being in agreement, harmony or correspondence; suitable, appropriate." (Webster)

and his ultimate promotability has been found to be impaired.

Further, there are ample reasons for believing that systems approaches hold many answers to the problems of improving safety programs and the relations between safety and the other functions in an organization.

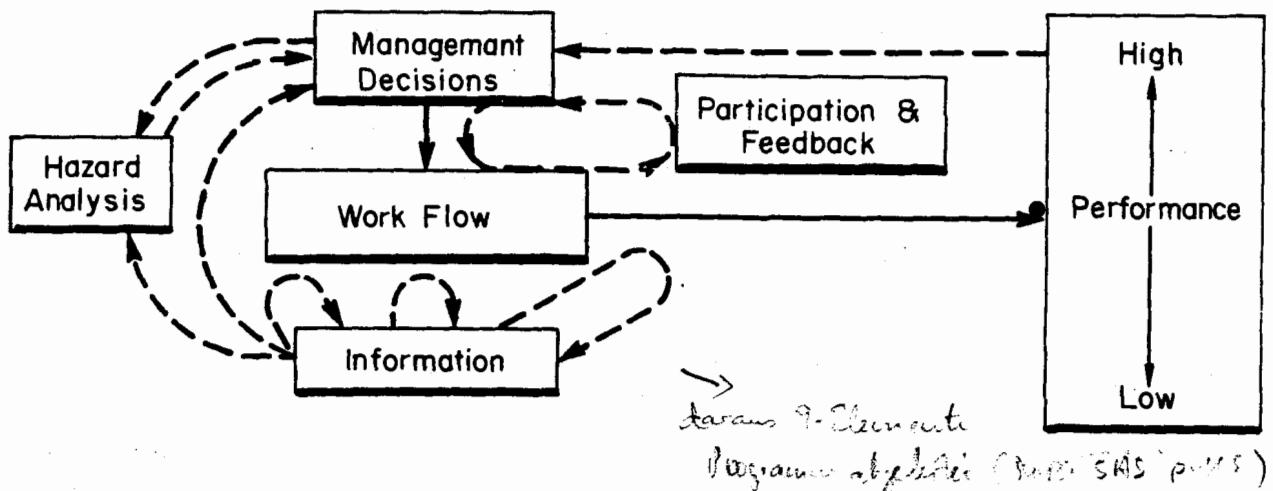
A Safety System as a Management System.

At its simplest level, a safety system (perhaps Safety Management System is a better term) can be shown to have but six elements:

Figure 11-1.

SAFETY SYSTEM

Congruous with Goal-Oriented, High- Performance System



Such a simplification has possible advantages in summarizing all the complex detail of MORT, as well as emphasizing safety support for management goals. (Note that the above items are the titles of Parts in this MORT text, and therefore the model shows how the parts interrelate.)

The general schematic (Figure 11-2) presents in more detail the major elements in this same safety system congruous with a goal-oriented, high performance system:

A MANAGEMENT DECISION PROCESS

Utilizes: Objectives, Requirements, Resources, and Constraints
to establish: Goals
and develop: Policies, Organization, Plans, and Implementation
a repertory of: Management Methods
requires: Evaluation of Planned Changes

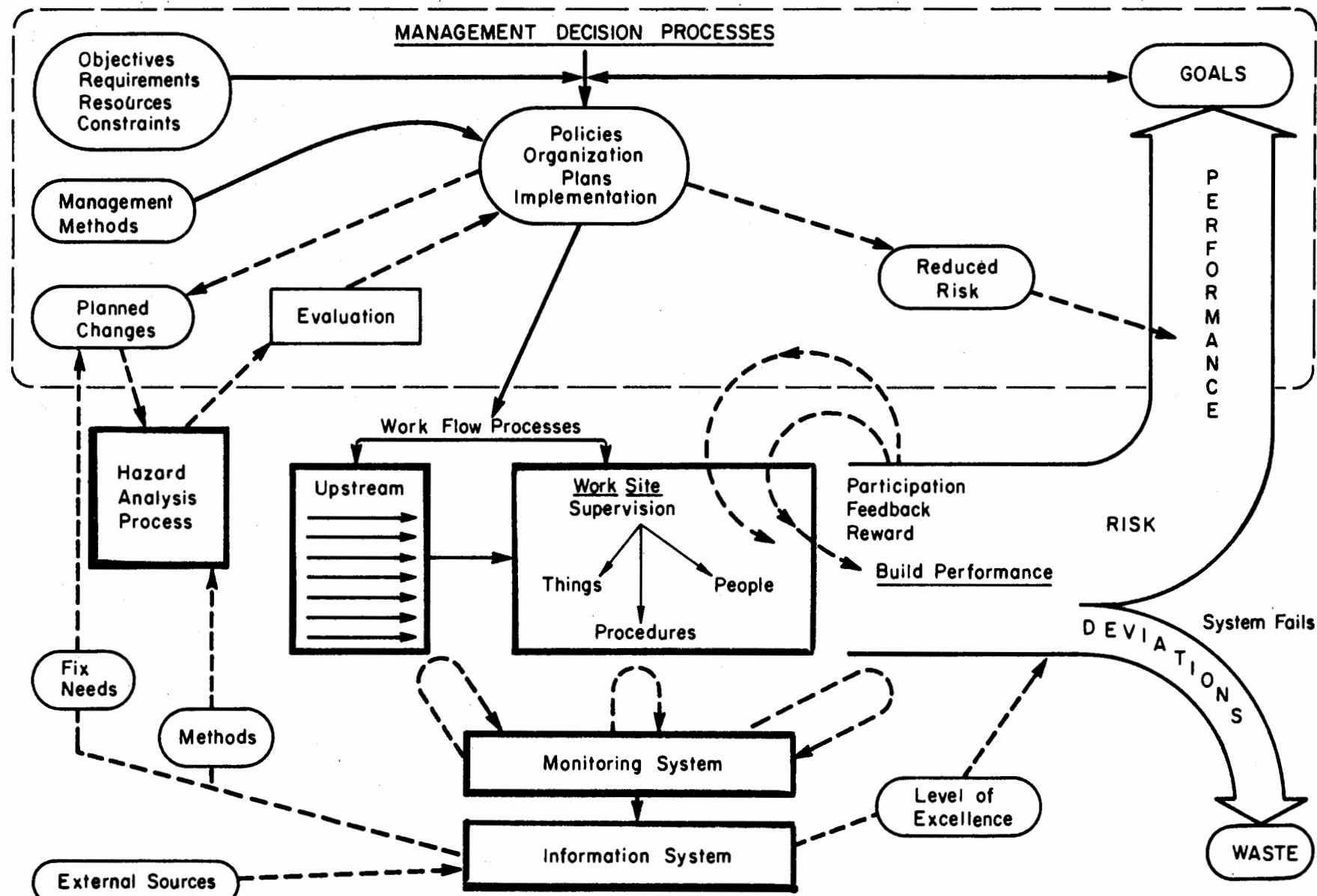
WORK FLOW PROCESSES (many)

Utilize: Supervision, Things, People and Procedures
Derived from "Upstream Processes" (e.g., design, construction, training)

Figure 11-2

DYNAMIC SAFETY SYSTEM

Congruous with Goal+ Oriented, High Performance System



PERFORMANCE is the output, but with Risk.

Deviations (accidents, errors, malfunctions) degrade performance, produce Waste,
because the System Fails.

Goals are used to measure Performance.

On this basic work system, we superimpose the subsystem components which we need for safety and for general performance:

Monitoring detects deviations from plans;

The Information component has three principal outputs:

measure Goal Attainment (level of excellence)
indicate Fix Needs (which become Planned Changes)
indicate Methods for fixes.

Planned Changes

are put through a Hazard Analysis Process.

Results receive Evaluation,
and revised Plans are Implemented.

The ultimate results should be Reduced Risk.

Participation, Feedback, Rewards (and Penalties?)

are necessary to Build Performance.

The safety subsystem is thus a dynamic feedback - control - modification sequence, and an iterative process which can improve, improve, improve!

Naturally, the model is less complex than real-life activities. For example, there are many fix cycles not shown: the employee receives a signal and corrects a deviation, the supervisor does this hour by hour continuously, and the "upstream processes" are continuously observing their output (we hope) and making adjustments and improvements.

A practical application of the Safety System schematic to recent overhead crane safety activities at Aerojet is represented by Exhibit 1.

The exhibit shows how some real-life activities at Aerojet follow a pattern similar to the model schematic.

A general safety system operates through iterative cycles to produce higher and higher degrees of safety. The past system operations are projected into a likely need for a high-level, national study and follow-up to secure the performance characteristics desired - for example, overhead cranes have acute need for highly skilled, professional human factors review.

Management Methods are the latest added ingredient in the schematic, Figure 11-2. It is the purpose of a subsequent discussion in this chapter to show that typical good management methods are also iterative cycles useful in safety analysis and planning, as well as in general management.

Examples of the operation of the "dynamic safety system" may be helpful.

In another illustration (Figure 11-3):

(1) A critical incident study* was made, one of the many monitoring plans.

The analyst then processed the information in three ways (numbers keyed to Figure below)

(2) He grouped related cases which, from his experience, might cumulate in more serious sequences and forwarded them to management as indicated needs for fixes or Planned Changes.

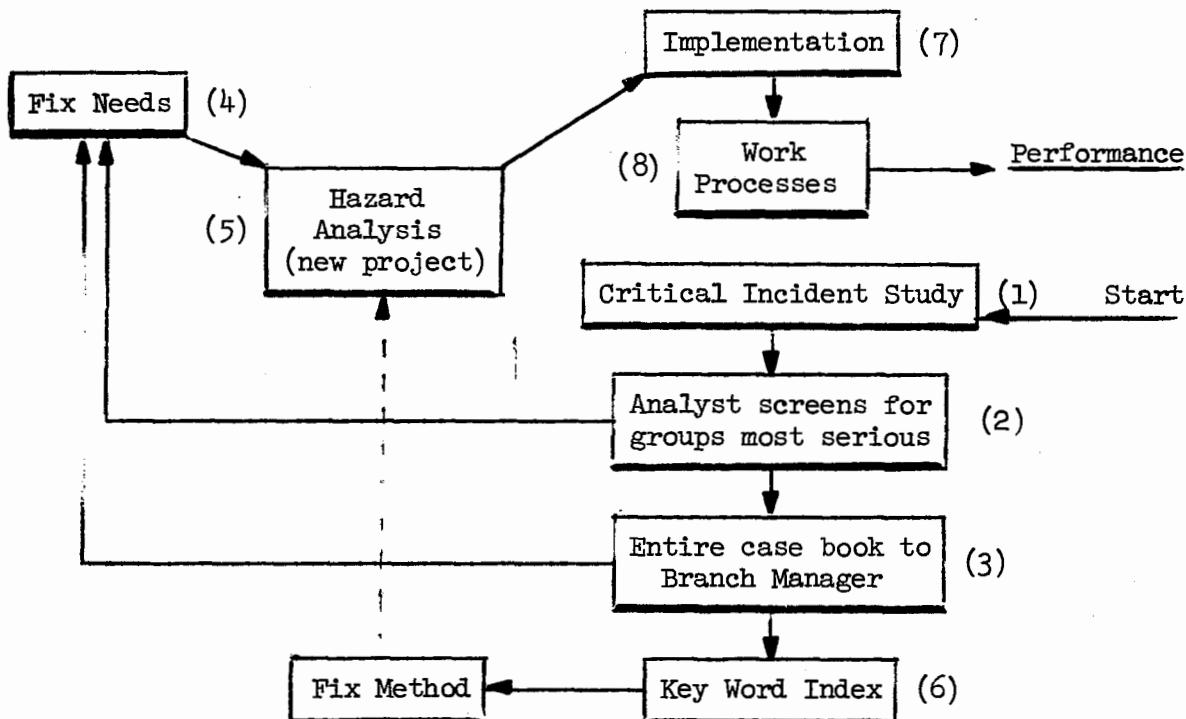
(3) He reproduced all cases in bound books for branch management review.

(6) He made a key word index so, for example, a project engineer could call out the things and features of a new project and find out what previous troubles suggested fix methods.

Fix needs (4) go through Hazard Analysis (5) with information search (6).

Results are evaluated and implemented (7) in the work process (8).

Figure 11-3. Operation of the Safety System for a Study



Similar handling is in effect for all formal and informal incident reporting plans.

A Repertory of General Management Methods.

Good management methods are ways of attaining goals and, as such, can be used at all levels of an organization, and in personal as well as organization

* called RSO, for "Recorded Significant Observation" at Aerojet because in reactor terminology they are neither "critical" nor "incidents." They are just what the name implies, observations collected for formal study.

activities. Greater proficiency in managing human affairs is sorely needed in our society, and a proper collateral objective of the safety system can be to increase skills in attaining goals.

A repertory of tested management practices, rather than a simplistic approach, seems best calculated to meet the complex and varied needs of safety, judging from experience before and during this study. The safety professional can use good management methods to improve his skills and work, and his management can help him to grow.

At the same time, and because accidents are a harsh and certain test of management systems, a safety system effort may help management people to grow. A recent serious accident was an escape from management controls, as well as an engineering fiasco. (See Figure 5-1)

From among the rather vast array of management protocols and dicta available for possible use, six were chosen for (1) their apparent relevance to the safety problem, and/or (2) present use by Aerojet. These six, by their nature embrace several other theories or practices. Also, these six seem to be adequate for a more detailed exposition of management methods, criteria and analysis in the MORT approach to cause analysis.

The six general management approaches, with brief reasons for selection, are:

For reasons of excellence and apparent usefulness for safety:

1. Juran

- a. Control to existing standards,
- b. Breakthrough to new higher standards,
- c. His disposition of traditional or conventional approaches.

2. Kepner-Tregoe

- a. Problem Analysis Worksheet as:

- (1) Accident investigation tool
- (2) Potential problem analysis tool
- b. Action Sequence related to problems; this because it well represents what a hazard analysis process ought to be. If read in an accident context, it sounds like the outline of a Safety Analysis Report!

3. Error Reduction (Improving Human Performance):

- a. Concepts described in MORT
- b. Concepts used by Sandia, and presumably reflecting AEC policy in the weapons area (e.g., Swain, 1972).
- c. Setting the stage for several useful concepts including:
 - (1) Correcting error-provocative situations
 - (2) Management errors mirror higher management service deficiencies.

For reasons of local use:

4. Aerojet's Management by Objectives Program

The reference literature supplied supervisors comprehends Drucker's Management by Objectives (1964); however, there are changes, semantic and other, which may differ from Drucker. Also, the Aerojet literature supplied includes;

5. G. E.'s Approach (incorporated in Aerojet's material under the title, "The Professional Manager at Aerojet Nuclear Company.")

6. A "Traditional Approach" - delegate, hold accountable, and reward or penalize. This approach includes the very useful concept that "the mark of a good manager is fast action at the trouble spots."

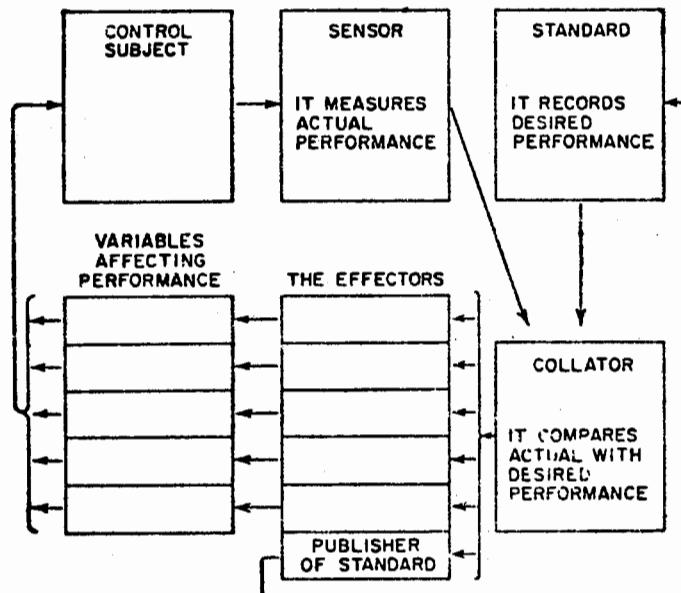
It is probably not as important which particular set of management concepts is articulated and used, as that some good set be clearly and explicitly chosen and used. Only if some reasonably firm platform of doctrine is well known in an organization does it seem possible: (1) to hold personnel to any standard of analysis, or (2) to judge the value of any standard of judgment and practice.

The purpose of the following material is not at all a full exposition (for this see the relevant texts). Rather, what is intended is a platform from which to launch a study and subsequent use of a selection of management methods particularly relevant to safety.

1. Juran

a. Juran's control cycle is succinctly pictured in this figure:

Figure 11- . Juran's Feedback for Control of Anything



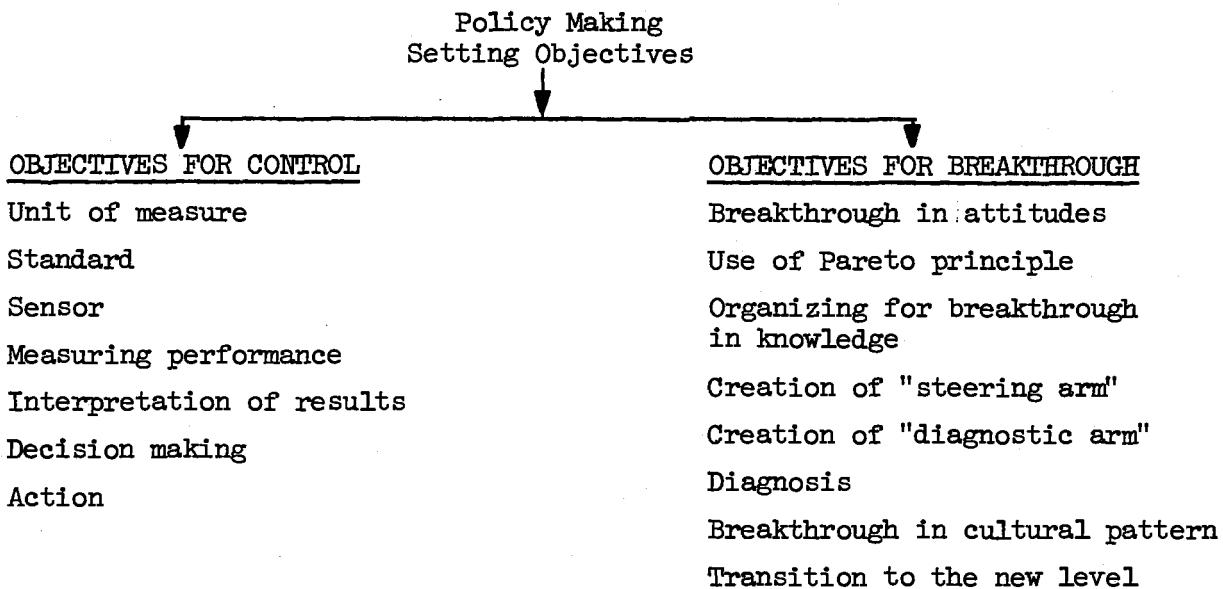
(Reproduced by permission)

This simple schematic on control, a function considered important in every organization, is largely unknown to the personnel (except R & QA), nor do personnel articulate a useful substitute concept. It has been difficult to understand how people can effectively cooperate and communicate on a day-to-day basis and on a basic subject without a common frame of reference. It may be that some aspects of the cooperative relationship, as well as the underlying control imperfections, stem in part from vague, unarticulated concepts of the process of control.

Juran (1964) provides a wealth of experience in the design of each element in the control cycle.

- b. Juran goes on to articulate the differences between Control and Breakthrough to new, higher levels of performance:

Figure 11-5. Juran's Managerial Breakthrough



"The drastic differences exhibited by these two sequences make it evident that when we talk of a single sequence for managerial action, we are straining our classification beyond the elastic limit. To be sure, whether we are creating or preventing change, we must organize, select, train, motivate, etc. But the organization forms are drastically different. The motivations are drastically different. And so on. Such differences should be brought out in the open, rather than be obscured by a common label."

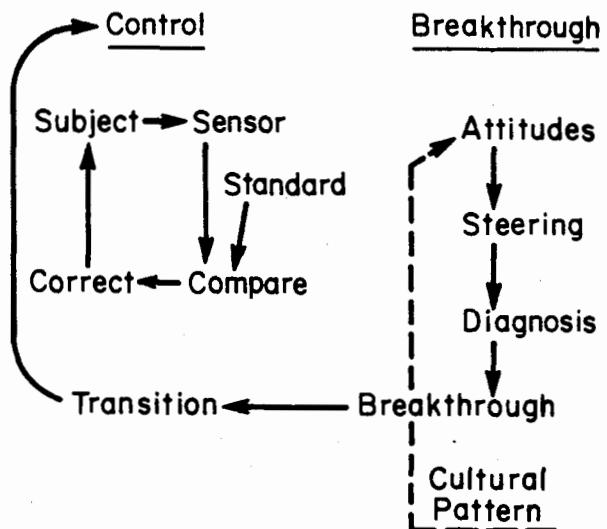
(Reproduced by permission)

We have endeavored to consciously utilize Juran's notions of "Breakthrough" in the MORT Trials at Aerojet, and they seem to work.

To inter-relate his two processes, we used the following figure:

Figure 11-6.

JURAN



In order to see the relation of the preceding figures to the Safety System (as postulated in Figures 11-1 and 11-2) it is merely necessary to visualize the MORT Hazard Analysis Process as an adjunct process at the following points:

1. Juran's Control cycle - in actions of Comparator and Effectors
2. Juran's Breakthrough cycle - in Diagnosis

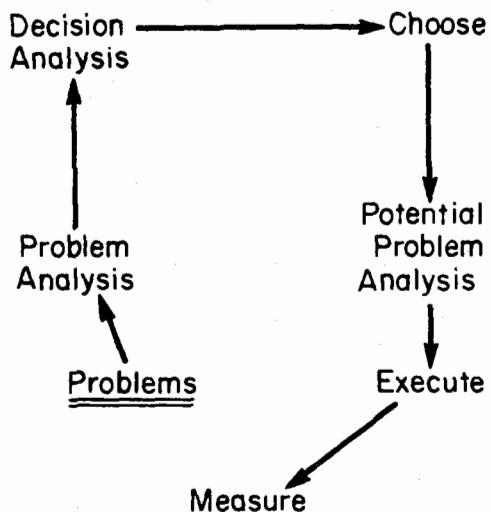
Juran's text contains useful materials on error reduction and training. Since he has an extremely complete base in general management experience and scientific study, his findings and observations are extremely helpful in relating important facets of the safety problem to common management beliefs and practices.

2. Kepner-Tregoe's "Rational Manager"

A managerial system useful for safety purposes has been developed by Kepner and Tregoe (1965). The system, originally developed by Rand Corporation for the Air Force, but now widely used in U. S. corporations, is particularly appropriate for a safety system in both language and logic - e.g., probable cause, minimum threat, problem probability and seriousness, preventive action, trigger contingent action.

The K-T Action Sequence (shown in detail in their text) can, as with Juran, also be seen as a simplified iterative cycle. Simplified, it can be superimposed on the basic safety system schematic (Figure 11-2) for comparison purposes.

Figure 11-7.
KEPNER - TREGOE



As with the Juran or other methods, the beauty of such a simple connection with the safety system is in ease of assimilation and growth. One picture of a safety process can be seen, first, in the simple functional flow of Figure 11-7; a second level of understanding can be gleaned from the Action Sequence and other elements of their book; a third level of proficiency can be attained by taking the K-T course (preferably the latter); and ultimate growth can come from use of the system, especially in an organization which also uses it widely for general management.

The safety professional, whose problems of professional growth are so widely discussed, would indeed be fortunate if his organization is one of those making intensive use of K-T methods. Many such organizations already have excellent safety programs, and the safety professional would have a golden opportunity to enlist his associates in an organizational effort to improve safety by more fully utilizing modern management methods. Opportunities for dialogue are always extremely valuable in assimilating new methods.

Examples of the relevance of K-T methods for accident analysis were given in Chapter 5, The Role of Change in Accidents.

Kepner-Tregoe particularly stress the quantified analysis of alternative solutions to problems. (Understandably they do not deal in specifics of probabilities and consequences of energy release, as must be done in safety.)

For broader problems or for value aspects of problems, their methods prove very useful. Consequently, an example is shown as Appendix C, using

the problem: How Can We Substantially Improve Excellent Safety Programs in the next Five Years?

* * *

In general, the Juran and Kepner-Tregoe techniques seem to have more value for safety than any other management packages.

Since both management approaches have been used extensively in the trials at Aerojet, as well as elsewhere, to gain insight into methods of improving safety, it may be fair to offer some comparative observations. The intent of the comparisons is to stress the point that a repertory of management methods is needed in safety.

Figure 11-8
Comparisons of Three Management Methods

<u>Aspect</u>	<u>Safety System</u>	<u>Juran</u>	<u>Kepner-Tregoe</u>
Direct relevance to safety	Primary Objective	Good, but Indirect	Excellent on Management methods
Emphasis on analysis	Primary, but covers numerous details	Good	Excellent on methods
Emphasis on control	Complexity requires complex monitoring	Primary (leading text)	Good
Emphasis on High Performance	Intended to be a <u>continuous process</u>	Special Breakthrough Goals	Selection of best alternatives
Emphasis on participation & acceptance	Strong	Good as to Breakthrough	Weak
Direct relevance to general management	Remains to be proven	Primary Broad base in management literature	Primary, a tight system

3. "Improving Human Performance"

MORT articulates many error-reduction concepts as evident in the literature, but perhaps imperfectly states or synthesizes the concepts. (See Index.)

Sandia's application of such concepts to the weapon safety program would seem to be the highest development of the "state of the art," and by their practice and existence seem to represent an AEC policy, but not presently stated as applicable to reactors and other work.

Error reduction concepts do an excellent job of stage-setting for further specification of the management criteria and analysis seemingly most useful for

greater safety achievement. Specifically, these are at least six:

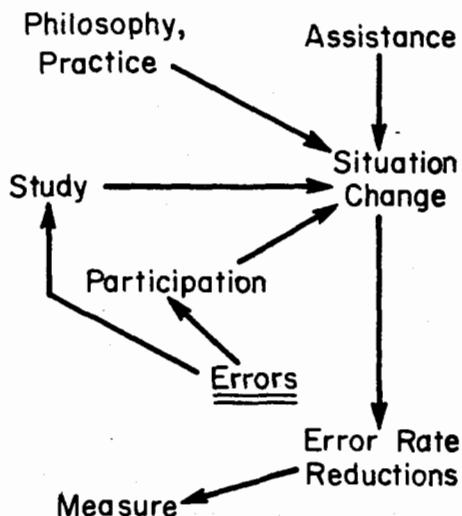
1. Errors are an inevitable (rate-measurable) concomitant of doing work or anything.
2. Situations may be error-provocative - changing the situation will likely do more than elocation or discipline.
3. Many error definitions are "forensic" (which is debatable, imprecise, and ineffective) rather than precise.
4. Errors at one level mirror service deficiencies at a higher level.
5. People mirror their bosses - if management problems are solved intuitively, or if chance is relied on for non-accident records, long-term success is unlikely.
6. Conventional methods of documenting organizational procedures (either AEC or Aerojet) seem to be somewhat error provocative.

In the earlier stages of the MORT Trials at Aerojet, a memorandum, "Acceptance of Proceduralized Systems," was created. The material is incorporated in this text.

The Aerojet management material (MBO) contains the McGregor's Theory X and Y assumptions about people - Traditional and Potential. But the relationship of these assumptions to personnel, acceptance and error reduction practices is far from clear, and the fact that the pendulum is apparently swinging toward a mid-point in general management practice is not noted.

Figure 11-9 .

IMPROVING HUMAN PERFORMANCE (Error Reduction)



[Based on Swain (AEC-Sandia) and others]

More recently a monograph by Alan Swain of the Sandia human reliability staff was received: "Improving Human Performance." (1972) This latter is a better statement of the case than MORT. Additional copies were obtained for study and possible policy revision in the AEC-Aerojet context.

What is suggested is that any organization review such literature, modify suggested precepts as may be warranted, and issue more useful guidelines as to the policies and practices which top management believes could improve human performance.

Such policy must, of course, be supported by at least minimal staff competencies in human factors work, preferably so utilized as to have organization-wide impact.

It is believed that such an action would likely have important effects on performance, and related aspects as well as:

1. A negative philosophy and practice: "Who is to blame?" and "What should the penalties be?" These tendencies have adverse effects on morale and performance, and inhibit study of the underlying causes of malfunctions.
2. A negative, unrewarding method - that is, a suspension or firing, usually results in picking another apple out of the same barrel. The hope for better results is probably forlorn, unless the situation is changed.
3. The sometimes poor cooperative relationship between various levels of an organization in attaining common goals.

The need to raise such questions arises out of the study of safety, and how safety may be improved, but the general management implications are difficult to sidestep.

Special aspects of improving human performance are discussed in Chapter 26, Human Factors Review; Chapter 32, Procedures; Chapter 35, Motivation; and elsewhere. The intention at this juncture is to emphasize the policy issue.

4. Professional Manager

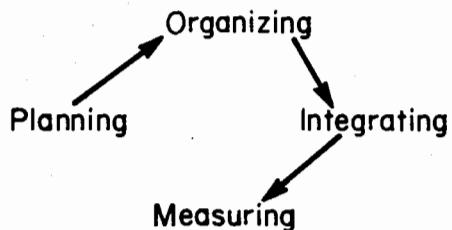
This process, widely used and highly successful in General Electric and other organizations, and used at Aerojet, can be succinctly shown in a simple schematic in Figure 11-10.

The method is described in nine pages of useful detail in Aerojet's "Managing by Objectives - Data for Supervisors and Foremen," August 13, 1971.

This method, while good and useful, is believed to be less explicit and useful for safety than the three foregoing methods.

Figure 11-10.

THE PROFESSIONAL MANAGER



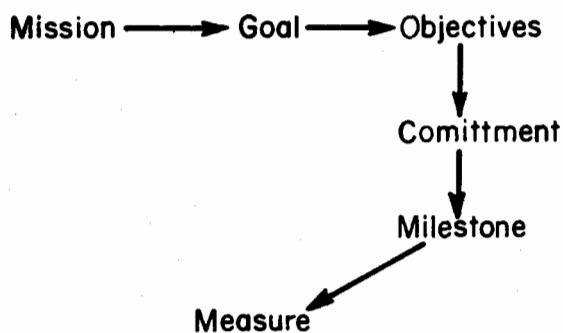
Tarrants (1972) discussed this approach. He presents a schematic, "An Industrial Accident Prevention Communications and Control System," which shows useful detail on constraints and pressures, but relates safety to direct financial loss rather than general performance.

5. Aerojet's "Management by Objectives"

The reference on MBO immediately above contains much useful material. The principal suggestion for increasing the usefulness of this program is to augment it with one or more of the fully-rounded, problem-solving and iterative processes previously described.

Figure 11-11.

MANAGEMENT BY OBJECTIVES



6. "Traditional Approaches"

These approaches, with incisive action by an aggressive manager, were used by earlier contractors at NRTS, and are often mentioned by long-service personnel who found that the aggressive, safety-minded manager did, in fact, take fast action at the trouble spots.

In general, the traditional delegation of responsibility, authority and resources is the main stem of AEC-contractor relationships, and should remain so. However, weaknesses, as well as strengths, should be recognized. A full repertory of management methods should offset such weaknesses as:

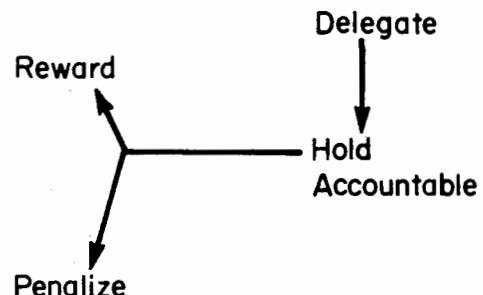
1. Little guidance, analysis and future correction, OR
2. Overly specific guidance on details, which in turn inhibits broad, fundamental corrective changes and initiative.
3. In a period of limited rewards (due to constraints), the penalty option of traditional approaches may be over-used and be unproductive.
4. There are unfortunate tendencies to "cover up" and "cover your number", neither of which does much for longer-term progress.

Two common traditional approaches are shown in the figure below:

Figure 11-12.

"TRADITIONAL"

Policy Making
Setting Objectives
Planning to Meet Objectives
Organizing to Execute the Plan
Selection and Training for
Manning the Organization
Motivation of the People
Appraising the Results



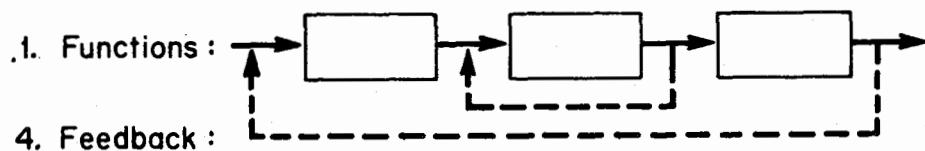
A finding of this study (discussed pages 193-95) that Aerojet's well-intended procedural documentation (and perhaps that of AEC) produces significant functional inadequacies must probably be considered in weighing the ways in which traditional approaches should be modified or augmented. There certainly is no basis for believing the traditional approaches could produce an order-of-magnitude improvement, either for safety or for other goals. The essence of an improved directive format is presented in Figure 11-13.

Relating Management Methods to the Safety System.

The elements of the various management approaches discussed can be portrayed as a generalized cyclic process, a performance cycle, comparable with the basic schematics of the safety system.

Initiation of an iterative cycle of improvement is portrayed in Figure 11-14. This figure has already shown itself to be a useful picture for professionals

Figure 11-13.
GOOD PROCEDURES



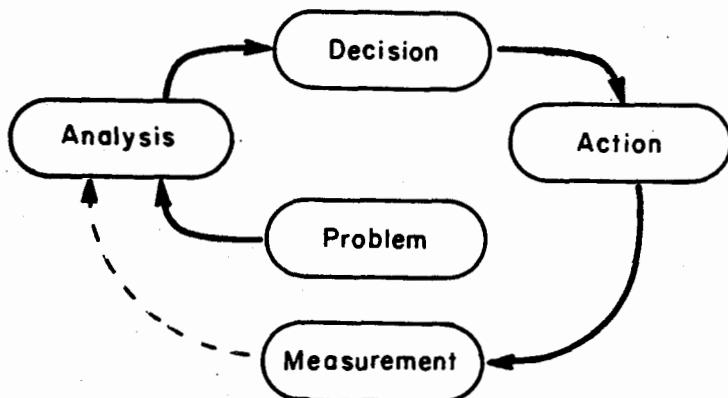
2. Steps to fulfill each Function

3. Criteria to Know When the Job is Well Done.

planning a safety program improvement.

Figure 11-14.
PERFORMANCE CYCLE

A REPERTORY OF MANAGEMENT METHODS USEFUL FOR SAFETY

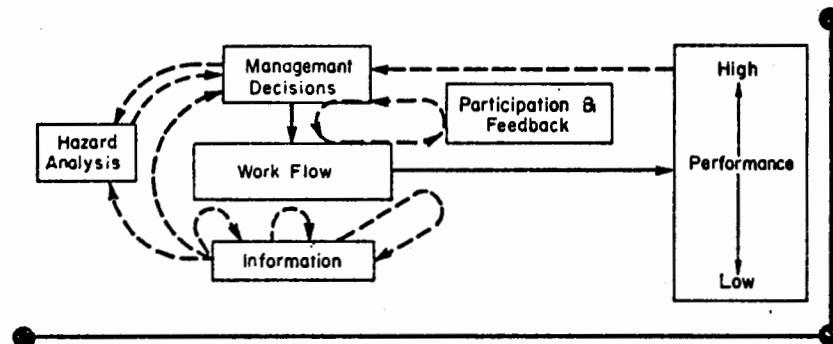


In order to show the congruence of the general management methods described and the general safety system, the models thereof have been condensed into Figure 11-15. The cyclic, iterative character of all the methods should be clear, as should their general correspondence. The elements in Figure 11-15 are used in wall charts at Aerojet, as reminders of the relevance of management methods in both problem solving and accident investigation.

A different approach to interrelating management and safety systems is suggested by Peterson (1972). He uses a "managerial grid" to diagnose and describe management styles, and counsels adjustment of the safety system to the existing management style. This may be wise as an adjustment, but does

Figure 11-16. A Repertory of MANAGEMENT METHODS relevant to the Safety System

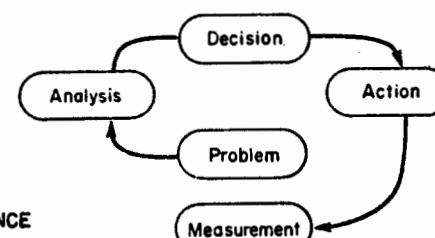
SAFETY SYSTEM --- Congruous with Goal-Oriented, High-Performance System



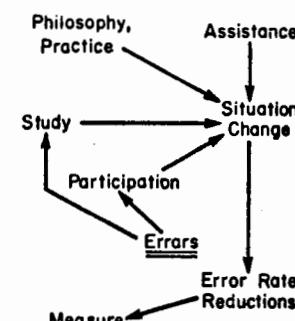
A Repertory of Management

Methods Useful in the Safety System

PERFORMANCE CYCLE



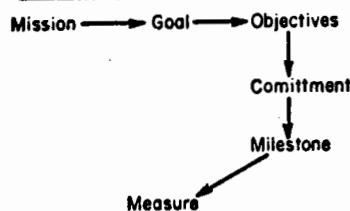
IMPROVING HUMAN PERFORMANCE (Error Reduction)



THE PROFESSIONAL MANAGER

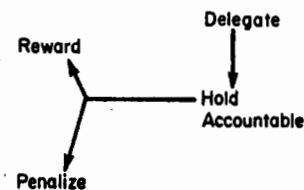


MANAGEMENT BY OBJECTIVES

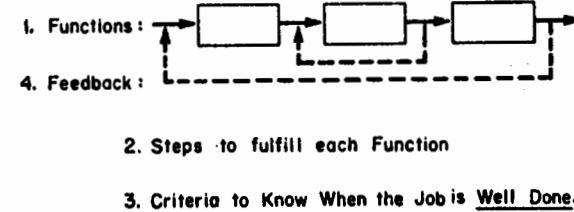


"TRADITIONAL"

- Policy Making
- Setting Objectives
- Planning to Meet Objectives
- Organizing to Execute the Plan
- Selection and Training for Manning the Organization
- Motivation of the People
- Appraising the Results



GOOD PROCEDURES



not seem to be a route whereby safety can enhance and supplement managerial methods improvement.

Uses of Safety Systems.

The presumed value of the Safety System Figures (11-1 and 11-2) lies in provision of a conceptual framework for safety performance measurement and accident analysis in order to answer questions, such as,

1. What are the effects of constraints on (a) the adequacy of knowledge, (b) the quality of the hazard analysis process, and (c) practicality of alternative countermeasures?
2. Were planned changes subjected to a hazard analysis process? If so, was the process inadequate? Or, was the failure in execution of the hazard reduction measures? Or, were additional countermeasures rejected on practical grounds? Or, was there pure oversight?
3. Do monitoring systems give management adequate assurance that the system is operating according to plan? And that plans are adequate?

Four key factors affecting safety and other functions in an organization are: technological, human, organizational and social inputs (Seiler, 1967). Accidents are systemic results of the four factors. In the Safety System the first three factors can be seen - the fourth, social factors within the system, has been treated as an aspect of the human factor, to be affected by, and also affecting the participative aspect of the system.

The system approach to safety is, first a method of thinking which forces one to understand and describe a process; such descriptions help guard against oversights and weaknesses, and also set the stage for monitoring the process. The system approach provides a logical way to determine where a safety problem is in the hazard reduction process, or where a problem slipped through the prior hazard reduction process.

The system approach requires quantification of information on the feedback loops. Fortunate to our present purpose of quantification (given the dearth of safety research), is the view of system safety engineers that "order of magnitude" estimates (of forces or failures) will suffice in the initial stages of analysis. And we shall be hard put to come up with even "order of magnitude" estimates for some elements of the system.

The system approach is essentially a performance-oriented synthesis of what is known or believed, forced upon us at a particular state of knowledge. As such it then becomes a method of identifying gaps or raising questions for study, particularly interfaces or interactions at a point in time. Further, by providing a context within which a multiplicity of variables can be considered simultaneously, the system concept aids in research.

However, Churchman (1970) constructed a hierarchy of measurements which he thought was relevant to safety with "suggestive measures" (i.e., accident rates) at one end of a spectrum which included "predictive, decisive and systemic measures." With regard to decisive measures, he said:

1. "Decisive information systems ... model the user within a bounded system."
2. "They recognize that safety by itself is only part of the picture; reducing accidents or accident potential ... must be coupled with other objectives, e.g., production ... The coupling consists of finding a common dimension."
3. "Rarely expressed as an index (or rate or percentage),"
4. "In the decisive mode one cannot really speak of safety as such as a separate and identifiable aspect of a system. Instead we have to think of safety as an inseparable element of a more comprehensive measure."

This seems to imply that non-safety measurements (e.g., production) would be used with safety measurements in evaluating a feature of a safety program. Of course such a measurement principle is fully consistent with the earlier-quoted policy statements of corporations - e.g., "production with safety" and "safety and production are one and the same thing. They cannot be separated."

Churchman says the concept of systemic measures, as applied to safety, may be more than a decade away, but some of his points are valuable:

1. "The systemic information system is interested in the next higher level."
2. An example might be: "reduction in accidents in the factory is the third most important project of the system."
3. The ambition is "information about the whole system."
4. "The aim ... is to keep controversy alive, to use action as experiment, to create problems whose study will increase scope of understanding."
5. It collects "rudiments of information ... but it never regards these rudiments as givens."
6. If the rudiments differ significantly, "the system tries to alter or enrich its model of reality." "Part of the control strategy of the system is the selection of those 'aspects of reality' which provide it with the best measure of its progress."
7. The system is "eternally restless."

12. GENERAL SAFETY PROGRAM THESES

The general theses of a safety program based on the concepts thus far discussed can be stated as follows:

- I. A superlative safety system must establish control over the risks of actual and potential sequences of change, error and energy transfer which can cause injury, damage or loss.
 - A. The control of energy with barriers to harmful, unwanted energy transfer is the basic aim of the safety system.
 - B. Safe task performance by employees -- managerial, technical and professional, craft and operative -- requires correction of error-provocative work situations. Safety-prone situations assist each employee to avoid hazardous error by adequate task definition and design of work to fit the people.
 - C. Monitoring to detect unplanned change, and analysis and counter-change for all significant changes are needed for timely protection.
 - D. Impending or actual emergencies require expeditious interruption of harmful sequences to prevent accidents, and rapid, effective amelioration of accident results when they do occur.
- II. The safety system draws on the best knowledge and practice to create visible, disciplined methods to identify hazards and design adequate controls, and thus minimizes error and oversights which can impair performance as well as safety.
 - A. The best practices of leaders in occupational safety are augmented by, and integrated with emerging system safety procedures and scientific findings -- technical, behavioral and organizational.
 - B. The use of visible, disciplined analytic method is efficient and effective in applying a wealth of specific standards and recommendations and also detecting and correcting those situations for which progressively higher degrees of protection are feasible.
 - C. A dynamic safety system has simple elements working together to achieve a high degree of safety in a manner congruous with management to attain high performance goals.
- III. The specific objective of the safety system is to compare adequately analyzed alternative measures and select the measures which provide the lowest practicable level of risk in a manner consistent with performance and social goals.
- IV. The basic elements of a safety system are:
 - A. Management implementation of a sound safety policy.
 - B. A defined hazard analysis process to minimize errors and oversights.
 - C. Work situations which provide the environment and direction to enable people to perform capably and safely.
 - D. An information system which provides:
 1. Monitoring to promptly detect risks and deviations from safety plans.

2. Knowledge of hazards and corrective measures.
3. Prompt, adequate feedback on safety performance.
- E. Opportunities to participate for all members of the organization, services and assistance to help them fully use their capabilities for developing and implementing safety measures, and recognition for good work on behalf of safety.
- V. Transition to a new, high order of safety is possible if safety activities are systematically defined, measured, assessed and improved to form a strong, comprehensive unified effort.

IV. MORT

The Management Oversight and Risk Tree

MORT is a logic tree which provides a disciplined method of analyzing an accident. The Tree can, then, also be a guide as to what facts to seek in an investigation.

Since MORT is predicated on high-level ideals as to what a safety program should be, it also provides a format for safety program evaluation.

MORT is sufficiently searching and revealing that full scale analysis of only a few serious accidents/incidents will reveal many needed program improvements. A few MORT analyses provide more useful information than less rigorous analysis of large numbers of accidents. Therefore MORT analysis is cheap.

MORT is too complex and time-consuming for use in minor accidents. However, it can guide the collection of objective data for portions of the tree in an ongoing program of accumulating useful facts about minor accident causation and the hazard control program.

MORT identifies 222 "basic problems"--causative problems, or preventive measures. These, in turn, underlie 98 generic problems composing successively broader areas in management and prevention. Yet the specified basic problems, if studied in a continuously more analytic direction, may be only a good beginning in analysis, there may be other subproblems, and there certainly are thousands of criteria. Among the above concepts are about 70 "new ideas" and this is highly subjective, depending on a person's background.

IV

This page intentionally blank

13. DEVELOPMENT OF ACCIDENT "TREE ANALYSIS"

In earlier phases of this study a number of questions were raised about accident investigation and analysis, specifically, the shocking lack of a methods literature was criticized. The question was asked, "Is accident investigation an intellectually disciplined procedure?" An essentially negative answer was given. Consequently, an exploratory method of accident analysis was developed to embody some energy transfer, change, and systems concepts which had been discussed in the background paper.

From data supplied during familiarization visits to two AEC research sites, two major accidents were analyzed: "High Level Spill at the Hילac" and "Environmental Chamber." (Appendices A-1 and A-2.) The early analytic formats provided useful ways of exploring the voids in systems approaches prior to these two accidents. Several major impressions emerged from this work, namely:

1. Use of the forms (as then conceived) was dependent on a rather full understanding of the systems control procedures from which the forms had been derived.
2. Therefore, the forms would not provide a practical test or discipline for accident investigators and analysts who might not be fully familiar with the premises.
3. The logic of the analysis was not fully clear, just the results.

Consequently, the use of a "Fault Tree," probably the most rigorous (and expensive) systems analysis technique, was attempted.

A first trial of a general, abstract "Tree" method was developed and applied experimentally to the "High Level Spill at the Hילac," based primarily on a report (9/24/59) published by Lawrence. (The results are shown in Appendix A-1.)

The first trial led to an improved general Tree method, which was then applied to an environmental chamber accident. (See Appendix A-2.)

The second trial led, in turn, to a third effort to develop a general method.

At this stage, major events were utilized as examples for two reasons:

1. Only major events have reports with sufficiently detailed factual findings to support any rigorous analysis against high standards of control.
2. Only major events would warrant the high standards of control hypothesized in the Tree.

The results of the first two applications of a logic tree to two major

accidents were encouraging and startling. The method was seemingly exposing significant numbers of basic problems not explicitly identified in the original reports, and was showing indications of the rigorous, disciplined mode of analysis which had been sought. Further, once completed, the trees provided an all-important visibility to analytic process which enabled a reviewer to review, ask searching questions, and alter the analysis as additional relevant facts or his judgment might warrant.

As these analyses proceeded, the method was constantly being altered and expanded to provide appropriate critical questions specific to the two events. However, at the same time, using memories of other significant accidents, a general format of a more rigorous and universal logic tree was emerging.

The consequence was development of a generalized analytic method, "The Management Oversight and Risk Tree" (MORT), and this Tree in its third generation was used in the trials at Aerojet. From the trials a fourth generation tree is emerging.

The term "fault" was discarded because it implied blame; also because the method uses generalized failures (e.g., management failures) on tracks parallel to specific content failures, which is not consistent with the Fault Tree.

The generalized tree is much more complex than any specific accident tree because the former must indicate all the avenues which should be explored. A specific accident analysis shows only the findings which were contributive or causal, or negative even though not causal. However, if analysis of a specific accident showed graphically all of the aspects checked and found either irrelevant or satisfactory, it would be equally complex (and this has usually been done on blank MORT worksheets leading up to a final analysis).

All through analysis of the two serious accidents and subsequent development of MORT, management's role was shown with increasing clarity. The data needed were shown to be facts on management's control process, as much as the facts about a specific event.

Interestingly, and helpfully, MORT quickly displayed a capacity to gain management confidence despite the fact that MORT puts the accidents on management's doorstep. Two senior vice-presidents of a large research and development organization said such things as: "interesting, valuable, very provocative, and certainly opened my eyes to a lot of things," and "the first scholarly, in depth approach to safety I've ever heard in industry or research." On the technological side, Paul Hernandez of Lawrence, the "mother" of the hydrogen bubble chamber, said the analytic format would have saved the Board investigating the Cambridge explosion and fire many expensive meetings needed to settle

on investigative and analytic approaches.

MORT, at this time, is a complex analytic procedure. However, it can guide analysis of truly serious events, and also guide data collection by sampling methods whereby a tree can be compiled for groups of less serious events. Also, as further experience is gained, the key questions may emerge in an every more simplified format. Even today, the complex tree is composed of relatively simple questions in a logical sequence.

Field sketches of MORT analysis of five additional accidents are also reproduced in Appendices A-3 to 6. The purpose of using the original sketches is to show how the techniques can be employed flexibly to meet the realities of situations.

In addition, the cases (1 through 6) show that the technique is evolving, and suggest that further evolvement will be in order. As a matter of fact, further experience may indicate that some of the approaches used in the early work are superior, and a return to those forms of analysis may be in order.

The results attained by early trials of MORT analysis will indicate why the technique seems so promising. The basic investigation reports were good reports, witness an average of 18 problems (and recommendations) in five serious accidents. However, MORT analysis exposed an additional 20 problems average per case for review and action. The total results for five serious accidents were 197 problems or 38 per case, a commentary on the complexity of causal information. The average results for the five cases were as follows:

Nature of Problem	Identified Prior to MORT			Additional From MORT	Total
	In Report	In Follow Up	ST		
Specific Content	15	2	17	7*	24
Systemic	1	0	1	13**	14
	16	2	18	20	38

*may include a few which will be shown to be impractical after review, e.g., by a Board.

** several of these are omissions of different steps in the hazard review process, but such an oversight is the equivalent to overall gross failure in such review.

It should be explicitly noted that MORT analysis is self-fulfilling. For example, MORT postulates an information search as an essential step in the Hazard Analysis Process. The information search was not made; ergo we have a potential causal factor. That the information search would have produced useful information in any particular case must be evaluated. However, the assumption can be tested against a retrospective review of what information was available. If pertinent information was available, but not easily retrievable, we have an additional defect in the information system itself. Actually, the lack of information search creates what has been termed earlier "uncertainty" rather

than "assumed risk."

As the general tree, MORT was utilized, an extremely important conclusion emerged: Since MORT was a method of analyzing a single accident for the failures which caused that accident, it also was a format for appraisal and assessment of the safety programs which were intended to control accidents in general. Thus, in the closing days of the work at the three research sites, and in the year-long trials at Aerojet, the MORT format was used to show the strengths and weaknesses of programs. MORT appeared to have the capacity to ask searching and relevant questions, seemed to show why conventional (ANSI) "cause analysis" data was little used in decision making, and seemed to provide a rational context wherein unusual, varied, and sometimes divergent programs could be described and assessed.

14. THE MORT DIAGRAMS - INTRODUCTION

The third generation Tree (as developed by late March 1971) is presented in eight pages of diagrams. Page 1 presents the overview. The other pages continue the analysis to more specific subproblems.

Probably the best way to get into the use of a logic tree is to briefly discuss some of the concepts on Page 1 of MORT. The the various symbols can be explained.

A next step would then be simply following through the diagrams visually, step-by-step, preferably applying them to a program, problem or accidents. The diagrams are, in large part, self-explanatory, and each fork in the Tree presents a relatively simple question.

Then a review of the fourth generation MORT outline is in order. It represents a somewhat tightened logic for essentially the same concepts. The detailed discussion of concepts constitutes the main body of this text and is keyed to the third and fourth generations of MORT by reference and page numbers.*

First, the final consequences of an adverse event are stated at the head of the page. They include not only all injuries, and direct and indirect costs, but also the effects of loss of current production and the adverse effects on quality and quantity of output which frequently were occurring prior to the accident.

Second, a symbolic reference to "Future Undesired Events" which will be affected by the Management System is noted.

S. All contributing factors in the accident are seen as Specific Oversight and Omissions, until such time as they may be transferred to Assumed Risks.

Assumed Risks are cumulated from specific decisions that a solution to a problem is not available, is impractical, or is to be delayed for stated reasons.

Assumed Risks are normal, expected aspects of any activity - even getting up in the morning, or staying in bed! Risks are inescapable.

Most important, the specific expression of assumed risks very often provokes additional study and effort to reduce risks. Unanalyzed risks are not assumed risks, nor are "uncertainties" as earlier defined.

G. Management System LTA. A judgment that management is "less than adequate" would not usually be expected from a single event, but it is remarkable how frequently in-depth reports of serious accidents do make such judgments, e.g.,

* In early stages of familiarization with the process, it doesn't seem to make a great difference whether the third generation diagrams or the fourth generation outline is used. Either one will produce a more searching, disciplined analysis.

"lack of firm policy" in the Hilac report.

In this version of the Tree, Management Systems are shown separate from the process which produced the specific adverse event. Two purposes seem furthered:

1. A depiction of Management Systems will suggest aspects of the background of the specific accident which should be closely examined.
2. The specific event may, in turn, suggest which aspects of Management Systems may truly be "LTA", that is, "less than adequate."

This consideration of general management is a conspicuous difference from the Fault Tree technique - that is, a generalized condition is related, at least presumptively or indirectly, to the specific failures.

The system faults can be seen as "planned foresight less than adequate." The specific faults use 20-20 hindsight to detect omissions, oversights and errors. Each of the latter may also be translatable into system improvements answering the question, "Why could it go wrong?"

The analysis proceeds primarily from the faults or failures shown as "Specific Oversights and Omissions" with transfers to Management or Assumed Risks only as the facts demand. This is the first of the "gates" in analysis and perhaps the most rigorous and potentially unpleasant.

The continuation of the logic working backward from the adverse event is shown as follows:

S1 "Accident" - occurs when an unwanted transfer of energy reaches persons and/or objects.

S2 Amelioration LTA - occurs after the initial accident event. There are a number of programs which should reduce the ultimate adverse effects - prevention of a second event, fire fighting, rescue, medical service, and rehabilitation.

These may be LTA (less than adequate). A transfer symbol shows that analysis of these programs is detailed on page 4 of the MORT diagrams. For example:

a1 Prevent the Second Accident. The analytic process seems self-evident, except perhaps that this phase is distinguished from Emergency Shut Off (page 7). The process for both phases is similar. A question to be asked is whether practice has occurred under emergency conditions, e.g., an electrical failure in the dark?

a4 Emergency Medical Service LTA. Check transportation times. Verify that the hospital meets the Emergency Room standards of the American College of Surgeons.

S1 "Incident" - an unwanted energy transfer not necessarily resulting in injury or damage. However, any "near miss" could be considered an incident worthy of analysis, regardless of energy transfer.

al. A distinctive symbol calls attention to the possible Failure to Monitor and Review incidents. F/M&R could mean failure to detect prior related incidents and failure to earlier correct causal factors. Thus F/M&R becomes a causal factor in the current event.

SB2 Barriers LTA - the concept of successive barriers to transfer of energy seems very constructive, that is, suggests a variety of practical actions. Early and multiple barriers should be associated with larger energies. (See Chapter 2.)

The first four barriers should have been taken care of in Concept and Design. What about the next four shown in the diagram? (All eight are in the fourth generation Tree.) Consider each kind of barrier separately for potential use.

Note the HE Press Explosion in Appendix A. It shows a check of Barriers for different classes of persons and objects. Don't overlook questions of shock absorption and how shock could be cushioned or redirected.

The notion of Barriers, both to separate energies and to protect people and objects should be most carefully considered for each energy transfer. This analysis tests the skill and imagination, and has already been shown to be a provocative and critical series of questions in accident investigation.

SB3 Persons, Objects - the analysis (also detailed on page 4) is usually, but not always, perfunctory. Questions of evasive action and functional presence are examined.

SC1 Unwanted Energy Flow #1. This is the energy which has the final, primary role in the Incident. A small transfer symbol calls attention to the fact that the same analytic process is used elsewhere.

SC3 Unwanted Energy Flow 2, 3, ... n - a significant, perhaps large, number of serious accidents involve successive interactions of different sources of energy. This complexity suggests the importance of intermediate Barriers (SC2), and thus gives further opportunities to interrupt the sequence. It also suggests a data collection goal: How many accidents involve interaction of two or more energies? In 12 serious accidents, four had two forms of energy and four had three forms.

Again note the HE Press diagram for a careful breakdown of energy flow, and note the number of barriers to energy flow. Also note that the Hilac, MAPP, and Initiators cases (in Appendix A) had two kinds of energy to be analyzed.

What triggered the first energy transfer?

Fire spread gives an interesting exercise in energy potentials, transfers and barriers.

In this study there have been an interesting number of cases where analysts untrained in the technology were able to suggest potential barriers which had been missed by the technologists who made the investigation!

For Unwanted Energy Transfer #2, etc., a fault tree transfer symbol is used to show that the analysis used for "Unwanted Energy Flow #1" is potentially useful for successive energy potentials (plus the requirement to consider and foresee the potential interaction of energy forms, and provide needed safeguards or barriers between energies).

Having introduced this much of the logic and symbolism used in MORT, it would be well to pause and show the definitions of symbols used in subsequent analyses.

15. DEFINITION OF SYMBOLS

The symbolism was altered from that of the Fault Tree for two reasons:

1. Efforts at clarity - for example, the AND and OR gates should have clearer symbolic distinctions.

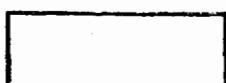
2. Efforts to explain - for example:

- a. Failures to monitor are judgmental as to where in the process they occur, and could be shown as specialized gates (rather than independent failures),
- b. A variety of contingent, fail-safe, and expected events should be provided for, and distinguished from one another.

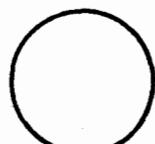
Fault Tree symbols are the subject of an ANSI code (Y32.14-1962) so variations may be questioned. However, a human factors specialist found the standard symbols error-provocative.

Figure 15-1. Tree Symbols

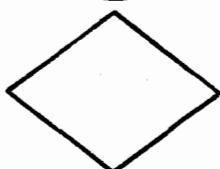
Events



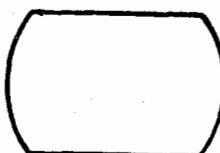
An event (usually a fault or malcondition) expressed in functional terms.



An event described by a basic component or part failure (these are the "independent" events).



An event at which fault sequence is terminated for lack of information or consequences, or for lack of solutions, in which case the event is usually transferred to assumed risks.



An event which is satisfactory, usually used to show completion of logical analysis.



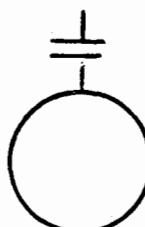
An event that is normally expected to occur.



A contingency event which alleviated or corrected.



A contingency event which aggravated problem.



A basic problem revealed in an investigation, and deserving recording and correction, but not a factor in the actual event which occurred.

Gates



AND Gate - Requires coexistence of all gate inputs for output.



OR Gate - Requires any one gate input for output, if more than one input exists, output will still occur.



PRIORITY AND Gate - Same as AND gate with the stipulation that one event must precede the other. Description is written in oval.



INHIBIT Gate - If input event occurs and the condition is satisfied, an output event will be generated; if the condition is not satisfied, no output will occur. Description of condition is written in figure.

Transfers



Transfer symbol used to transfer an entire sequence of analytic operations from another part of the tree (essentially a ditto mark), but the elements may have different numerical values or different and appropriate nomenclature.



Transfer to assumed risks for problems for which there is no countermeasure, or no practical countermeasure.



Transfers to another page for completion of process.

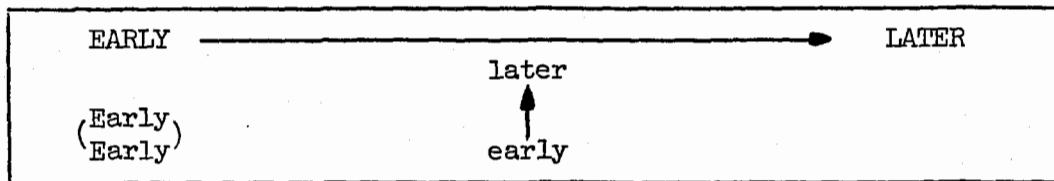
Abbreviations

LTA	= Less Than Adequate
D/N	= Did Not
D/NP	= Did Not Provide
F/	= Failed, or Failure to
F/M	= Failed to Monitor or Measure
F/M&R	= Failed to Monitor and Review

In general the schematic layout of the diagrams was as follows:

1. horizontally - left to right, from earlier to later in the Safety Precedence Sequence, and in the concept of successive barriers to energy transfers.
2. vertically - from bottom toward top as the causal sequences progressed.

Both of these rough dimensions are keyed to time as well as process.
Thus the rough order of arrangements can be seen as:



The value in this arrangement seems to be that early interruption of accident sequences is to be preferred.

This page intentionally blank

16. MORT CHARTS

At this point the eight pages of the charts should be reviewed briefly, but in their entirety.

Many concepts, and the analytic process envisaged, should be largely self-explanatory.

Then, a second review of the charts should be made, this time using the cross references (code numbers and page numbers) to consult the detailed text regarding items not clear from the diagrams. A complete reading of the text is necessary to fully develop the process.

Finally, practice and experience with the technique is needed to develop dexterity and skill.

A less studied, but practical approach is described on page 23--a tested recipe for GETTING STARTED.

From experience with the diagrams the following suggestions can be given:

1. The analytic diagrams work best if they are used as work sheets and pertinent facts about an accident or problem are noted in margins at appropriate places. Informality is a key--the diagram will take care of the discipline. MORT is a screening guide, helps avoid personal hobbies or bias.
2. It has been common to find on a first reading of a report that the report of what happened seems complete. But on second reading, and continuing to make notes on the MORT form, the gaps in information about what happened begin to be revealed. Questions about why it could happen begin to emerge. If a "problem" shown in MORT was satisfactory or irrelevant, it helps to write o.k., or X out aspects not needed. Red (bad) and green (good) can also be used, with blue for "don't know."
3. A third, slower, more disciplined trip through the diagrams is then in order. It is usually necessary to trace energy flow meticulously on a separate sheet, and then examine the nature of possible barriers, step-by-step. Also, if the diagrams do not clearly reflect adequate logic to get to the roots, draw special little trees.
4. At this point you are probably ready to mark up or draw a tree. Do not overlook the outline form shown for the Hilac case. However, the outline is only for easy reproduction of final results, not for analysis.

Cover Sheet - It has proven useful to have a place to note certain basic facts about each analysis. (See Figure on next page.)

Investment \$	Benefits \$	Risks	Values
---------------	-------------	-------	--------

Accident types and numbers	Years, cycles, uses, etc.
----------------------------	---------------------------

Life Cycle Estimates

Energies, Tasks, Functions, Exposures, etc.	History
---	---------

Brief Descriptions

Dates	Reviewed by

Subject

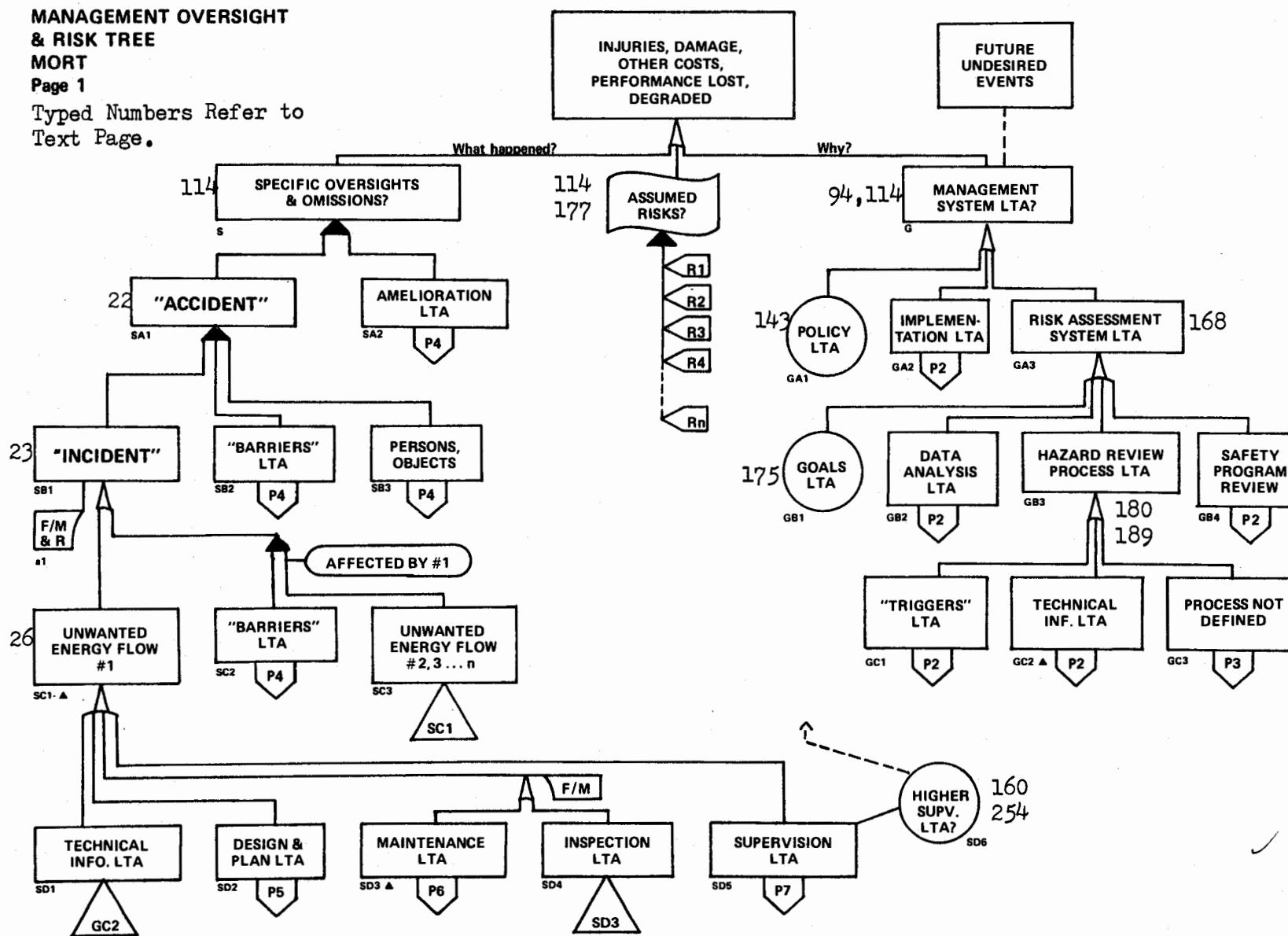
MORT WORKSHEETS

MANAGEMENT OVERSIGHT & RISK TREE

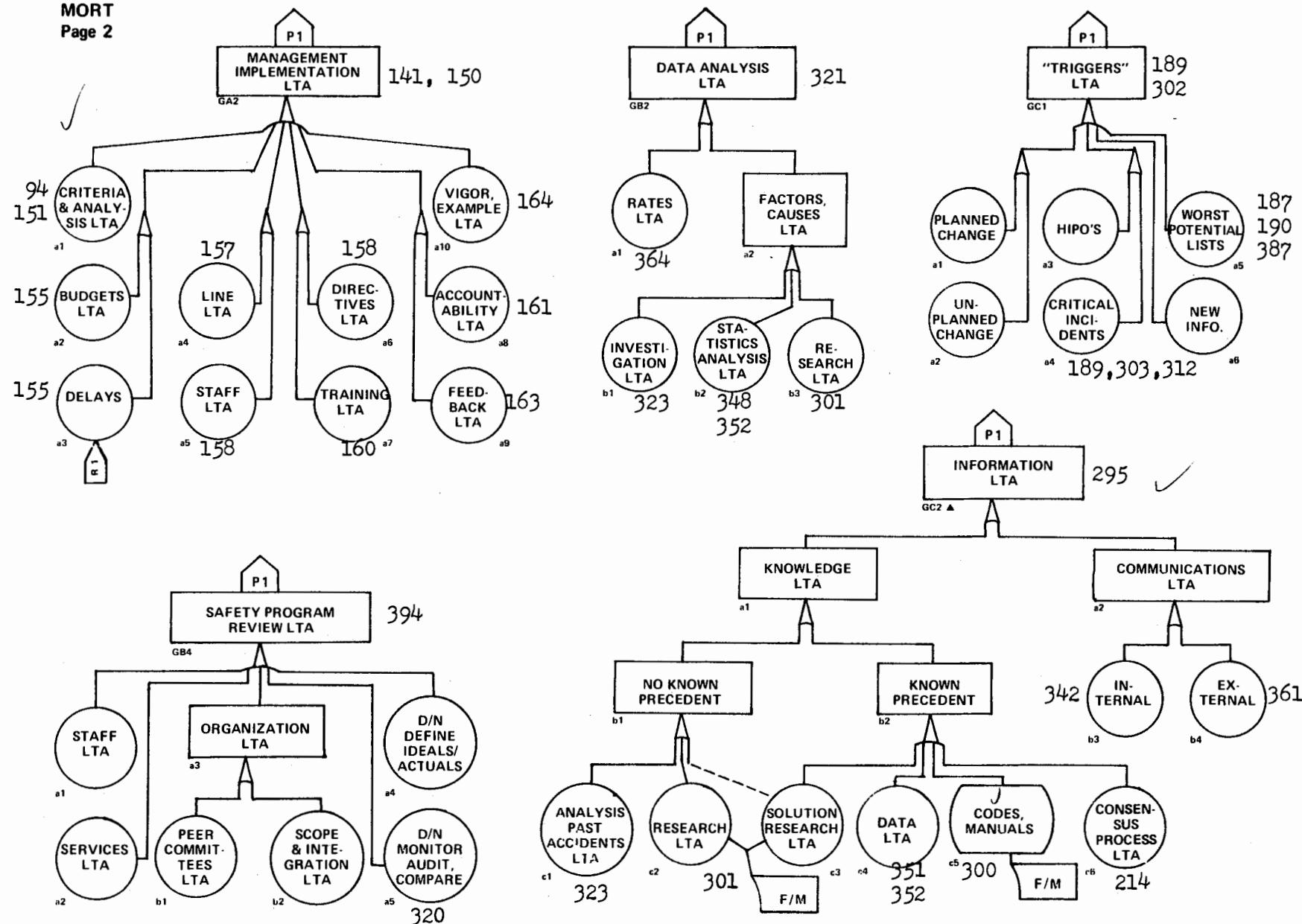
MORT

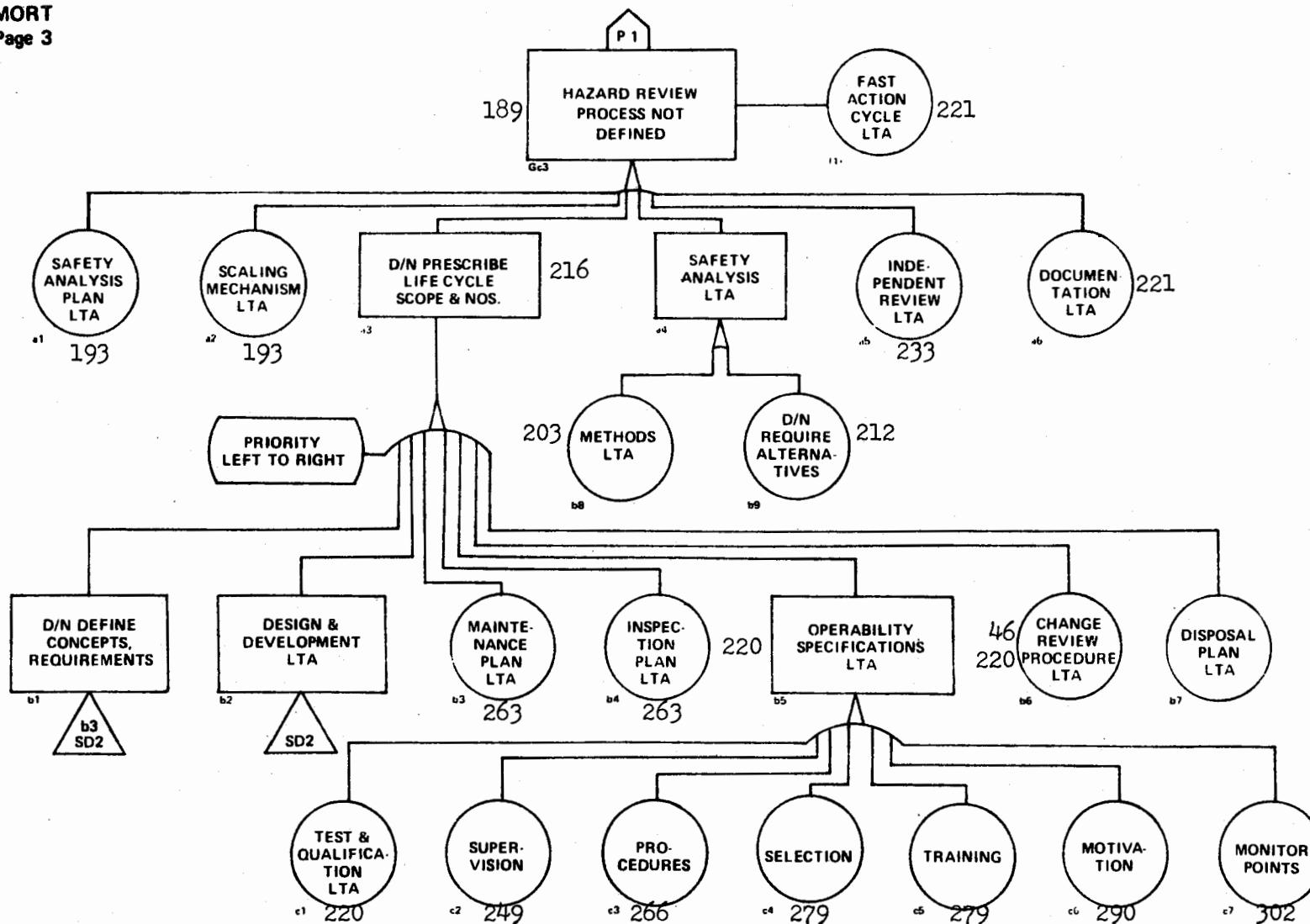
Page 1

Typed Numbers Refer to
Text Page.

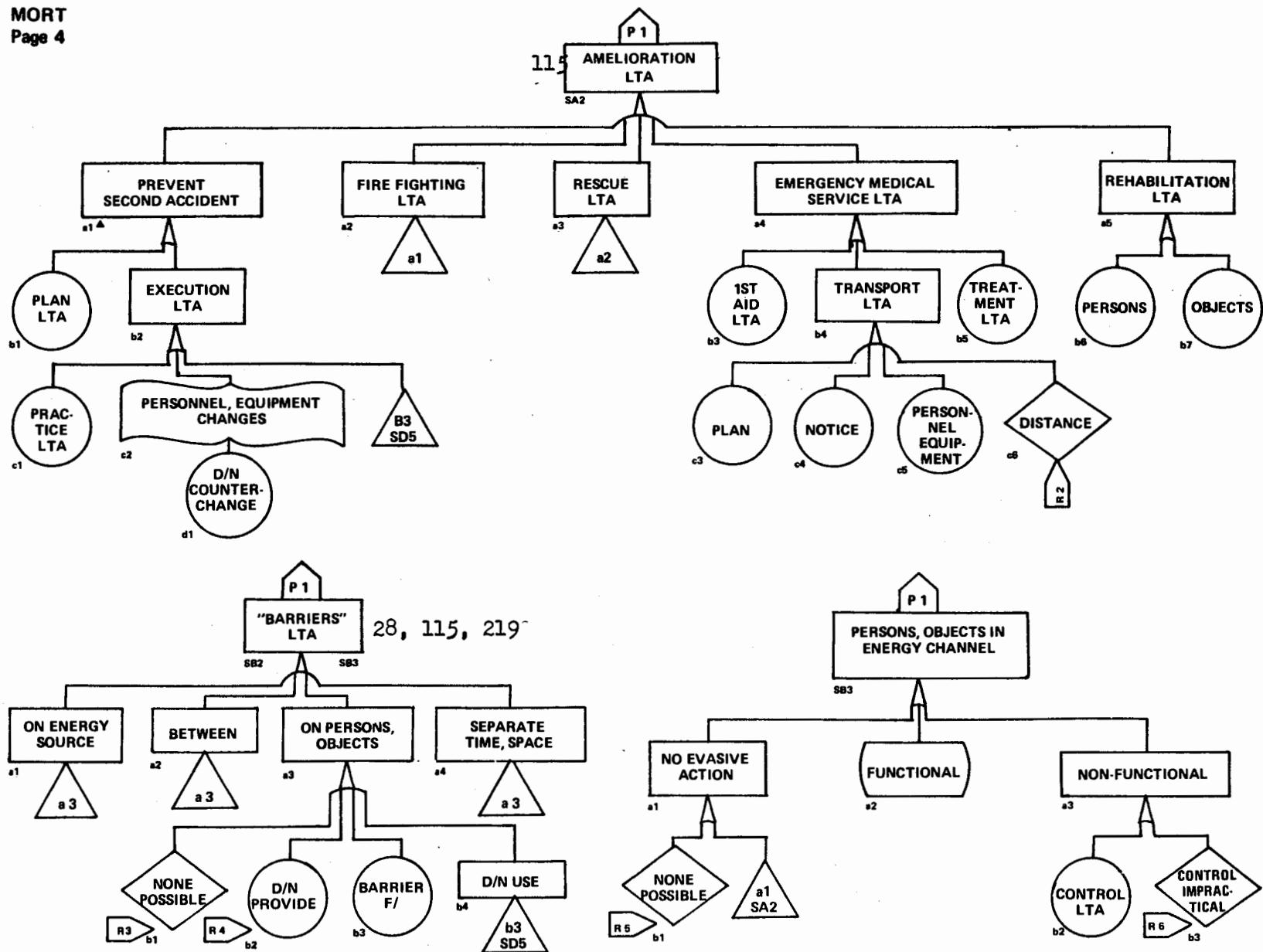


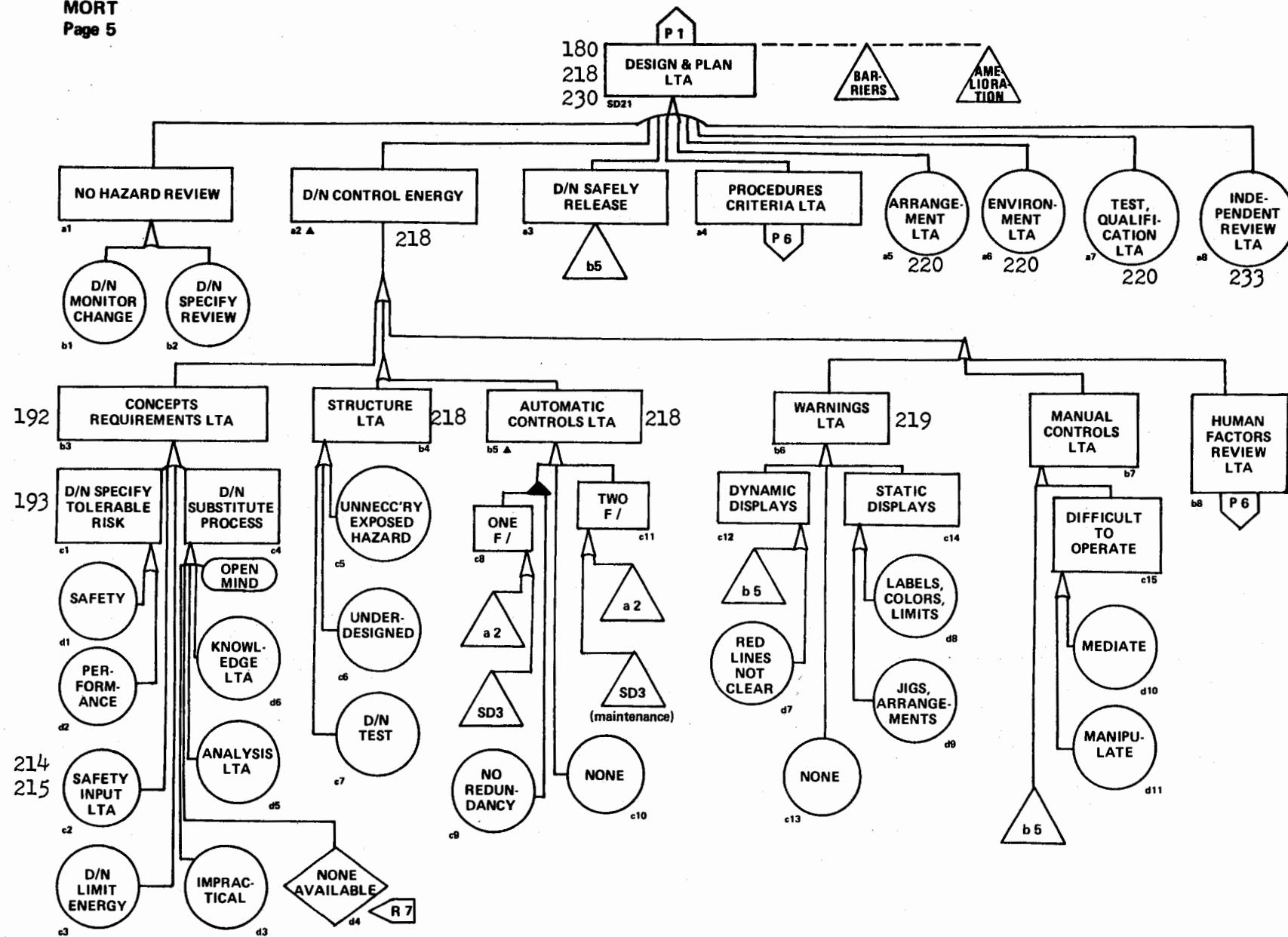
MORT
Page 2

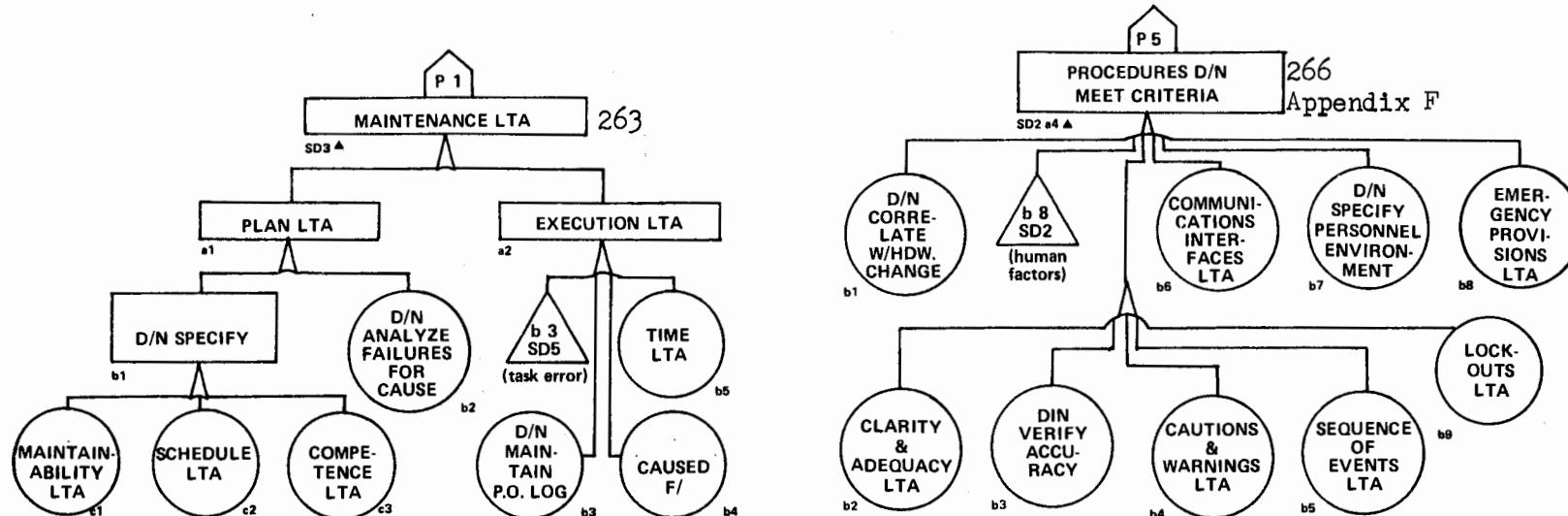
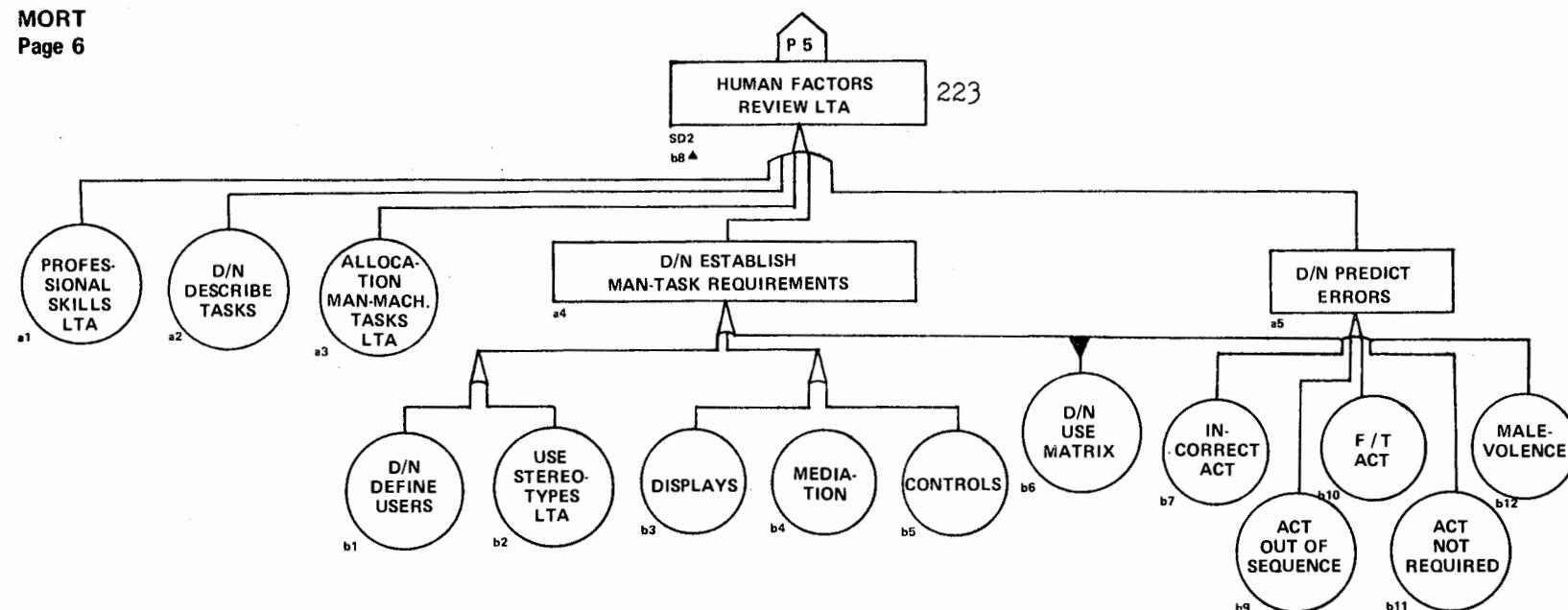


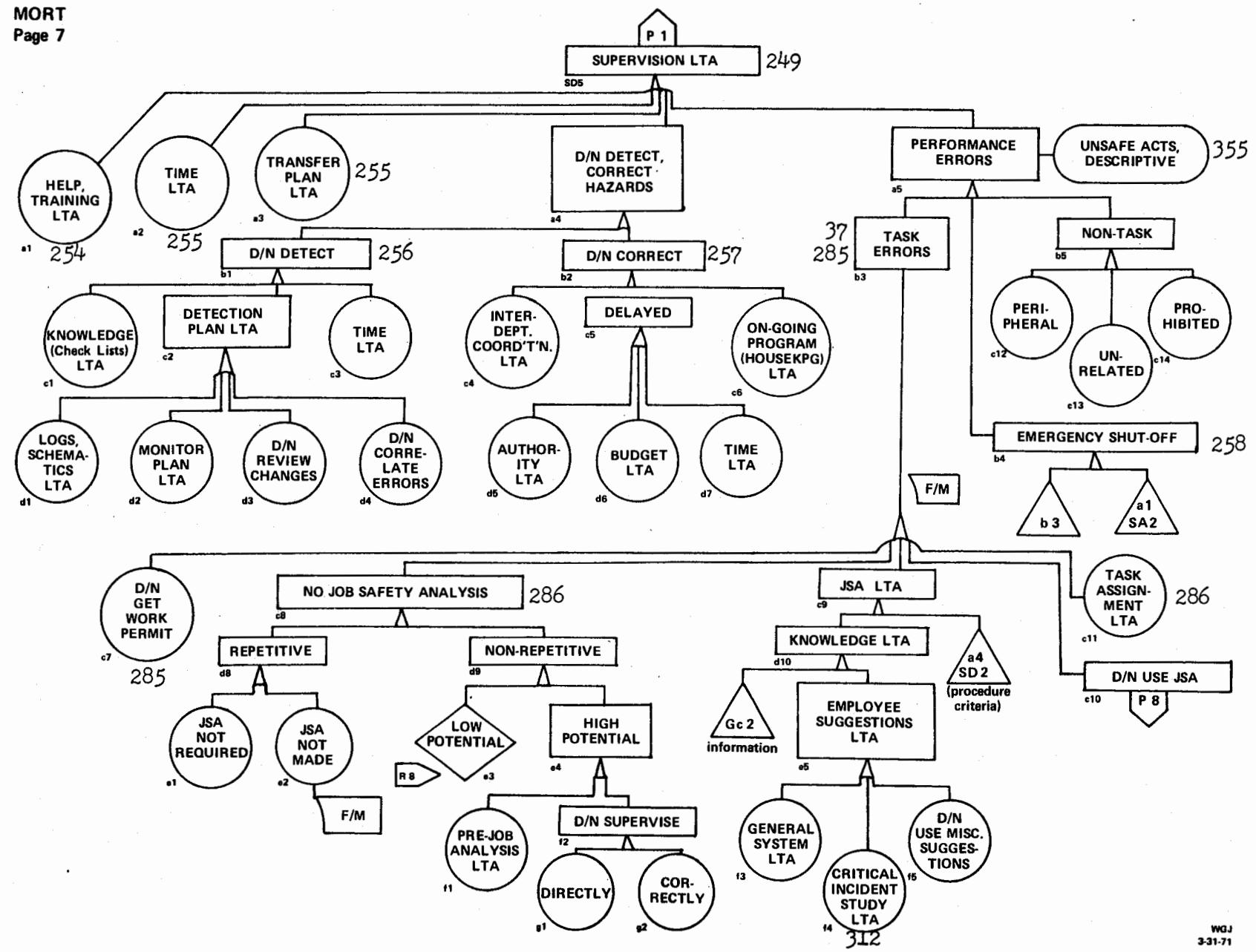


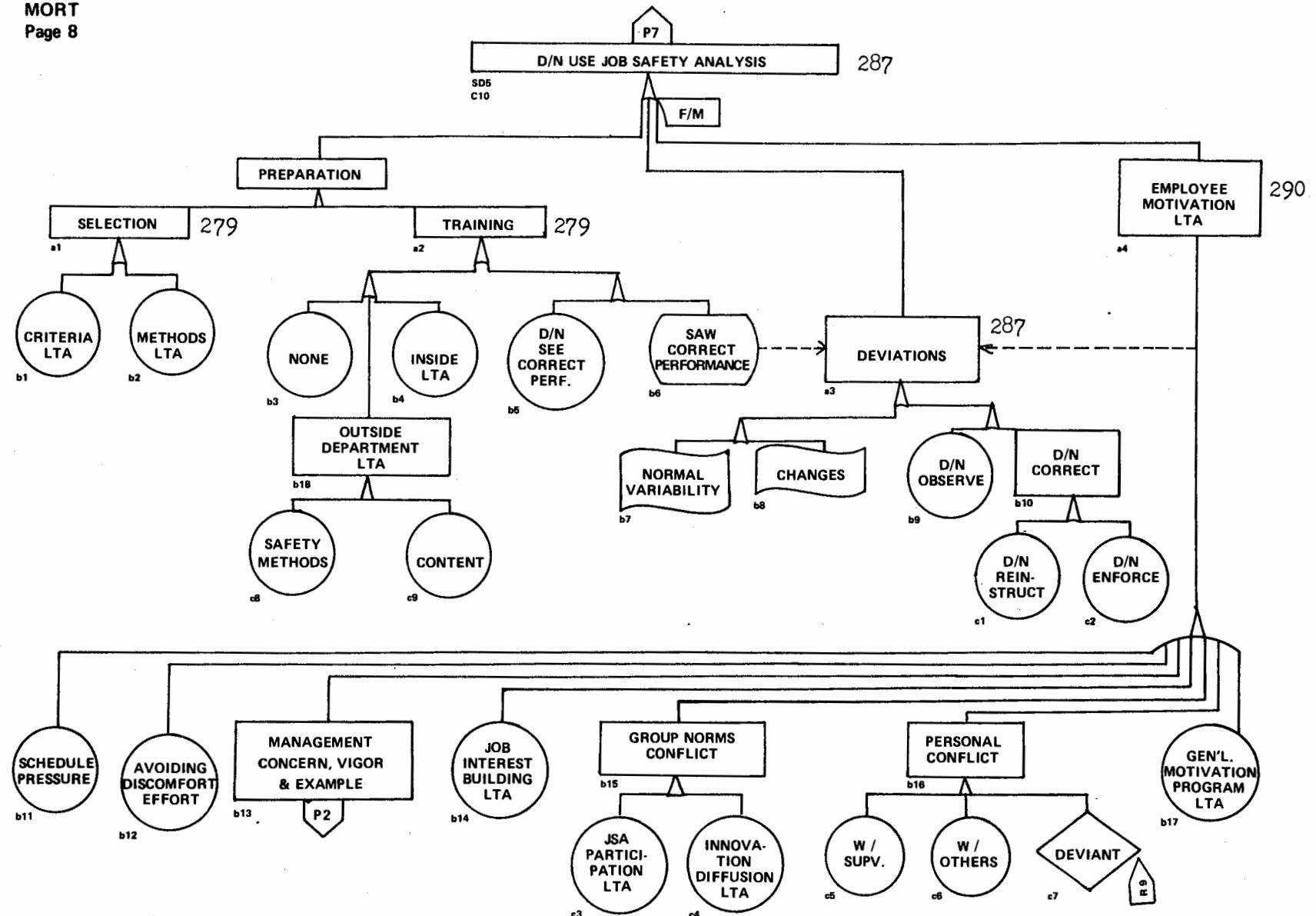
Appendix F











The concepts of causation or prevention postulated in MORT have been derived in a number of ways:

1. In analysis of events, specific accidents/incidents, and in analyzing problems and programs:
 - a. The absence of measures has seemed to be causative,
 - b. The presence of measures has seemed to be preventive;
2. A similar opinion consensus of safety professionals as revealed in literature and discussion.
3. Opinion consensus of non-safety professionals, most especially managers, was similar, but had important additional impact:
 - a. The articulation of a methodology made sense of safety (some said, "For the first time.")
 - b. Techniques were seen whereby the skills of the entire organization might be better utilized in the safety program.

This page intentionally blank

17. FOURTH GENERATION OF MORT

The trials at Aerojet revealed a number of developmental needs, and also suggested numerous points at which logic might be tightened, detailed, refined and improved.

Consequently, in recent months a somewhat improved outline, particularly for the General Management System, was developed but has not been tested.

Experience has shown that in almost every category of the diagram or outline a final item "Other" or "What Else?" could be shown. Analysts should not hesitate to add items omitted from the analysis.

Figure 17-1. Fourth Generation MORT

Numbers refer to text page:

G. General Management Systems Less Than Adequate (LTA) 114, 173

I. Policy LTA 175

II. Goals LTA 206

III. Implementation LTA 173

A. Methods, criteria and analysis LTA 185

B. Line responsibility LTA 190

C. Staff responsibility LTA 192

D. Organization and directives 193

 1. Organization LTA

 2. Directives LTA

E. Management training and assistance LTA 195

F. Budgets LTA 189

G. Delays (= Assumed Risks) 189

H. Accountability LTA 198

I. Vigor and example LTA 200

IV. Risk Assessment System LTA 205, 90

A. Information System LTA 343

 1. Technical Information LTA 349

 a. Knowledge LTA

 (1) Known Precedent

 (a) Codes, manuals, recommendations LTA* 260

 (b) Precedent LTA**

 (c) Lists of expertise LTA 347

 (d) Solution research LTA 97, 265

 (2) No Known Precedent

 (a) Accident investigation & analysis LTA 375

 (b) Research LTA 97

 b. Communications LTA

 (1) Internal 391

 (a) Network not defined

 (b) Operations LTA**

 (2) External 411

 (a) Network not defined

 (b) Operations LTA**

*This deceptively simple item is the entry into the vast body of content catalogued by the Nuclear Safety Information Center, NASA, and National Safety Council.

**Weak in all of above systems, especially retrieval.

2. Monitoring Systems LTA 351
 - a. Management routine supervision
 - b. Search-out
 - c. Accident/Incident systems LTA
 - d. RSO Studies LTA*
 - e. Error sampling systems LTA
 - f. Routine - HP, inspection, etc.
 - g. Upstream process audit LTA
 - h. General health monitoring LTA
 3. Data Reduction LTA 234
 - a. "Worst Potential" list LTA 435
 - b. Summaries, rates, projections, trend analysis LTA 415
 - c. Diagnostic statistical analysis LTA 391
 - d. Depth analysis of special problems LTA
 4. "Fix" Controls (HAP Triggers LTA) 443
 - a. One-on-one fixes
 - b. "Worst Potential" fixes
 - c. Planned change controls LTA
 - d. Unplanned change fixes LTA
 - e. New information use LTA
 5. Managerial assessment LTA 435
- B. Hazard Analysis Process Criteria LTA 223
1. Concepts and Requirements LTA 237
 - a. D/N Specify Tolerable Risks 237
 - (1) Safety
 - (2) Performance
 - b. Safety Analysis Criteria LTA 238
 - (1) Plan LTA
 - (2) Scaling Mechanism LTA 238
 - (3) Analysis methods LTA 248
 - (4) D/N require alternatives 259, 90
 - (5) D/N specify safety precedence sequence (e.g., priority for design) 225
 - (6) D/N analyze environmental impact 259
 - c. D/N Specify Requirements Criteria 260
 - (1) AEC
 - (2) OHSA
 - (3) Other Federal
 - (4) State and Local
 - (5) Other National Codes, Standards, and Recommendations
 - (6) Internal Standards
 - d. D/N Specify Information Search 262
 - (1) Nature
 - (2) Scope
 - e. Life Cycle Analysis LTA 225, 263
 - (1) D/N Specify Life Cycle Scope
 - (2) D/N require life cycle use, and failure estimates
 - (3) D/N require safety factors for extended use

* The well-known "critical incident" technique, in AEC called "Recorded Significant Observations" for semantic reasons.

- f. General design and plan criteria LTA* 281
 - (1) Design planning techniques LTA
 - (2) Organizational and functional responsibilities LTA
 - (3) Interfaces with operations, maintenance, test organizations LTA
 - (4) Definition of safety-related criteria LTA.
(Operating considerations and availability, materials, fabrication, construction, test, operation, maintenance, and quality assurance requirements.)
 - (5) Internal review
 - g. No hazard review
 - (1) D/N Require
 - (2) D/N Monitor
2. Design and Development Procedures LTA 267
- a. Energy control procedures LTA
 - (1) Unnecessary exposed hazards
 - (2) Under-design
 - (3) Automatic controls LTA 267
 - (4) Warnings LTA 268
 - (5) Manual controls LTA
 - (6) Safe energy release LTA
 - (7) Barriers LTA 33
 - b. Human Factors Review LTA 273
 - c. Maintenance plan LTA 311
 - d. Inspection plan LTA 311
 - e. Arrangement LTA 269
 - f. Environment LTA 269
 - g. Operability Specifications LTA ** 269
 - (1) Test and qualification 269
 - (2) Supervision 297
 - (3) Procedure criteria 315
 - (4) Personnel selection 325
 - (5) Personnel training & qualification 325
 - (6) Personnel motivation 337
 - (7) Monitor points 351
 - (8) Emergency plans (including amelioration) 306
 - h. Change review procedures LTA 270
 - i. Disposal plan 271
 - j. General Design process LTA* 281
 - (1) Procedures for code compliance
 - (2) Procedures for use of new codes
 - (3) Procedures for use of information
 - (4) Engineering studies to assure compliance of criteria
 - (5) Identification of weaknesses and analysis of "trade offs"
 - (6) Provision for preventive design features
 - (7) Standardization of parts
 - (8) Qualification of non-standard parts
 - (9) Design descriptions
 - (10) Classification of items - essentiality and safety
 - (11) Identification of items

* Based on RDT Standard F2-2T, USAEC.

** This section, which has major importance, can be further elaborated from material in Specific Oversight or a new major section could be inserted after Safety Program Review.

- (12) Acceptance criteria
- (13) Interface control within design process
- (14) Development planning
- (15) Development and Qualification testing
- (16) Test control
- (17) Development review
- (18) Failure reporting
- k. Independent review 283
 - (1) Internal
 - (2) External
- l. Configuration control 270
- m. Documentation 271
- n. Fast Action, Expedient Cycle LTA 271

C. Safety Program Review LTA 445

- 1. D/N define ideals
- 2. D/N describe and/or schematics LTA
- 3. D/N monitor, audit, compare 446
- 4. Organization LTA 449
 - a. Scope LTA 448
 - b. Integration (or coordination) LTA
 - c. Management peer committees LTA 453
- 5. Staff LTA 450, 454
- 6. Services LTA 455

R. Results - Injuries, Other Costs, Performance Lost or Degraded.

S. Specific Oversights and Omissions

- I. Amelioration LTA 140
- II. The Accident 25
- III. Persons, Objects in Energy Path
- IV. Barriers LTA 33
 - A. Limit the Energy (or substitute a safer form)
 - B. Prevent the Build-Up
 - C. Prevent the Release
 - D. Provide for Slow Release
 - E. On Energy Source
 - 1. D/N provide (Assumed Risk?)
 - 2. Barrier F/
 - 3. D/N Use (Insert by transfer, analysis of D/N Use JSA)
 - 4. None possible (Assumed Risk?)
 - F. Between Source & Person/Object } (Repeat 1-4
 - G. On Persons/Objects } above
 - H. Separate in Time or Space } above
- V. The Incident
- VI. Unwanted Energy Flows #1, 2, 3, ... n. 31
 - A. Barriers between energies LTA
 - (repeat Barrier analysis above for each energy interface)
 - B. Information LTA (repeat analysis G-IV-A above)
 - C. Hazard Review Process LTA (repeat analysis G-IV-B above)

- D. Maintenance LTA 311
- E. Inspection LTA 311
- F. Supervision LTA (includes JSA & personnel) 297
(Task errors should require use of Rigby's "error tolerance limits" (MORT, P.52,155) since accidents reveal all-too-common reliance on custom, habit, and forensic limits.)

(Details of above three items remain the same as the preceding MORT diagrams.)

AR. Assumed Risk 91

To be inserted by name when identified, analyzed and accepted.

Insert "Worst Potential" List indicating status of study or planned corrections.

The fourth generation of MORT will be tested in seminars and workshops, and in the continuing trials at Aerojet. It can be expected that a revised fourth generation tree will be available by July 1973.

This page intentionally blank

18. MORT VALUES, STYLES AND OBSTACLES

Values in MORT.

The principal values in MORT seem to be three:

1. Provide a disciplined method of investigating, analyzing and recording findings.
2. Provide a comprehensive framework for assessment of safety program.
3. Provide an orderly pattern for assimilation of new information on safety programming, i.e., facilitate professional growth.

The third of these is proving very useful. New information frequently drops into place in the diagrams. If it fits, it narrows gaps and uncertainties, and often strengthens concepts in greater degree than would be expected from an isolated finding.

These and other values are embraced in Figures 18-1 and 18-2, visuals used in presenting the scheme.

A related aspect, research, seems facilitated by improved concepts of factors needing to be held constant for an experiment or comparison.

Finally, the open-ended, experimental approach to problems and solutions has seemed to be aided, provided that a willingness to modify the MORT analysis is retained. Rigidity is still to be avoided.

All in all, it appears that the MORT system is a basis for managing the higher energies we utilize, and reducing the stresses, accidents, and other troubles inherent in our technology.

Styles of MORT.

There could be at least three alternate styles of MORT:

1. The present, failure type of tree,
2. A positive tree, which organizes what should be done,
3. A question tree which asks what was needed.

The present, failure tree seems to provide a logic, focus, and motivation for searching analysis. The motivation factor may be, in part, a fear of being shown wrong in an investigation or analysis.

The positive tree tends to be preachy and pious, a long-list of "you shoulds." However, an experimental use of a positive tree is embodied in some 17"x23" wall charts developed to show that the basic safety schematic (chapter 11) is consistent with the fourth generation tree (chapter 17), and that the tree is, in turn, an elaboration of the schematic. This chart will be used in workshops and in trials at Aerojet to examine its value.

Inherently a positive tree has one possible advantage, namely an OR gate for an aspect such as Barriers says any barrier will interrupt the sequence.

Figure 18-1.

MORT = A NEW SAFETY SYSTEM

CONTAINS: BEST ORGANIZATION PRACTICES +
SYSTEMS SAFETY +
OTHER IDEAS - NOT WIDELY USED +
SOME THAT ARE NEW!

METHOD - ORIENTED (TO HANDLE CONTENT)

COMPREHENDS: I.E. IS COHERENT & WHOLE
(NOT PARTIAL & FRAGMENTED)

FRAMEWORK — (A) FOR INVESTIGATION
(B) FOR PROGRAM
(C) FOR ASSIMILATION OF IDEAS & GROWTH

Open-ended
VIABLE — (A) CAN EXAMINE ITS FAILURES & CORRECT ITSELF
(B) IS THE LOW COST APPROACH!

GENERAL — (A) OCCUPATIONAL, FIRE
(B) RADIATION, TOXIC MATERIAL
NUCLEAR + WASTE

Figure 18-2

CRITICISM - "MORT IS TOO EXPENSIVE"

MORT IS PROBABLY THE LOW COST APPROACH

CONCEPTS

STANDARDS OF JUDGEMENT

INFORMATION SEARCH

ANALYSIS

}

CHEAP COMPARED TO
HARDWARE
ACCIDENTS

MORT INVESTIGATIONS - CHEAP COMPARED TO:

- A. "TYPE A" BOARDS
- B. STERILE MASS DATA FOR 1,000'S

MORT SOLUTIONS ARE CHEAPER THAN ENDLESS BRUSH FIRE FIXES THAT DON'T STAY FIXED

* * *

SCALE MORT TO SIZE OF PROBLEM OR BUDGET

BUT, DON'T SKIP STEPS

This is good in showing the many roads to injury prevention. In a negative tree an AND gate is needed, that is, all barriers to energy transfer were absent or failed.

A question form of the tree could be ideal in some respects - provocative and open ended. For example, "What criteria and analysis did management use to assess the situation prior to the accident? Or, to take a more difficult question, "Are safety engineers present on a big, complex construction project to continue the study of safe operability (not just construction safety)?" At an English seminar the answer to this question for Royal Dutch Shell was revealed to be, "Yes."

One disadvantage of the questions seems to be wordiness added to an already complex scheme. Also, there is the lack of precision, which seems to deny the existence of criteria.

Another type of question about MORT is: Should it represent the ideals, or should it represent the actual standards effective at a given time. This question is easier to answer, because the answer is, "Both." At least two sets of criteria should be used in any given environment:

1. The standards of program and prevention in effect at a given time, but organized in the MORT format. An example might be, "Was Job Safety Analysis required by management?"
2. The higher ideals of MORT. For example, "Should management require Job Safety Analysis?" (if the answer above was "No"). "Should management require a visible, recorded information search as a part of a Hazard Analysis Process?" or "Should management require change analysis as part of HAP?"

Further, there is the alternative of having at least two ideals:

1. the MORT ideal.
2. The ideal articulated by any safety professional in similar outline or tree form. The latter may, of course, be the "practical ideal" for a given organization.

In a sense it is perhaps not so important which ideal be used as that the actual and an ideal be articulated. If you don't agree with a MORT concept, just set down in a clear, analytic format what you believe to be the ideals.

Any logic tree becomes a method of structuring a problem. As such it contains certain "rules of thumb:" or "heuristics" as they are called in present-day problem-solving techniques. An example would be a factor of safety of seven in a structural problem, or a requirement for information search in a

hazard analysis process. These devices are necessary short-cuts to a satisfactory solution, but not always the optimum solution. Thus, the tree anyone may construct, using MORT as a point of departure, is an orderly way for stating the assumptions and devices which a given organization will use to solve its safety problems.

The term "less than adequate" could be varied in several ways. The term derives from a finding by a management research organization that people were apparently more objective about scoring and accepting scoring if a five class grouping was used:

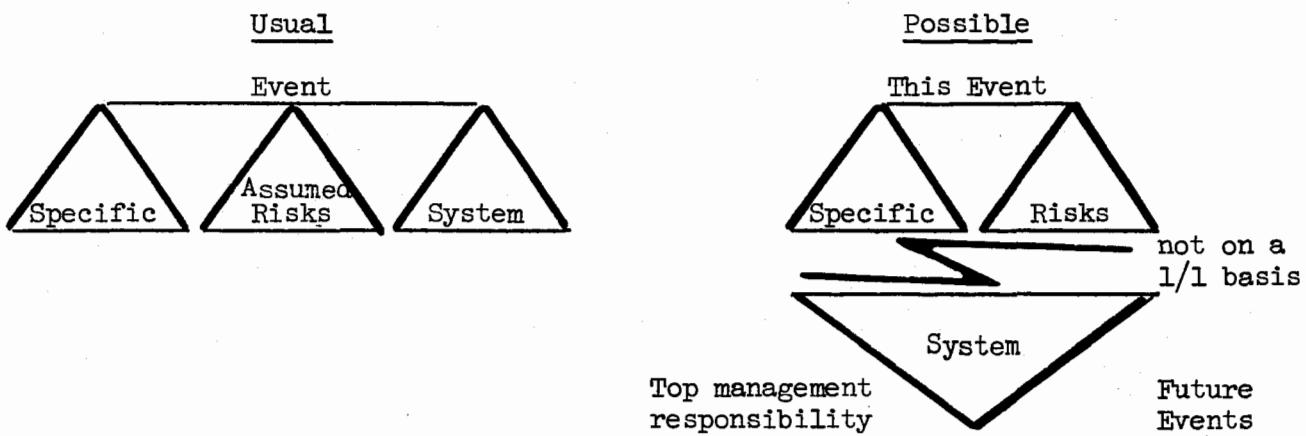
1. Excellent
2. More than adequate
3. Adequate
4. Less than adequate
5. Poor.

The "poor" category is often under-used. The "less than adequate" term seemed to create fewer emotional problems.

Obviously we could score all the program features used in MORT across this five stage scoring system.

Another possible alternate form of MORT is represented in Figure 18-1. The question is: Should the analysis be presented as two parallel, primary trees or as a specific tree stemming from an inverse management tree.

Figure 18-3. Some Alternative Forms of MORT



In many respects the portrayal on the right above seems the most accurate and correct picture of the role of the system in a particular event.

Another question of format is the choice of the fault-tree type diagram versus the outline format used in Chapter 17 and in Appendix A-1 as an alternate format. The diagram has seemed to be more provocative of thought and consideration. On the other hand, the diagram is more laborious, particularly if well

drawn artwork is a requirement. The practical solutions seem to be (1) use the diagram for analytic work or field sketches, and (2) use the outline form for formal reporting.

All of these alternate formats will continue to be examined, and deserve trial in various organizations.

Obstacles.

Apparent cost and difficulty of MORT analysis are serious obstacles.

The cost is, however, low compared with the overall expenditure in investigating serious accidents. The cost is low, for results obtained, compared with the aggregate effort required for superficial investigations of larger numbers of events.

One obstacle is the need for advance study of the method, well before the event to be analyzed. However, one analyst used the method to good effect without prior study.

As with any problem-solving technique, it is desirable that two or more persons be familiar with the method so that dialogue is possible. The obstacles are summarized in Figures 18-3 and 18-4, and other visuals used in presenting or discussing MORT.

The greatest obstacle is seemingly an inability to get started--a paralysis of the writing mechanism. For this the cure seemed to be in the recipe for GETTING STARTED (page 23). This approach seems to move an inexperienced analyst to action. Thereafter, the process is one of collecting more information and gradually formalizing and disciplining the analysis. The final step is a meticulous application of the analytic logic to the final assemblage of facts.

In review of complex, highly technical events, the analysis commonly takes four hours. For less serious and complex events, as little as twenty minutes has produced useful results.

As a practical matter it is well to keep in mind that there are simple solutions to many accident problems. On the "fast track" for known hazards with known solutions, apply the solution. The problem is application.

On the "slow track," that is for boundary problems or known hazards with imperfect solutions, the problem is finding better solutions.

Figure 18-4

THE NEW SYSTEM

SUGGESTS THAT THIS



GOAL

"ORDER OF MAGNITUDE
IMPROVEMENT"

CANNOT BE ATTAINED BY JUST
IMPROVING OLD APPROACHES

* * *

WARNING - MORT IS "NO RESPECTOR OF MAJESTY"

"DEFICIENCIES AT ONE LEVEL MIRROR DEFICIENCIES IN SERVICE
AT THE NEXT HIGHER LEVEL"

This page intentionally blank

V. MANAGEMENT IMPLEMENTATION OF THE SAFETY SYSTEM

In Chapter 11 a safety system congruous with management methods and management for high performance was described. In this Part we shall examine some aspects of management implementation of such a system--policies, criteria and goals, budgets, delays, line and staff responsibility, directives and organization, training and other assistance, feedback, and the vigor and example of higher management.

We shall begin to examine management errors according to the methods and criteria usually applied only to operator errors.

Mainly, we shall try to make the point that when an accident occurs it is the system that fails, more than persons.

The risk assessment system is discussed in terms of methods and goals. Some elements of the risk assessment system--the Hazard Analysis Process, the information system, and safety program review--are obviously a part of management implementation, but are discussed in subsequent sections as a matter of convenience in breaking up a large, complex subject.

The MORT analysis has already served a useful purpose in the opinion of some Aerojet and other personnel by simply placing management implementation of safety out on the table as a proper topic for investigation, analysis, and recommendation. Management is widely recognized as the most basic and fundamental aspect of safety. It is also the most difficult to measure. A general silence in the safety field on the specific characteristics of effective and ineffective management is ending, and well it should.

To be unmistakably clear and avoid surprises, it must be emphasized that when MORT is operating properly, the responsibility for accidents is traced to top management failures and deficiencies--operating, technical, supervisory, and middle-management errors are

subsidiary to the top management oversights and omissions which allowed the failures to occur.

The correction of an organizational weakness is usually more significant than the correction of a physical condition.

The Management System failures (right hand of MORT diagram) will be discussed first, because such material gives broader, more comprehensive guidance to investigative questions than the specific failures in the accidents thus far analyzed. The systemic failures suggest the kinds of specific data which should be sought for individual accidents, or groups of accidents.

The revised MORT criteria follow:

MANAGEMENT IMPLEMENTATION

1. Methods, criteria and analysis
2. Line responsibility
3. Staff responsibility
4. Organization
5. Directives
6. Management training and assistance
7. Budgets
8. Delays (= Assumed Risks)
9. Accountability
10. Vigor and example

19. MANAGEMENT POLICY AND DIRECTION

There is broad agreement that vigorous top management leadership is an essential and conspicuous feature of the best corporate and government employee safety programs.

Recent National Safety Congresses have featured presentations of just such corporate programs, and it has been common for the president or executive vice-president to lead off the presentation. Both words and attitude displayed leadership, and the management position was almost invariably crystallized in a policy statement or statement of corporate objectives which ranked safety side-by-side with the other principal corporate objectives.

The report of a British chemical industry working party (1969) on U. S. safety practices (an excellent and concise reference) provides an objective, independent appraisal:

"Safety policy is based on the absolute conviction that for maximum profitability and efficient operation it is necessary to reduce damage to people and property, whether through accident or fire, to the minimum. Supporting this view is the belief that management has a responsibility to its employees to provide a safe place to work."

This summary statement touches on three motivations or values of top management, and review of policy statements and actions of corporations adds others:

1. Welfare of the employee.
2. Cost of accidents and injuries.
3. Efficiency and effectiveness of the organization as a system.
4. Legal requirements.
5. Be a "good citizen" in the community.

Although all of these motivational forces are commonly found, the policy statement of a particular organization is not likely to contain all, but is more likely to emphasize one or the other. The NSC's Industrial Conference collected a substantial group of such policy statements some years ago to attempt to derive a general consensus. However, a consensus was not then apparent and the outcome was publication of many examples. (NSC, 1966).

If any given combination of the motivational forces has in fact in a particular organization produced the requisite top leadership, all well and good. However, if we are concerned with developing and building even greater leadership, or creating such top leadership in other organizations, we must examine the nature and force of the motivations.

The attitude of concern for the welfare of the employee is a fine and wonderful thing. Its history began in 1906 when Judge Elbert Gary, president

of the United States Steel Corporation wrote:

"The United States Steel Corporation expects its subsidiary companies to make every effort practicable to prevent injury to its employees. Expenditures necessary for such purposes will be authorized. Nothing which will add to the protection of the workmen should be neglected."

And a strong tradition has been built up in U. S. Steel which has one of our country's best programs. Certainly duPont, AT&T, Kodak, and General Motors, just to cite a few other prominent examples, have powerful concern for employee welfare.

The welfare motivation cannot be disparaged where it is strong, but what if it is weak? Will it be easy to change such an attitude? It seems more difficult to change than a less emotional, more rational motivational basis.

An interesting insight into motivation was given by Crawford Greenewalt, while president of duPont. He said that his company had had a safety program for 150 years. The program was instituted as the result of a French law requiring an explosives manufacturer to live on the premises with his family!

Some change in management attitude might be brought about by peers in other companies, as for example in safety activities of a trade association. But is the safety professional in a favorable position to change a welfare-based attitude? Probably not.

* * *

The costs of accidents and injuries and the motivation to reduce them are powerful, as far as they go. But there are problems in getting complete data on all direct costs, including damage, and even greater problems in measuring indirect costs.

Costs are highly variable by industry (e.g., high in lumbering, mining and construction). Costs may be overwhelming if catastrophic (e.g., a chemical plant or refinery explosion, or major fires in general). Costs may be high if public or product liability is involved. In all such organizations, cost reduction motivation may be useful.

The cost reduction motivation may not be strong enough to do more than get a program started. Consequently, cost data and even insurance savings must be used cautiously, that is, they may boomerang to place safety well down on management's list of concerns.

If a safety program has reduced the cost of a compensation-medical insurance program from \$100,000 to \$60,000, the reported results will never be greeted with other than acclaim by a top manager. However, if just before and just after the acclamation, the top manager is concerned about such problems as a multi-million dollar plant expansion, quality programs on a million dollar product line, or resignation of a sales executive who pro-

duced a doubling of sales in four years, you can guess where safety will wind up in his priorities--well down the list!

Projection of worst potential losses may be powerful.

One seemingly effective technique has been to equate accident losses to the amount of sales needed to recoup the losses.

A variety of methods of cost calculation and cost motivation have been urged. Heinrich found a four to one ratio for indirect and direct costs, a useful number, but neither precise nor very persuasive. More recently Tuz and DeGracia (1967) found a ratio of 7.2 to 1. (Also see Brenner and Mathewson, 1969, and Simonds and Grimaldi, also 1969.) Bird (1966) has given great visibility to the values in property damage reporting and analysis, which is a valuable prevention tool, but is not the same as relying on cost motivation of management for the fundamental thrust supporting the safety program.

A primary tenet of this text is that a wide variety of apparently non-accident events are in fact also associated with safety via common cause. From this it must follow that tabulatable costs of accidents, even if indirect costs are put in by a ratio or other method, will inevitably underestimate the true value of eliminating accident factors.

* * *

The efficiency motivation, which seems to be the primary and most forceful motivation, is more difficult to define and describe, even though studies as early as 1922 showed productivity and safety jointly varying: accidents down and productivity up, and vice versa. Certainly what is meant here is something more than just cost reduction. Perhaps it is better stated as the correct, efficient, and error-free way to operate and control. Hopefully, the safety system schematics (Chapter 11) will advance this effort.

A Canadian wood products company says, "Safety and efficient operation are one and the same thing. They cannot be separated." Other significant quotations from management policy statements are available in NSC's Data Sheet 585.

Certainly the companies cited as examples of strong welfare motivations also recognize this aspect. For example, the General Motors policy also emphasizes that a good safety record is clear evidence of good management. And the duPont philosophy clearly reflects a belief that the safe way is the only proper way to manage.

A duPont manager spoke of safety as his "sharpest tool to measure supervisory performance." The objective of safety was "essentially unqualified in his company. (Cost and quality objectives are mutually qualifying.) Therefore, if a supervisor couldn't manage to get safety, he probably couldn't manage anything else. Moser (1964) gives persuasive arguments for "safety first." His own performance record, and that of his company in the stock market, attest to their credentials.

And in another large company:

A highly illuminating story was told by a Shreveport, Louisiana, plant manager at the time he was receiving a safety award. Some five years previous the plant had been at the poor end of the corporation's ratings of all of its plants in profitability, quality, waste control, employee turnover - and safety. The plant had a fatal accident. The manager received a wire from the president which asked, "Can't Shreveport do anything right?" The manager decided to have the best safety program he could mount. By the time Shreveport got the safety award, the plant had moved near the top in the ratings on profitability and efficiency. It could do things the right way.

Among the production hindrances reported to have the same causes as accidents are: reduced output, scrap and re-work, materials handling, man-hours per unit, machine-hours per unit, morale and turnover.

Somehow safety professionals are still weak in the language and conceptual development to state the true significance of accidents in the overall performance of a company. The fact that accidents interrupt work, or have human and economic costs, is not the full measure of their relation to efficiency. If the accident is seen as a symptom of managerial failure to establish reliable control of work, as an error resulting from poor management or managerial omission, which also produced inefficiencies, we shall be closer to the mark.

The principle that "The Safe Way is the Right Way" is not based in morality, ethics or a welfare attitude. It is a principle of good management.

Pope and Nicolai (1968) had this to say:

"Management must be educated to the fact that the function of safety is to locate and define operational errors involving incomplete decision-making, faulty judgments, administrative miscalculations, and just plain stupidity. These expressions are well understood up and down the ranks. Success with this approach is possible, but it will require considerable study, discussion, and change of viewpoint before being accepted."

General Motors has described safety as "planned order," which is really a system approach. When examining the role of chance in accidents, we also saw in chance phenomena some interesting relations to efficient production (e.g., the car assembly case).

It would seem that the efficiency-safety relationship is even more difficult to measure in government or non-profit agencies which cannot use as background, the relatively simple profit yardstick.

* * *

The legislated motivation for increased safety is, of course, a primary force in the U. S. today due to the passage of the Occupational Health and Safety Act (OSHA). Considering that OSHA standards represent a consensus of past wisdom and recommendations, but hearing the screams about OSHA, one can only conclude that there were a lot of hazards to be corrected and that many are being corrected.

In a text for a British seminar prepared in mid-1969 the author said:

Governmental regulation and inspection of working conditions is primarily a state responsibility in the U. S., and all too many of our states have weak laws and regulations and inadequate inspection forces. The Federal government is rapidly moving into this area. Certainly adequate governmental controls over minimal conditions are a must. But, the higher goals of safety are not attainable by regulations, at least not by the conventional regulatory methods. Some new and potentially better regulatory methods have been proposed, but have hardly had serious thought in most circles.

It has frequently been said that guarding is superior in England and several European countries. For example, the chemical industry working party said:

"Finally, the lack of guarding on machines is particularly noticeable, and is almost certainly due to lack of legislative requirements. Although the U. S. worker is indoctrinated in the need to avoid contact with machines, we believe that the U. K. system of physical protection is better."

It is difficult to reconcile this comparative condition with the generally lower U. S. rates. It is said in the U. S. that European managements tend to comply with physical standards supplied by government inspectors, but stop with that action. Whereas U. S. companies have stronger management and supervisory programs. Obviously our goal should be both, but it may be that the compensating effects between government and private initiative prevent both being maximized.

It is unfortunate that at precisely the time that we should be aggressively seeking improved methods, the U. S. is primarily concerned with meeting minimal conditions largely attained in Europe a decade or more past.

* * *

It seems correct to suggest that simple compliance with such regulations as OSHA will entail a good part of the costs of a higher grade, performance-oriented, hazard analysis process, but will produce fewer benefits. Compliance with regulations may become a ceiling rather than a floor.

Optimum long-term relationships between OSHA and voluntary approaches are extraordinarily difficult to perceive at this time. However, British experience with national regulations may provide insight. Some British views of U. S. management leadership are cited (page 175), and the superiority of British physical protection is cited above.

Some possible insight into our U. S. situation may be provided by Lord Robens' Committee Report to Parliament (July, 1972):

"We need a more self-regulating system of provision for safety and health at work. The traditional approach based on ever-increasing, detailed statutory regulation is outdated, overcomplex and inadequate. Reform should be aimed at creating conditions for more effective self-regulation by employers and workpeople jointly.

"The efforts of industry and commerce to tackle their own safety and health problems should be encouraged, supported and supplemented by

up-to-date provisions unified within a single, comprehensive framework of legislation. Much greater use should be made of agreed voluntary standards and codes of practice to promote progressively better conditions.

"This broader and more flexible framework would enable the statutory inspection services to be used more constructively in advising and assisting employers and workpeople. At the same time it would enable them to be concentrated more effectively on serious problems where tighter monitoring and control might be needed.

"There is a lack of balance between the regulatory and voluntary elements of the overall 'system' of provision for safety and health at work. The primary responsibility for doing something about present levels of occupational accidents and diseases lies with those who create the risks and those who work with them. The statutory arrangements should be reformed with this in mind. The present approach tends to encourage people to think and behave as if safety and health at work were primarily a matter of detailed regulation by external agencies."

These British views suggest that management, while dealing with the requirements of OSHA, not fail to work toward higher goals, in the interests of total performance as well as safety.

It is of further interest that some of the best current reports of system approaches to occupational safety are coming from European companies. For example, a senior executive in England (Reynolds, 1970) outlines a successful program largely consistent with this text.

The interrelations of public and employee protection policies is highly variable, depending on the nature of the industry. In nuclear industries public protection is the first consideration, and occupational safety program has the collateral value of helping to ensure public protection by reliable control of work. But in industry generally the occupational program, frequently placed in a personnel function, has not commonly been related to product safety problems, nor always to environmental problems. However, management concern in these areas is growing. Some product and waste management problems stem from the same root causes as occupational accidents, and are amenable to similar controls. Consequently, it is appropriate to inquire whether and how public protection policies are articulated and implemented.

Public and environmental concerns will undoubtedly have increasing influence on all safety policy, including occupational safety.* It is difficult to perceive the ultimate effects on occupational safety of these broader concerns, because they range far beyond the domain of employee safety. The increasing concern for public safety may have at least the following four implications for

* "Public Safety: A Growing Factor in Modern Design" (National Academy of Engineering) is an example.

employee safety:

1. Occupational safety is increasingly a public concern, as in OSHA, or a specific hazard such as "black lung" disease in miners.
2. Occupational safety is an aspect of reliable control of work, thus affecting a broad category of accidents in waste management.
3. Occupational safety is a factor in product safety, not only in control of work and workmanship, but also in product design. The higher the employee safety standards, the more difficult is non-regard for protective principles in products.
4. Occupational safety analysis, where well done, may provide analytic techniques helpful in the more difficult areas of environmental impact.

Without knowing the relative force of these policy concerns, nor what government-private methods may eventuate, it seems impossible to predict the ultimate impact of essentially public concerns, except to say that their force will ultimately increase in policy areas normally considered the largely internal organizational problem of employee safety.

Other motivational forces which appear to have been potent with top management are personal pride in safety accomplishments and pride in a corporate image of safety. It follows from this that opportunities should be sought for management to speak of its successes at trade group meetings and in the business press. Trade association programs have been seen primarily for their values in reaching smaller employers, but their effect on leaders from larger organizations has probably also been great.

It has been said that no aspect of management projects a better image of an organization than a sincere concern for safety.

Further, it is common for management to take an active part in community safety affairs as civic leaders. And it appears that such participation has reinforced in-plant safety by supplying a strong, comprehensive philosophy.

A factor not widely discussed is management's concern for employee relations in a time when so many aspects are union dominated and when such delicate matters as productivity are involved. Safety is an area of clear mutual concern and has been said to be the topic on which it is easiest to "get along," not that safety grievances and issues may not at times also be sore points. Strong employee participation in safety programs, as for example in Job Safety Analysis, are required for effectiveness and acceptance of the safety program, and can certainly make an important contribution to improved employee relations. As on-the-job programs have been extended to off-the-job concerns, safety has been the basis for a bond of mutual concern of manager and employee (provided the

work place has been made safe).

We commonly say that safety begins with top management. But it may well be that the concepts and practices of leading U. S. managers are the end of several decades of evolution and mutual influence, rather than the beginning. And if we wish to take another management group from a more primitive to a more enlightened state, we may need a most carefully drawn, long-term plan for building understanding and acceptance.

* * *

The foregoing discussion suggests that management beliefs about safety be concisely and forcefully articulated in the areas of employee welfare, cost reduction, efficiency and performance, social concern (laws, environmental impact, product, and community), employee relations, and pride or image. Each top management group must do this for itself.

One policy aspect--practicality--remains to be considered. There is nothing wrong with articulating practicality. It has been written into many federal laws as a proper criterion. (Compliance with consensus standards is, however, always practicable by definition!)

To establish a platform, Currie (1968) examined a wide variety of definitions and concluded that the essentials were best captured in this wording:

"Safety is the objective conservation of men and equipment in a timely manner, and within the operational and economic requirements necessary in a progressive industrial community."

A sampling of management policy statements (NSC, 1966) reflects the difficulties and range of ideas in defining degrees of safety. Arranged in roughly descending order, they are:

- "...operate our plants and offices without accidents"
- "...work without danger"
- "...first importance"
- "...maximum safety"
- "...providing the safest conditions for our employees."
- "Accident control is thus essential"
- "Taking any action necessary to improve safety conditions."
- "...control unnecessary loss."
- "...everything within reason"
- "...every reasonable precaution"
- "...every reasonable effort"
- "...all practical steps"
- "...take time to perform our work safely"
- "...an effective safety program"

These are fine,
but probably
impractical

"...discharge our moral and legal responsibility for safety"
"...meet accepted standards"
"...conform to basic safety principles and sound management
practices."
These may
not be
good
enough.

"Adequate:

"Production with safety" represents a somewhat different approach.

Moser (1964) gave sound reasons, subtly involved in the organization's and individual's performance goals, for putting safety first. Further, he would appear to discount the relevance of cost/effectiveness measures as applied directly to safety program.

* * *

In MORT analysis:

GAI Policy. Characteristics to be examined include: Written? When updated? Comprehensive for all major problems (e.g., employee, transportation, public)? Comprehensive for all major motivations (e.g., humane, cost, efficiency, legal compliance, work near boundary conditions)?

During the trials at Aerojet, the corporate policy was revised. Excerpts are: "It is the policy of the Aerojet Nuclear Company:

- a. To provide for employee safety, to assure safe operation of government facilities, and to comply with applicable government and industry health and safety regulations.
- b. To provide for all employees a safe place to work, free from recognized hazards that are likely to cause death, serious injury, or illness.
- c. To develop, operate and maintain the Atomic Energy Commission's facilities and installations, for which it is contractually responsible, in a manner calculated to protect the health and safety of the public, prevent damage to government or private property, minimize adverse effects upon the environment, and preserve effective community relations, regarding health and safety matters.
- d. To comply with all applicable health and safety rules and regulations of the Atomic Energy Commission, including any special requirements formally imposed by the AEC Contracting Officer, to comply with the safety and health standards promulgated under the Occupational Safety and Health Act (OSHA) of 1970, and to adhere to generally recognized and accepted high standards of performance in the areas of occupational health, and nuclear, radiological, industrial and fire safety."

"The goals of health and safety are congruous with, and inseparable from, the goals of efficient and effective operation; i.e., to achieve high quality performance without interruption due to mishap, failure or accident. Therefore, nuclear and operational safety is primarily a line management responsibility."

In an interim report, the author suggested the following format to properly express what is, in reality, already AEC's policy:

"Protection of the health and safety of employees and the public is the first consideration in AEC programs. Associated efforts will be directed

at the prudent conservation and protection of government and private property and the environment.

Safety is congruous with, and inseparable from, management for efficient attainment of goals, and is supported by the reliability and quality assurance programs which are also required to assure performance without mishap, failure, or accident.

AEC pioneered the concept that advanced technological development and research near boundary conditions require prior analysis and planning to assure that activities attain the goal, 'First Time Safe,' rather than relying on the traditional sequences of trial, accident, and correction.

Thus AEC expects that adequate analysis and protective measures will be provided for all activities. Naturally the best utilization of resources dictates that major hazards receive major attention and a proportionate depth of preplanning, proceduralization, independent review, supervision, and monitoring to detect deviation from plans, prompt corrective measures and appraisal of results.

AEC holds top management of every AEC contractor responsible for adequate managerial systems to fulfill policy requirements and attain progressively higher goals in health and safety."

20. MANAGEMENT IMPLEMENTATION

In this chapter we use the MORT diagrams, and code numbers therein.

GA2 Implementation.

al Criteria and Analysis. Concept of relating overall methods to the safety program has been discussed in Chapter 11. Any lack of use of an adequate repertory of management methods suggests an organization may have difficulty attaining high performance goals, as well as high safety goals.

Sound practices for acceptance of proceduralized systems and improving human performance begin here. A small beginning in use of rewards in a manner suggested by the scientific literature has been initiated at Aerojet, by attaching a routine commendation cycle to one surveillance schematic. Also, initial Job Safety Analysis and "critical incident" studies seemed to have favorable effects on morale and performance, as well as on safety. However, a major policy study of methods of improving human performance and subsequent implementation still seems to be in order, likely in most organizations.

It is common to assume that safety is compromised by value conflicts in which safety motivations are of insufficient strength. However, we lack case histories which would pinpoint managerial factors in terms of values. It appears at least as likely, in the best companies, that weaknesses in safety analysis, failures to provide successive and alternative countermeasures, are major factors.

A concept of attitudes as information processing structures has potential value in designing programs to change management beliefs as well as attempting to create some measurement of values and attitudes. Schroeder (1970) has said:

"It is not simply a question of the value of safety ... It is rather a question of the nature of this belief ... 'Immaturity'... is the level or complexity of conceptual structure for processing information. The initial question is to determine the number of independent classes (or scales) of information the person selects as being relevant ... , weighting ... should also be assessed."

If then we can define the criteria of system safety which management ought to use in assessing safety, we may also have criteria for measuring the strength and nature of beliefs in practical and useful ways. Such a method would also test the limits of values by examining a larger list of alternatives to see whether they might have changed attitudes and decisions.

Examine the number and complexity of criteria and constraints used in safety decisions in order to evaluate maturity of judgment. Faulty criteria or analysis may lie behind program imbalance. Or, conflicting criteria (e.g., hazard control versus freedom of researchers) may be unresolved. Is adequate

analysis demanded by management? Are alternative countermeasures examined? What questions are used to test proposals?

All too often weak criteria and analysis are reflected in management safety action (at whatever level), which is frequently:

Re-Action	rather than	Pre-Action
1. Proportionate to recency of latest catastrophes.	" "	1. Proportionate to catastrophe potentials in the future.
2. Topical in terms of most recent catastrophes	" "	2. Designed to correct systemic failures.
3. Is perceived by some as "over-reaction."	" "	3. Balanced action proportionate to true potentials.
4. Sporadic.	" "	4. Continuous

When safety clashes with budget and schedule constraints, the trade off criteria and mechanisms are weak (this may be a failing of the safety profession, rather than management). Wilmotte (NASA, 1971) has argued that benefit comparisons tend to the short run - costs, schedules, etc., - and suggests that the longer term uncertainties, even though difficult to quantify, must be somehow made known to management. This seems a very useful point. For example, a failure to require Information Search in a Hazard Analysis Process creates great uncertainty as to performance - almost creates certainty that previous errors will be repeated and performance degraded.

Wilmotte further suggests that management require more confrontation between alternative solutions in its bases for choices and decisions.

Decision makers receive from proponents proposals which tend to state a strong, positive case for a project. The negative aspects are not emphasized or well presented. Consequently the requirement for alternatives and/or standard analytic requirements which will expose problems and obstacles are necessary.

Safety (or accidents) seem to be a harsher, long term measure of performance than any other yardstick except the long range profitability yardstick in a business. The difficulty with the budget-schedule-performance goals represented in a development or construction project is that short term accomplishment may be at expense of operational accidents, and ultimate performance degradation.

An example of inadequate criteria could seemingly be seen in a recent accident which implied that the project was expected to turn out well even though:

1. Difficult research near technologic boundaries experienced repeated failures,

- . 2. Budgets were cut,
3. Changes and delays occurred,
4. Work was transferred from a well-organized engineering group to an ad hoc group without off-setting counterchange,
5. Surveillance and review plans were inoperative,
6. Stated objectives omitted a major program,
7. Reorganization plans were held in abeyance.

Thus, functions of management (above the first level of supervision) provide the following kinds of criteria:

1. Planning and control adequacy
2. Trouble-shooting
3. Priority problem solving - depth analysis, research and study, etc.
4. Adequate work site observation, inspection, review and analysis.

An example of simplistic, inadequate criteria would be an assumption that safety is attained by compliance with codes, standards, and regulations.

Legal inhibitions and ill-founded cost criticisms are two common obstacles to safety program improvement. The management handling of these obstacles will test the adequacy and maturity of management's criteria and analysis.

Frequently the lawyers who protect organizations are quick to raise potential liability fears arising from information or analysis intended to improve safety. The objections of lawyers, if not circumvented in ways which protect both individuals and organizations, can set the stage for longer-range serious accident and liability problems. Any inhibition on program improvement is, of course, contrary to wise public policy; if not corrected voluntarily, the heavy and often awkward hand of regulation will be used by government.

Standards of judgment as to what constitutes "reasonable care" by an organization are rising rapidly. In the near future MORT and/or other forms of systems safety analysis will almost certainly constitute yardsticks as to the adequacy of safety programs (Hayes in NASA, 1971). Therefore, some lawyers are saying that the most careful search-out and analytic techniques are a best answer to "reasonable care."

A specific example of non-use of one MORT requirement is illustrative. MORT postulates use of the "Critical Incident Technique" to obtain otherwise unavailable but valuable data on near-misses and similar incidents. Use of the technique in aviation safety has an illustrious history. Nevertheless, an effort to systematically collect such reports from scheduled airline pilots foundered on legal objections. Yet techniques for protecting individual pilots and organizations are available. Thus long-range safety is sacrificed for short-range protection. Management's failure to circumvent the obstacles

suggests inadequate criteria and immaturity. (A current inquiry into an English crash has identified this same deficiency.)

Systems safety techniques in general, and MORT during its short life, have often prompted quick, unstudied criticisms, such as, "too expensive." These may be convenient labels for those who find it intellectually or administratively inconvenient to change past methods.

Cost criticisms can be dealt with in four ways:

1. Many costs, as for example, for Critical Incident studies, are marginal and negligible - the people involved continue to fulfill their regular task assignments.
2. Some improved methods are cheaper than old, sloppy methods, without even considering the injury and damage which slips through old loopholes.
3. Many systems methods are being developed in low-cost forms. (See, for example, Vesely's illustrations below, or see the Section, "Accident Investigation" which reports costs of MORT analyses.
4. Many MORT processes provide for scaling efforts to size of problem, and have low thresholds for minimum examination of any accident problem.

Again we see criteria by which management can analyze its safety program development.

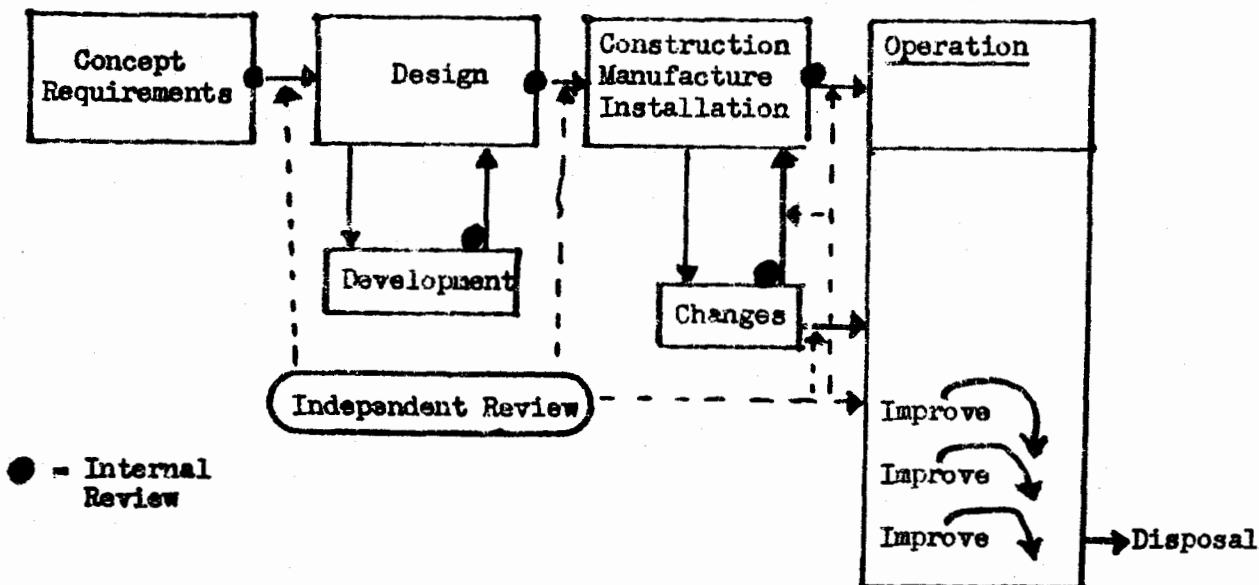
The Fault Tree has been the most rigorous analytic method, but has been vulnerable to cost criticisms. Recht has provided simple illustrations which suggest that the first requirement is intellectual, namely, the willingness to develop improved skills. Further, an Aerojet scientist, Vesely (NASA, 1971) has cited uses of Fault Trees to examine alternative approaches to reactor safety, which typically involved two man-weeks of engineering time and a few minutes on a large computer. More or less simultaneously, representatives of the regulatory function of AEC are still saying, in effect, "We've found the Fault Tree too expensive." Hardly a tolerable position in reactor safety.

Analysis. Recent events in NASA, as well as AEC-Aerojet, suggest need for specific analytic devices to discover where or how management implementation processes may fail.

The Life Cycle concept is required in the Hazard Analysis Process (Figure 20-1). In addition, events suggest its continuing use as a management device (a long wall chart, if you please) in the hope that problems, especially those with long leadtime for solution, be better anticipated.

Figure 20-1.

LIFE CYCLE SCOPE - and Numbers: Uses
Error Rates
Accidents



a2 Budgets. In general, the budgets for visible safety functions have not been amenable to simple yardstick measurements of any great value. Too much depends on what specific functions are classified as "safety" in a particular accounting system. So, without most careful definition of function, inter-organization comparisons should be treated with great caution. Of even greater significance would be the very substantial budgets for design and construction of safety features throughout the organization.

The level of budget support might be tested by listing recent major authorizations for substantial safety improvements, and listing additional protective measures not authorized. Budget records for the study or alleviation of the worst problems can be reviewed. Particularly where high-level peers constitute a safety committee, the quality and quantity of management support could be assessed by examining decisions in issues presented by such a committee.

As with other aspects of management actions shown in the MORT diagram, the measurements are in part anecdotes or case histories.

a3 Delays. These become Assumed Risks. Frequently these are routine, normal and acceptable management decisions. However, in recent months, a "Problem Postponement Syndrome" has emerged as a concept.

The organizational syndrome whereby solutions to safety problems are postponed or avoided in early life cycle phases of a project has been a recurrent concern within AEC and NASA, and the latter is studying possible controls.

In Figure 20-2, the first four phases of the life cycle of a project are shown. Needed steps in the first two phases are listed in the Hazard Analysis Process.

Under constraints of budget, schedule and intermediate mission fulfillment (e.g., construction), steps tend to be omitted or stinted, and trade off decisions tend to avoid or compromise safety. For example, fire protection of instrumentation and computers may be minimal, rather than "improved risk" which AEC requires.

In later phases, some of these may be remedied by retro-fixes, but typically with higher costs and fewer safety benefits.

This process continues down to and into the operational phase during which operation may be delayed or degraded because of deficiencies, retro-fixes and expedients, which may have higher cost/benefit ratios, or continuing deficiencies may be manifest in accidents (with further degradation of performance). Ultimate costs multiply. Final mission fulfillment may be impaired.

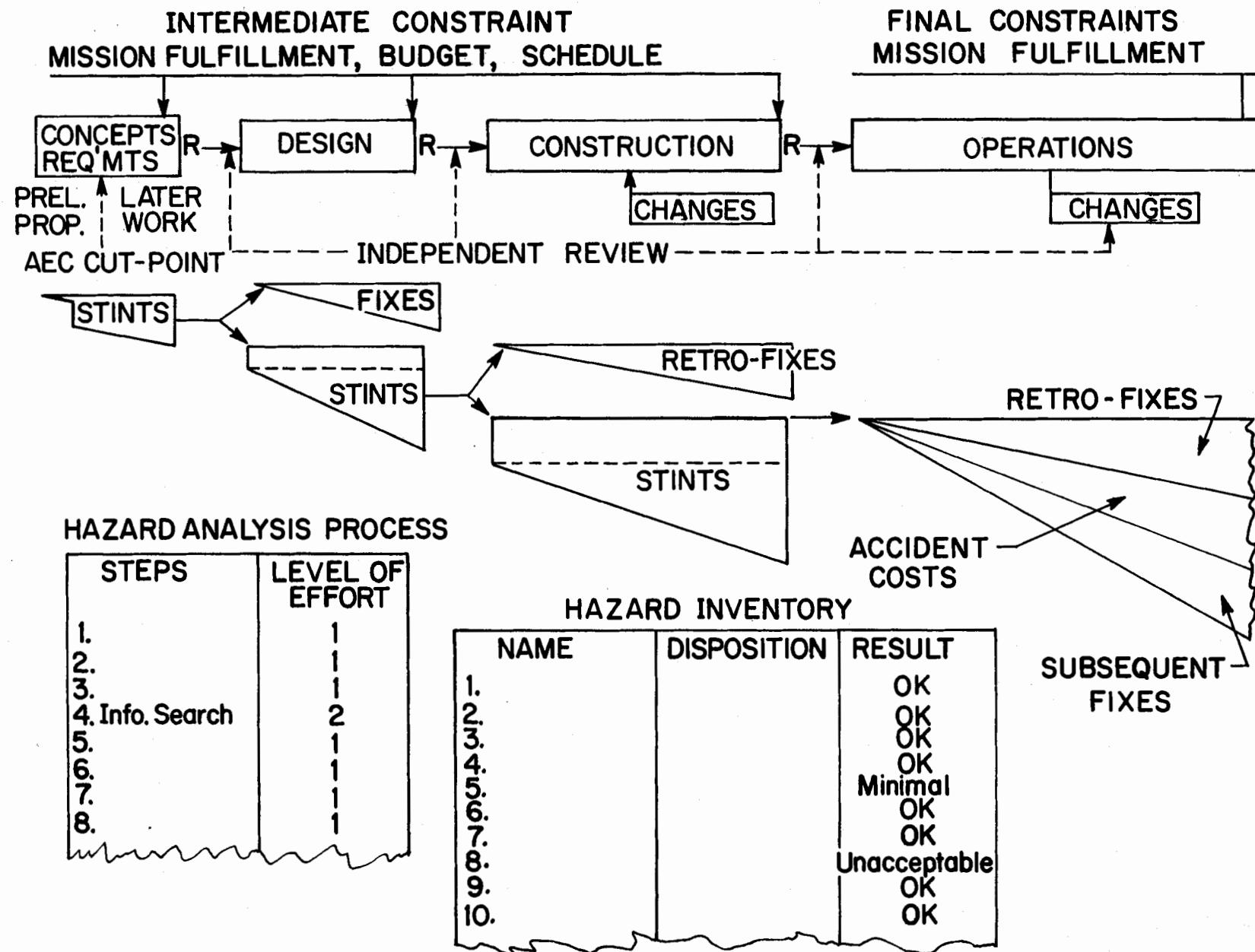
To control in some degree the Hazard Analysis Process itself, a project check list for entry of level of effort may be useful.

To control the omission of a known hazard simply because the planner's constraints prevent appropriate solution work, NASA is considering a Hazard Inventory, a catalogue showing disposition of hazards and trade offs, thus making risks visible. A NASA safety engineer suggested a long-hand docket, maintained daily, be utilized for audit or surveillance to minimize the doctored lists which may turn up in final reports.

As with a given disease, e.g., measles, it is probably useful to have a name of the common disease, in this case "Problem Postponement Syndrome," rather than just list the symptoms as if they were unique. Management's detection and cure for this disease is also a test of maturity of criteria.

a4 Line Responsibility. The safety responsibility of the line organization from the Chairman of the Board down through the first line foreman to the individual employee is made amply clear in the outstanding safety programs. Written terms of reference, consistent with the safety policy, are almost universal. And it follows that safety performance is a consideration in promoting an individual to a better position.

Figure 20-2.
PROBLEM POSTPONEMENT SYNDROME



Aerojet places primary responsibility for safety analysis on line management.

In seeking full participation in the safety program by the entire management organization, there are three mutually reinforcing approaches:

1. The basic line responsibility.
2. Clear assignment of functional responsibilities for appropriate elements of the safety program to various departments, e.g., engineering, maintenance, research, training, finance, transportation, etc.
3. Management safety committees or review boards, chaired by senior executives, with revolving representation from various levels of supervision.

These three kinds of arrangements, with top leadership, can create a team approach.

The use of management committees could be seen as interference with the line process. However, they seem to have had considerable influence on peers, and probably should be retained as a criterion of program until other criteria emerge as more significant.

Considering the importance of line responsibility, accident reports are remarkably silent on the relevant actions or failures to act by upper and middle management. Pertinent questions might be:

1. When did higher supervision last review plans applicable to this area? What was found?
2. Have requirements, time or budget for hazard review processes changed? When? How?
3. When did higher supervision last inspect this area? What was found?
4. When did higher supervision last review the supervisor's inspection reports? What was found as to basic causes of unsafe conditions? What was done?
5. Describe the monitoring or work sampling plans used by higher supervision to audit performance.
6. When did higher supervision last discuss safety with the supervisor? Describe what happened.
7. Give instances of help given the supervisor by higher supervision.

a5 Staff. Examine provisions for assigning and implementing specific safety functions to staff departments, such as: engineering, maintenance, purchasing, transportation, personnel, training, health, security, quality control, etc.

Firenze (1972) has recently organized the essentials of a hazard control management effort in a system much similar to the general safety system (Figures 11-1 and 11-2). He uses his concept to effectively argue that the effort

cannot be carried out by the safety staff, but requires cooperation of all management subsystems--including manufacturing engineering, quality control, purchasing, maintenance, industrial relations, finance, and medical. More important, he provides lists of typical functions for each in analysis and investigation; improvement plans and implementation; audit; research development and testing; provision and maintenance of adequate materials, equipment, personnel and environment; information procurement and processing; and financial practicality and performance.

a6 Directives and Organization. Implementation of safety policy in detailed directives can be examined. Clarity and use of schematics and flow charts can be criteria. Observation suggests that directives may be overly concerned with specific rules for kinds of hazards, rather than the functions of hazard review, monitoring, etc., again the distinction between method and content. Also, directives tend to over-react to past events and under-react to future potentials.

The MORT Trials have made an unexpected contribution, very likely of considerable significance, to the concept of how error-free procedures can be developed and published. In the earliest stages of monitoring upstream processes, Clark and Alvord of Aerojet detected significant process gaps and failures in the initial walks through various processes, despite the extensive proceduralization documentation of Aerojet. Interestingly, the scientific literature, e.g., Berelson & Steiner (1964), shows that step-by-step procedures are better understood than text paragraphs. The episode above led the Reactor Operations Division Manager to rework and revise his administrative methods. Figure 20-3 shows the method which evolved from the trials: block functional diagrams, steps to fulfill each function, and criteria for knowing when the step is well done.

One strongly recommended step in studying the usefulness of the MORT approach is a simple walk-through of the process for producing the design and plan for a project--almost universally a need for better criteria and arrangements, and a better statement of such, is quickly detected. The work situation is often error-provocative.

In preparing directives for work processes in the function-step-criteria form it is important to note and include those things which are being done in ways better than previously specified. The process gaps which are filled by informal communications are a little more difficult to handle. On one hand, it seems almost impossible to specify the intricate web of useful communications. On the other hand, accident reports reveal what happens when such

Figure 20-3.
BETTER PLANS AND PROCEDURES

REDUCE

CONFUSION

OVERLAPS

GAPS

MISSUNDERSTANDING

OMISSIONS

OBSCURITY

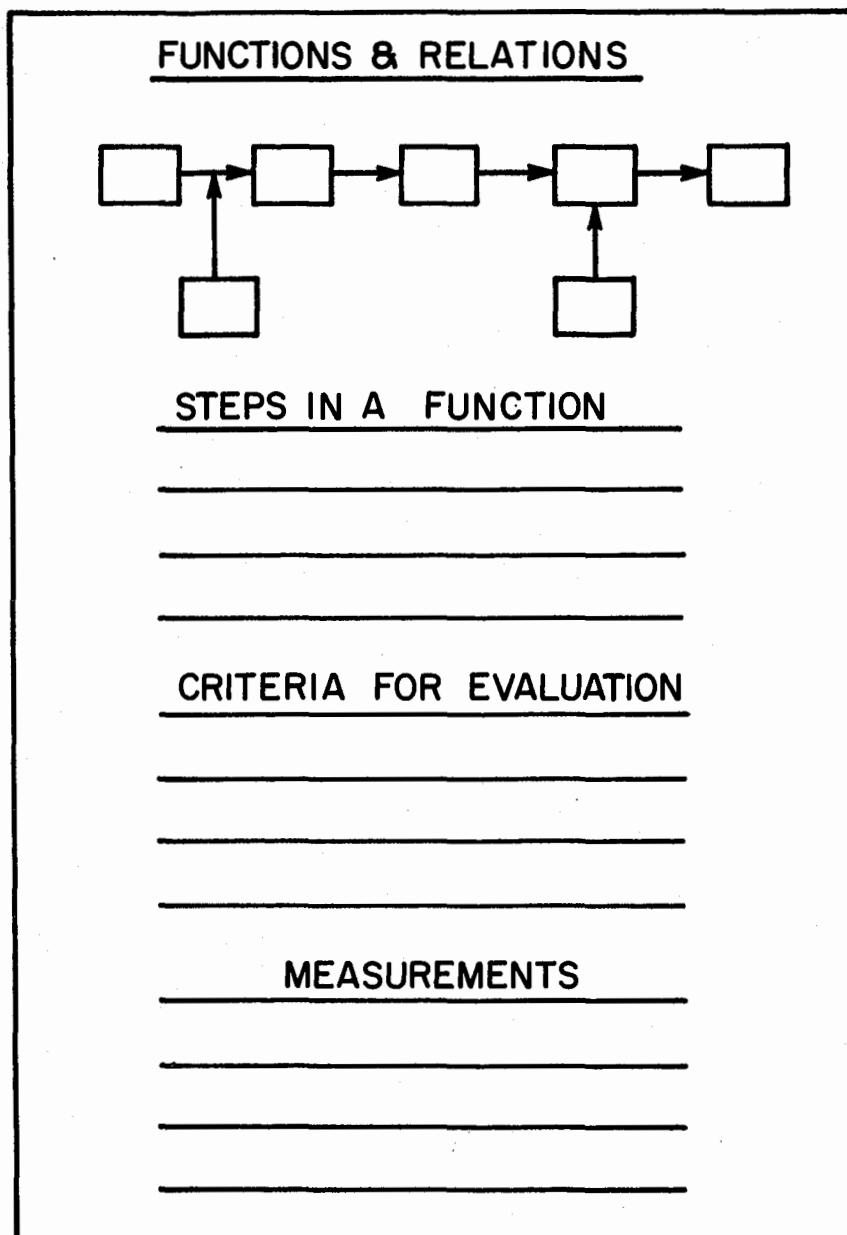
COMPLEXITY

MINIMIZE

LEGALISTIC
JARGON



SCHEMATICS



CLARIFY

SIMPLIFY

INTER-RELATE

COORDINATE

ASSIST

- 194 -

* FOOTNOTES =
DETAIL, CASES,
LEGALISTIC
EXCEPTIONS, &
INCLUSIONS

networks are damaged by a change in the personnel. The question--is it necessary and important to safety?--will probably give the best guidance.

While the superiority of some organization forms over others can hardly be denied, there is a safety-related requirement to make almost any organization work. Thus the art of management may make use of such specific ad hoc devices as project teams, special assignments, matrix forms of organizing, and complex webs of sociometric relations to achieve performance. In short, an organizational deficiency should not be seen as a causal factor correctible only by reorganization. The schematics described in Figure 20-3 reflecting informal as well as formal arrangements can adequately handle processes which are interdepartmental and complex.

Additional examples of schematics used at Aerojet, such as development of procedures and OSHA variances are provided in Part VII, Work Flow Processes in a discussion of the upstream processes which govern quality of work site ingredients.

a7 Training and Assistance. Although we talk of the role of the supervisor as the "Key Man" and discuss supervisor training, we should be aware that the chain of responsibility should be unbroken at all levels of supervision. In principle, the supervisor training program has reached all levels because the higher ranking executives came up through the ranks, or were affected by peers in safety committees or decision making. Therefore, "management training" might be more appropriate.

Formal training programs are universal in the most successful companies. The programs can be seen in four types:

1. General programs in management and supervision,
2. Specific technology,
3. Human relations and communications,
4. Safety.

Most of the larger companies have their own safety training programs. The National Safety Council has produced a variety of programs which have been widely used: instructional methods include films and text, class and home study, and programmed learning. Some NSC courses combine human relations and safety, which has been a "two for one" deal.

Management associations, vocational schools, community colleges and state labor departments make available a wide variety of courses. Recently, community safety councils have intensified their supervisor training offerings. Considering the critical importance of the training needs of smaller establish-

ments, there is no substitute for a comprehensive network of training opportunities.

DuPont makes the major point that on-job experience is the primary source of training, particularly the boss's example. If then the management process for hazard control conforms with sound principles for management of any problem, the efficacy of on-job experience can be enhanced.

Relations (including some friction) between successive echelons of an organization, as well as between safety and operating personnel, suggest that the role of service be increased vis-a-vis the role of policing. A useful concept holds that a deficiency at one level is mirrored by a service deficiency at the higher level. Thus, an accident or the finding of a hazard should prompt three kinds of action:

1. Correction,
2. Reexamination of the prevention process,
3. Reexamination of higher-level services to increase effectiveness of the prevention process.

A method of appraising safety services provided from one level to another in a multi-layer organization, or from staff to line at a location, consists of listing the major technical operations of the organization, and then for each listing and evaluating service under the following categories (Johnson, et al, 1957):

1. Research and fact-finding.
2. Exchange of information - periodicals, bulletins, meetings.
3. Standards and recommendations.
4. Training opportunities.
5. Technical assistance on problems.
6. Program aids.
7. Measurement of performance.

At Lawrence the safety function is very heavily oriented toward a service role, and this seemed especially useful under university research conditions.

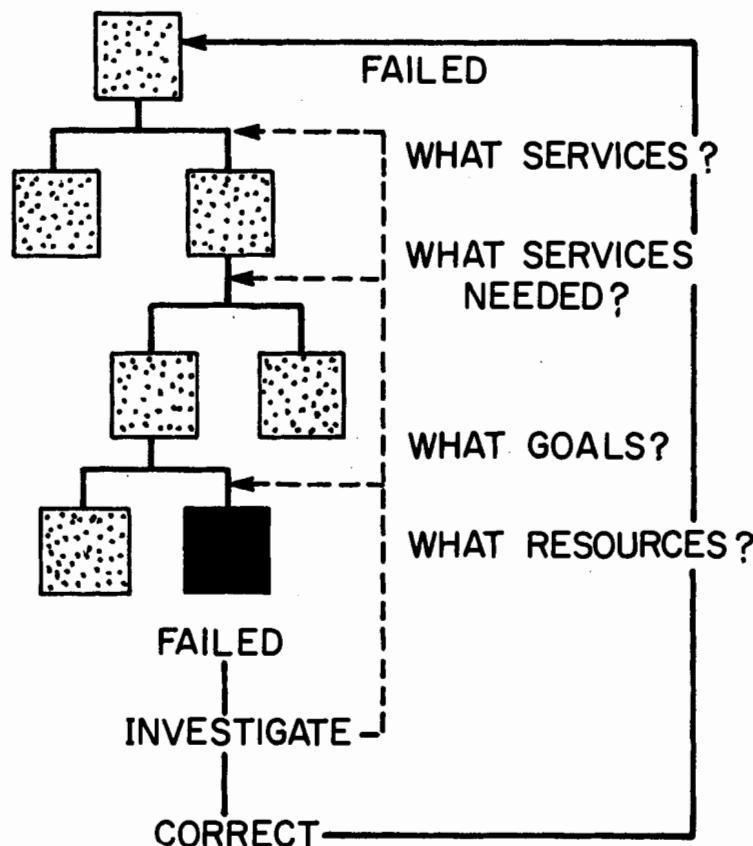
Figure 20-4 attempts to show the service deficiency process as it occurs in organizations, and accidents which reflect the deficiencies are not hard to find.

A discussion of low cost, efficient production of services using production-line approaches is included in Part IX, Safety Program review.

If management allows a project form of organization (as contrasted with use of the on-going, presumably well organized staff departments), there is a

Figure 20-4.

FAILURE MIRRORS FAILURE:



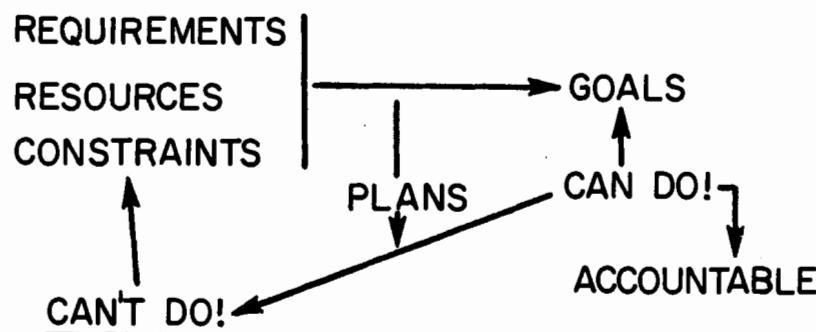
* IN SERVICES AND ASSISTANCE

- 1) RESEARCH AND FACT FINDING
- 2) EXCHANGE OF INFORMATION

3. STANDARDS OF JUDGEMENT

 - 4. TRAINING
 - 5. TECHNICAL ASSISTANCE
 - 6. PROGRAM AIDS
 - 7. MEASUREMENT OF PERFORMANCE
 - 8. COORDINATION

* IN PLANNING EVALUATION



special management responsibility to see that the various safety and review functions are adequate and well run.

a8 Accountability. Although a policy of holding supervisors accountable for safety function is commonly reported, the method of measuring such performance is far from clear. For example: What criteria are used to evaluate high rate exposures, such as maintenance, versus low rate functions, such as office work? How attain statistical reliability in comparisons? How interpret "bodily movement" accidents, such as walking or ordinary lifting, in the absence of clear cut, effective, and management-approved prevention programs?

Accountability without an appropriate control standard may have a negative effect on supervisor attitudes.

Peterson (1969) provides a useful checklist of facets in developing accountability: accounting for costs, appraisals, and measures of program, including sampling. Unless the supervisor is provided with information, training and aids, accountability may be capricious and unfair.

a9 Feedback. Accident investigations reflect prior lack of feedback to management on actual operating conditions. Lack of feedback may allow hazards to go uncorrected, or may inhibit supervisory attainment of safety goals by routine, good administration. Much evidence exists that lack of feedback is also a cause of performance problems. Therefore, the development of a defined feedback system is a criterion of management implementation. (A more extensive discussion of Monitoring is in a later section.)

The reporting upward of budget restrictions and delays (which create assumed risks) should be particularly examined and a formal plan for reporting worst potentials or priority problems appears to be a need. Otherwise only good news floats up.

In many organizations, non-safety, general operating control data and monitoring systems have become well-developed (but probably not so for R & D work). In any organization, management's criteria for measuring general performance should be systematically and carefully reviewed for safety implications; that is, do weak points in general operations reflect adverse situations which also affect safety?

During the trials at Aerojet, it became clear that some incidents were due to deficiency in ordinary channels of reporting. This led to an effort to specify the needed redundancy in managerial control systems.

The executive at a higher level requires redundant sensing systems if he is to have assurance that his systems are operating properly and are not failing.

The first level of redundancy consists of the normal line management channel and the parallel information channels from independent agencies such as Safety, R & QA, and management control or audit. (These latter may all be operating, but without unnecessary duplication of functions.)

On the first of these two, the line channel, four types of information should be required:

1. The normal line channel of authority, requirements, resources, goals and progress.
2. The system was operating properly. (This may be determined by audit, in which case the report may say "with the following exceptions which are being corrected.")
3. The system is not failing. (This may be determined by one or more of a variety of monitoring devices - RSO studies, surveillance, search out, accident/incident data, etc.)
4. Higher level verification, particularly when the above signals are not received, or are impaired.

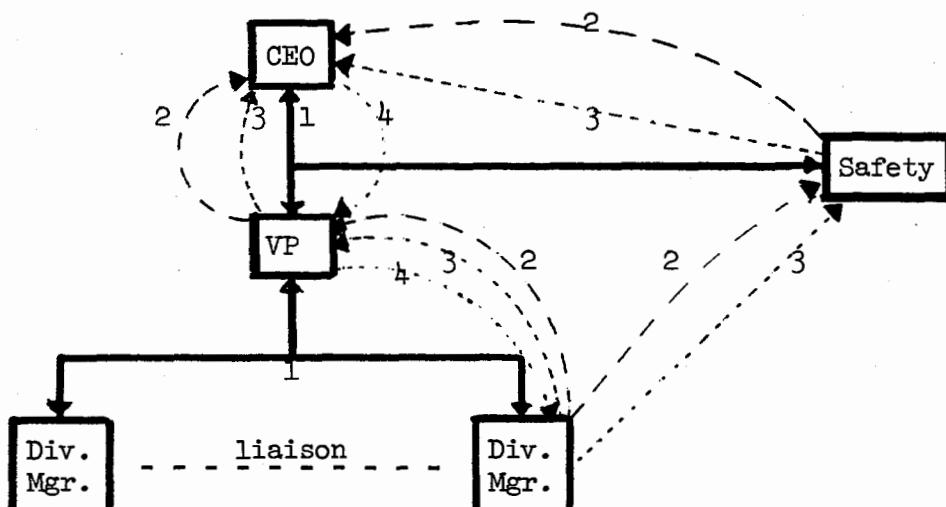
On the redundant channels, information of types 2 and 3 is required.

At the higher management level the red signal light should glow whenever any report (of six) has failed to arrive, or a negative report is received.

If an intermediate level of management has been impaired by extended absence on other assignments (as in a recent accident), the higher level of management must secure the needed information.

The types of information flow are then:

Figure 20-5. Management Safety Information Flow



Vital feedback is also provided by the Risk Assessment System and its Information subsystem. This analytic format should show that

management's criteria and analysis must ensure that bad news about risks and uncertainties flows upward early for corrective action, rather than after the failure.

Bad news may be withheld if higher management responses are adverse - e.g., "Why didn't you clean it up a long time ago?" Problems are difficult, or they would have been cured long ago. A proper management reception, a view that a problem report is an opportunity to give help, may be essential to the free, upward flow of needed information.

also Vigor and Example. Vigor and example are difficult to measure.

Leading corporate safety programs commonly have anecdotes of direct, personal action (above and beyond the routine) by top executives. This is obviously an imperfect and unscaled yardstick, but nevertheless a vital and revealing criterion.

At Lawrence, a little inquiry produced an appropriate example: Dr. John Lawrence was known to check employees for film badges (radiation monitoring devices). If the employee did not have the badge, Dr. Lawrence is said to have explained the purpose and promise to personally escort the violator off the project in the event of a second violation.

Interestingly, a repeated use of illustrative anecdotes at another research site produced no tales of management vigor, and this was a site later criticized by AEC as the worst of its type (although still good by conventional standards).

At a third site, the anecdotes frequently told involved a manager long gone from the project, and the program seemed to lack strong drive.

A small number of such examples of management concern may do as much for safety as policies and specified standards. Therefore, an effort to unearth such tales seemed to produce positive or negative indications of the depth of management conviction.

A few of the anecdotes used in the exploration of vigor will probably be useful.

The Chairman of the Board of AT&T stopped his car to call a lineman off a pole to explain a safety procedure, and to reemphasize why safety procedures are important to both employees and the company. The news of this event crossed the country at the speed of light!

Another example demonstrates the role of the manager and the safety professional, as well as vigor.

A senior executive of one of the largest oil companies described his attitude and action when he managed one of the world's largest refineries in the following terms:

"When I was shaving in the morning, I asked myself, 'What can go wrong?'

"When I stopped at a traffic light, I asked myself, 'What can go wrong?'

"When I got to the refinery gate, I phoned my office to say where I'd be, and then I went to the place where something might go wrong.

"I usually found that matters were properly controlled, but if not, prompt action on potential trouble not only stopped the trouble, but also projected a management concern throughout the refinery. Even if there wasn't trouble, I found that my concern was known, respected, and mirrored at all management and employee levels.

"If the refinery burns, the President calls the manager, he doesn't call the safety director."

The Reactor Operations Division Manager at Aerojet provided confirmation of the importance MORT attached to this factor of vigor.

If management vigor is such an important factor, it would be nice to have a definition, as well as illustrative anecdotes. Webster uses the following phrases:

1. "Active strength or force of body or mind."
2. "Intensity of action or effect."

Our definition of management vigor in safety will have to specify some additional aspects, such as:

3. Directed force - a high sense of safety values.
4. Hazard recognition
5. Search-out
6. Certainty that what can go wrong, will go wrong.
7. Fast action at potential trouble spots.

In short, the vigorous manager will display a "killer instinct" for hazards.

It is increasingly possible to frame objective questions about management vigor, coupled with management maturity:

1. Does management have a list of residual risks or worst potential problems? Are good studies available for these? What's being done?
2. When was safety policy last reviewed? When last enunciated by top management?
3. What safety actions have recently been taken? Were any of these taken despite some internal opposition? List the last six major safety proposals and show whether they were approved or disapproved. Do the same for collateral areas - training, maintenance, engineering, etc.
4. When did management last formally assess the trend of accident rates and other indices of safety performance? What action was taken when trends were unsatisfactory?
5. Has management assessed its feedback systems in terms of the last four serious accidents/incidents?

The System Fails. Early in the MORT text, the view of the human factors specialists - accidents occur when the system fails - was articulated. However, repeatedly in accident or error investigation, the question of blame is arising. Therefore, the point is being repeated in a number of schematics - management methods, management assistance, as well as in accident investigation - the system fails.

Any system should be designed to be operated by reasonably competent people of the types available, not super-men. To the degree a system relies on excellence above the levels of reasonably available competence, the system will fail. The job of management is thus presented as making good people better, helping people grow in competence and performance.

Views that it is systems that fail and that people require help and assistance need not be weak nor fail to challenge people. Rather the desired vigor of management can display concern, but also be directed into counsel and assistance to develop the people.

* * *

A useful overview of management's role in general occupational safety practice is provided by the ratings of program aspects by 100 leading experts. (Planek, 1967.)

Rank Order of Major Safety Program Area

1. Supervisory Participation
2. Top Management Participation
3. Engineering, Inspection, Maintenance
4. Middle Management Participation
5. Screening and Training of Employees
6. Records
7. Coordination by Safety Personnel
8. Motivational and Educational Techniques

Top Ten Activities

1. Enforcing safe job procedures (implies written definition)
2. Setting an example by safe behavior
3. Middle management setting an example by behavior in accord with safety requirements.
4. Training new or transferred employees in safe job procedures
5. Making safety a part of every new employee's orientation
6. Top management setting an example by behavior in accordance with safety regulations

7. Top management assigning someone to coordinate safety on a full or part time basis.
8. Including safety in supervisory training courses
9. Top management publishing a policy expressing management's attitude on safety.
10. Advising management in the formulation of safety policy.

It is interesting that "motivational and educational techniques" was ranked last among major areas, but that "setting an example" (perhaps the strongest motivational force) accounted for three of the top ten activities.

A study (Allen, 1965) concluded:

"effective management action is the key to controlling and reducing industrial accidents. The quality and quantity of management efforts in the promotion of safety are decisive in motivating employees to accept their personal responsibility for the prevention of industrial injuries."

In 1964 the author reported on criteria used in judging a safety competition among Federal agencies as follows:

Management leadership

1. Did a published policy issued by the agency head exist throughout the contest year?
2. Is the agency policy clear, concise, direct, and all-inclusive in scope?
3. Is the agency policy broadly publicized to assure that it is known and understood by all concerned?
4. Is basic policy supported by guidance and instructions concerning organization, scope, responsibilities, functions, personnel, standards, and awards?
5. Is the agency adequately staffed with safety personnel to assure a continuing safety effort? Headquarters? Subordinate echelons, activities, and units?
6. Has agency provided adequate funds for aggressive and continuous safety programming?
7. Does the agency have operating safety rules and regulations?
8. Does the agency support the Federal Safety Council in holding offices, attendance at meetings, and committee in project activities?
9. Are program objectives established and areas of special emphasis identified on an annual basis?

10. Are program objectives and performance reviewed and analyzed at regular periodic intervals?
11. Has top management given adequate expression of its interest and support of aggressive accident prevention throughout the year?
12. How often are regular and special reports on the agency accident record prepared for and reviewed by top management?
13. Does top management follow up on departments or units with poor or unacceptable accident records?

Assignment of responsibilities

1. Do organization charts reflect a clear-cut line of organizational authority and responsibility?
2. Do program directives relate the line of normal organizational responsibility to the agency program to prevent accidents?
3. Do agency instructions identify responsibility for funding, assignment of personnel, organizational placement, functions, reviews, councils, programming, and coordination?
4. Are duty requirements (responsibilities) of safety personnel at all levels spelled out in details?
5. Are safety responsibilities of all headquarters staff elements clearly delineated?
6. Are the safety responsibilities of first-line superiors and employees emphasized?

Further criteria used in the competition may be useful in considering the depth and quality of the Federal government's internal safety effort, as well as in developing criteria for a general examination of safety program measurement. These are listed in Part IX, Safety Program Review.

This page intentionally blank

21. RISK ASSESSMENT SYSTEM

Ga3 Risk Assessment System. The MORT charts postulate a risk assessment system with the following elements:

1. Comparison with Goals.
2. Experience Data
 - a. Rates
 - b. Causes and circumstances.
3. A Hazard Review Process with three factors:
 - a. Triggers to activate hazard analysis,
 - b. Knowledge and information on hazard reduction,
 - c. An adequate Hazard Analysis Process: definition showing analytic operations to be performed.
4. Safety Program Review.

Before examining specific criteria under the four headings, the purposes and processes of a general risk assessment system should be examined. Background discussion from Phase II follows.

The primary objectives of a risk assessment system should be to provide a manager (at any level) with the information he needs to:

1. Assess residual risk, and
2. Take appropriate action, if he finds residual risk unacceptable.

Important, but secondary objectives would include:

3. Comparative evaluation of two or more units,
4. Research evaluation of two or more hazard reduction schemes to add to the "state of the art."

Discussion of measurement of occupational safety performance has been focused on questions 3 and 4, and not enough on the first two, primary questions.

Repeating a basic view expressed earlier:

"Since management (specifically the Chief Executive Officer of the organization) has legal and moral responsibility for safety, it seems to follow that safety information and measurement programs should be primarily designed to answer the critical safety questions of management:

1. What are the nature and magnitude of the organization's accident potentials?
2. What has been done to reduce risk?
3. What is the long-term level of residual risk?
4. What additional measures to reduce risk have been considered and rejected on "practical" (Investment/benefit/value) grounds?
5. Are the safety programs actually operating as described in manuals and procedures?"

It has been argued that "safety performance" means "performing a job without undergoing or causing injury, damage, or loss." This may be satis-

factory, as far as it goes, but if we specify that the past must also be predictive, we broaden the requirements in terms consonant with management's responsibilities and information needs. But it is precisely the predictive value that is hard to develop.

A viewpoint of safety measurement of potential significance to managers has been articulated for airline accidents in terms of the adverse effects of number of catastrophes (not rates) on public confidence (Lundberg, 1966). Translated into occupational terms, this implies that the number of major events (death, multi-death, major fire, explosion or other disaster) will govern confidence in the manager by his superiors or others outside the organization. This view seems consistent with the managerial trauma which appears to follow serious accidents. Consequently, the strong emphasis in trial procedures has been placed on limiting severe consequences, and lesser emphasis on the less severe injuries which make up the conventional frequency rates.

A concept of needed long-term measures (for an organization or a person) in terms of system effects is:

- | | |
|--|---------------------------|
| I. "Non-survivable" events | "Catastrophic" |
| II. Degradation of performance | |
| A. "Non-survivable" in major parts of the system | "Critical" |
| B. Major degradation in parts | "Major" |
| C. Systemic degradation of the whole, symptomized by frequent degradation of parts | "Minor"
(but frequent) |

Such a concept should be carried over into the risk assessment system in both rates and predictions.

The remainder of this Chapter covers three topics:

1. Goals--policies and criteria used to assess risk.
2. General System for Assessing Organizational Risks--a model for periodic review of an organization as a whole.
3. Analysis of Project or System Risk--two models for evaluation of a specific activity.

Goals

The development and articulation of goals in occupational safety has not been consistently and sufficiently well done to provide strong, viable criteria at times of risk assessment. Consequently, occupational safety suffers in trade-offs with more specific, quantified, short-range, "practical" goals.

Goals are of two types having increasing specificity for risk decisions:

1. Policy and Implementation criteria--management approaches, broad goals, and risk assessment methodology.
2. Project specific data.

Despite the supposed force of policy and management criteria, the project specific data are likely to prevail in practical decisions under pressures, and safety frequently comes out second best in these trade-offs. This indicates two kinds of developmental needs: (1) more usable statements of policy, criteria and risk assessment methods, the context for risk decisions, and (2) better hazard analysis to compete with quantified data on non-safety trade-offs.

Policy and Implementation Criteria. These can probably by crystallized in three categories to clarify relevance to specific risk assessment:

1. Context of work--Are management policy, methods, directives, error-reduction policy and services, consistency and strength of support for safety and reliable control of work such as to define the environment in which a project will be carried out? (How are questions raised in Chapters 19 and 20 seen by project risk assessors?)
2. Broad goals:
 - a. Is the organization's goal limited to legal compliance? Or, does it seek higher degrees of safety? Are investments in safety going well beyond the minima of codes, standards and regulations commonly authorized?
 - b. Is the organization's goal seen as control of accidents at past levels? Or is it working toward a breakthrough? Are goals quantified in probability terms?
 - c. Risk assessment excellence and methodology, as specified by management, may be such as to force searching and thorough examination of factors in risk, or a lack of specifications may permit superficial, poorly considered decisions. Affecting quality of study are the definitions of hazard analysis process, life cycle concern, and the requirement for analysis of alternatives and their trade-offs, and the quality of independent review agencies and their criteria.
3. Project Specific Criteria--the criteria immediately before those who must assess risk and make decisions.
 - a. These involve the sometimes conflicting criteria of cost, schedule, reliability and quality assurance (usually, not always, favorable for safety), maintainability, and marketability--and safety--and long-term profitability.
 - b. It is usually less difficult to resolve trade-offs within one of these competing areas than between the areas.

c. Safety data for a variety of alternatives is more likely to be of high quality and to provide a desirable flexibility in trade-off considerations.

d. A difficulty occurs when safety data are less than conclusive.

Information may be in broad categories, such as:

- (1) Codes, standards and regulations,
- (2) Recommendations--a partial consensus (e.g., in the NSC),
- (3) Limited study and known precedents,
- (4) No known precedent or study, but presumed hazard.

The first two will ordinarily be followed and very frequently, the third. Both the third and the fourth classes will be jeopardized and easily put aside if trade-offs of any strength appear.

e. General phrases, such as OSHA's "free of recognized hazards ... generally recognized in the industry," and "potential for causing death or serious injury" are relevant and binding, but suffer from the same lack of specificity as the term "practical."

The problem of defining safety levels is obviously difficult. One method of defining goals might be conceptualized as follows:

A level of "all practical steps" to reduce hazards is attained when residual risks have a series of alternative reduction measures which had to be rejected after an Investment/Benefit/Value/Threat analysis.

This requirement would enable management to follow the sound practice of testing the extremes and pulling back.

f. Some criteria are in areas difficult to quantify--an example is the trade-offs between "reliable control of work" and "freedom of researchers." Researchers indulge in a certain amount of flag-waving on this issue--"reliable control of work" can also mean good research! But, external rules and procedures are resisted by some researchers, often by those who shortly destroy the equipment or kill someone. Management (perhaps the lab director) does, however, by word or deed, have to put his weight on goal and direction in this kind of area.

Control vs. Breakthrough? Goal definition in terms of an order-of-magnitude improvement is relevant primarily to the general assessment of organizational risks, rather than a specific or project risk. However, even in the latter, it can be asked whether a project is designed to meet the higher goal.

The system approach clearly implies that short and long range goals have been established for safety. The setting of defined goals, qualified

by numbers where at all possible, has a number of advantages:

1. It makes visible the risks we are willing to accept.
2. It helps measure progress.
3. The degree of challenge in the goals helps determine the kind and amount of resources we will need.

If a goal is to halt accident increases, or to get a 10% reduction in accidents in ten years, we can make plans. If the goal is a 50% reduction in five years we shall make a rather different plan. The latter goal is likely to involve major changes and will therefore demand major study and plans.

There are said to be S-shaped "Growth Curves" which tend to describe product and service cycles in any organization. A slow rate of progress characterizes introduction of an innovation, then a longer period of straight line growth is terminated by a progressively decelerating rate of improvement. If the occupational accident rate is the inverse of the growth in acceptance of occupational safety ideas, the rate patterns of the past 10-15 years would fit an S-curve assumption.

The "Growth Curve" notion holds that a breakthrough to a new cycle of progress is just that--a breakthrough, something new has been added--and is not attainable by a simple increase in effort.

In Chapter 11 Juran's concept that a breakthrough goal is attained in a distinctive manner was outlined. Juran has defined Control as change prevention and Breakthrough as change production, or as we would say, "counterchange production."

In the Aerojet trials a breakthrough issue emerged, namely, pace of improvement. Aerojet has an excellent program, but wants to have the "best safety system in the world." Under budget and general mission constraints, what proportion of resources (including management attention) can be given to safety program improvement? A difficult, very practical question. Endeavoring to formulate the issue in objective terms, two questions emerge:

1. Goal - What degree of excellence should be attained when?
2. Practice - What additional management attention, budget and other resources are being directed to safety program improvement? What is being done to involve and activate all personnel in an upgraded safety effort?

Goal definition is a facet of measurement as well as risk assessment. The magnitude of effort can be assessed in terms of goals. It has been said that many small gains can be made by "tinkering" (not a very good word for

safety) and in general this can be done by line organization. Major gains usually involve more sweeping changes, and require in-depth staff study.

During the NSC Measurement Symposium, one group said:

"In order to design effective measurement programs it is necessary that:

"First, Goals must be clearly defined, including conflicting or potentially conflicting goals of the system or organization. We need these statements in order to judge trade-offs.

"Second, the information required for a decision must be known, or at least defined. It is at least helpful, and perhaps necessary, to know what information decision-makers are likely to use when decisions are made."

Attaining Major Goals. In a complex organizational situation, many steps in parallel and sequence will have to be taken to reach a major goal. The charting of such steps, their relationships and their time requirements by PERT Charts are an aid in planning and assessing progress or risk.

Milestones, points at which progress is assessed, are commonly lacking in occupational safety. The safety effort moves along on the basis of trying to "do better." Or, short-range program goals, such as starting a contest, or developing an inspection schedule, become the focal points of efforts. Milestones - for example, annual or phase review of a five-year plan - can provide the essential measuring points.

The actions taken after disastrous events often constitute the setting of major improvement goals. Goal formulation before disasters seems the more rewarding approach.

Thus we have yet another aspect of measurement - the development and status of plans for attaining major goals. When were they last assessed by top management?

Probability Goals. The willingness and ability to quantify safety goals seems essential to risk assessment for major progress in risk reduction. During this study, probability values were found to be used on several major projects. A possible conceptualization of goals in terms of three levels is emerging:

1. The general levels of all U. S. work.
2. The level of "present best practice," as in AEC operations.
3. Future design goals or targets.

Such goals, stated as probabilities in injury per man-year, could be expressed as follows:

	U. S. Work	"Best Practice"	Design Goal
Death	2×10^{-4}	3×10^{-5}	1×10^{-6}
Disabling Injury	3×10^{-2}	1×10^{-3}	1×10^{-4}

Converted to a guideline, such values would permit management to say: In designing process or work, endeavor to lower risk to 1 in a million (deaths per man-year), thus we can improve on present "best practice." If the nature of work is especially hazardous (e.g., some research work) and cannot be improved, the general work risk in the U. S., 2 deaths in 10,000 man-years should be considered a ceiling we shall not knowingly exceed. (This latter statement may not be acceptable, but is given to demonstrate a method.)

Other examples of probability goals will be found on page 4 and in the project models later in this chapter. Such goal quantification is increasingly practical and efforts toward this end should be pressed.

General System for Assessing Organization Risks

A model or plan for the periodic (preferably monthly or quarterly) assessment of an organization's risks is needed to design an information system which will fill management's needs. Use of conventional frequency and severity rates, grossly inadequate and frequently misleading, has been so pervasive that an improved model is needed to define the other kinds of data which are more significant.

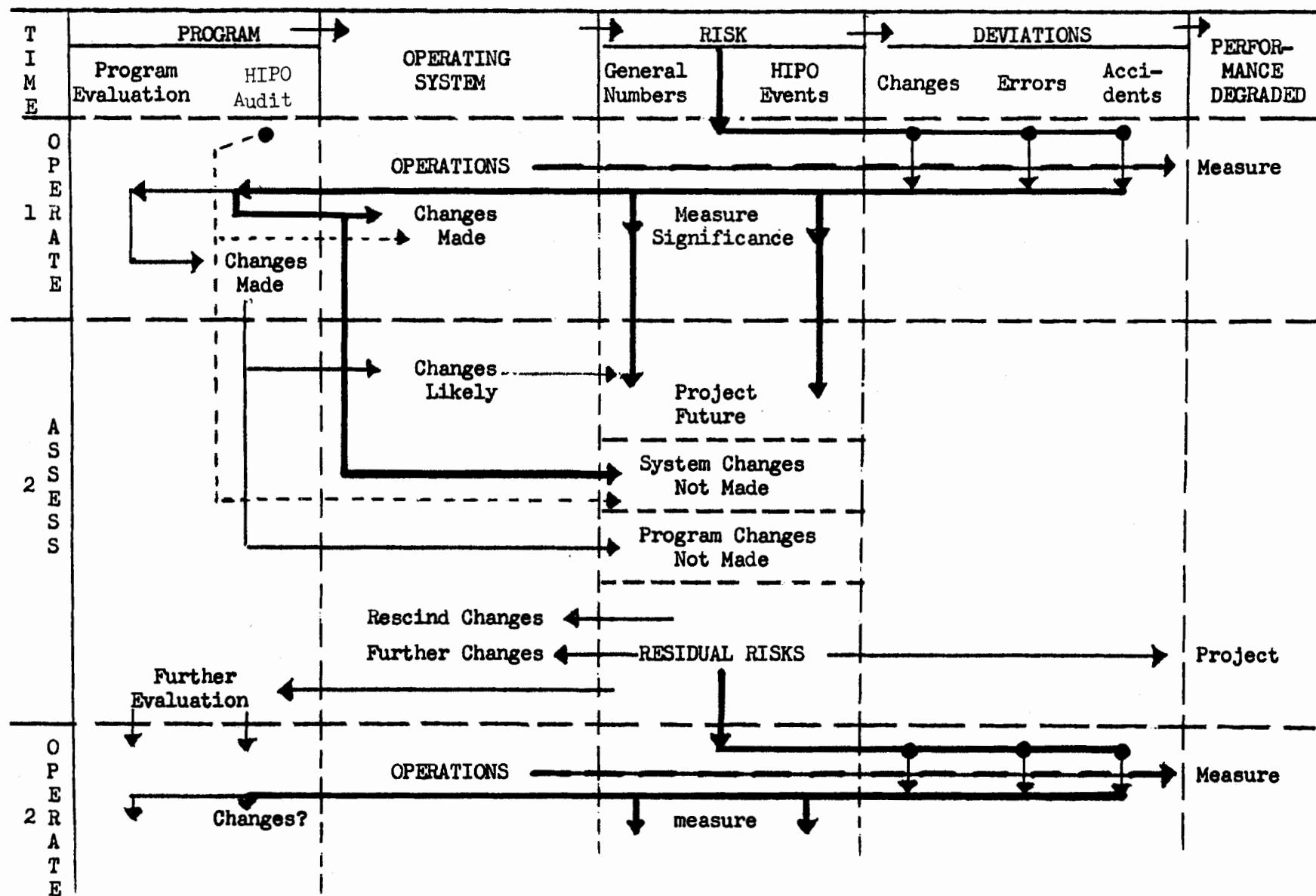
A manager (at any level) appears to need five general categories of information to assess residual risk:

1. High Potential Situations--audit of the degree of control.
2. Planned Changes (new plant, equipment, employees, or procedures)--the quality of the Hazard Analysis given to changes.
3. Current HIPO Deviations--changes, errors and accidents, and preventive countermeasures taken.
4. Long-term and Short-term Assessment of Accident and Error Rates--numbers, costs.
5. The Safety Program--what is it, is it operating as intended, and wherein does it fall short of ideals?

A model for providing these kinds of information and indicating decision points is diagrammed in Figure 21-1. In the trials at Aerojet, the construction of the risk assessment system has generally followed the model.

The collection of data on deviations--changes, errors, and accidents--is described in great detail in Part VIII, Information System, particularly Chapter 37, Monitoring, and 41, Measurement Techniques. These cover both (1) High Potential Events--managed by the name of the event, and (2) projection of general group numbers.

Figure 21-1. GENERAL SYSTEM FOR ASSESSING ORGANIZATION RISK



The events of interest (both HIPO and general) should have also been the basis for hazard analysis. The manager needs to know what changes were then made in the operating system to lower risk, and what potential changes were not made (and if any changes are still under study). He needs this information on individual HIPO events and in summary for general events in order to assess the probable effect on future risk projections.

The events of interest also monitor the hazard reduction program itself. Why did the deviations slip through the preventive network? Taken in conjunction with evaluative studies of the program, the events become the basis for changes in the hazard reduction program, and these are anticipated to produce likely future changes in the operating system to further lower risk. Together with potential changes not made in the program, the manager has a further basis for modifying the projections of future risk.

Audits of high potential situations, such as high energy departments and activities are also shown, and would have effects on the operating system. Accident experience during the trials reflects this need.

Four kinds of data then form the basis for the assessment of residual risk for future operations:

1. Projections of past events.
2. Audits of high potential situations.
3. Modifications in the operating system.
4. Modifications in the hazard reduction program, likely to produce further changes in the operating system.

If the manager finds the residual risk unacceptable, he can take three kinds of action:

1. Rescind changes already made,
2. Order further changes,
3. Order further evaluation.

After such action, or when forced by time, he accepts the residual risk and projects the probable performance in future operations.

Subsequently this managerial cycle is repeated.

The scheme implies that all potential changes have been evaluated to the point that some alternatives are recommended and others rejected.

It is understood that at each point in the cycle, some standards of judgment will be used for classifying and evaluating information, and standards will also be used for evaluating corrective actions under consideration. At the inception the judgmental standards may be variable and highly personal - they become better defined as the plan is operated.

The model was developed from two kinds of considerations:

1. It seemed to represent, albeit laborously, the way good managers appear to manage.
2. It represents an extension of an ideal hazard reduction system, showing how good managers ought to manage.

The scheme appears capable of reflecting the way good managers take "fast action at the trouble spots" if the assumption is made that subordinates make immediate reports of certain kinds of HIPO events. (They don't wait for "Time Period 2" if that period be construed as a month or a year away.)

The model also seems to reflect a usable system for first line managers, intermediate managers, and top managers. At each successive level, as reports are cumulated for higher management, the threshold level of HIPO events of interest is automatically raised, and consequently more events are handled as groups.

At the top, management wants an assessment regarding disaster potentials and big energies, major changes, critical errors, major accidents, (and wants to know what process was used to assess them) and also wants a continuing assessment of general error and accident rates, and programs to control them. More sophisticated analytic tools can be used to provide the data top management needs.

The model has been exercised on a wide variety of hypothetical and actual cases (from available information on the latter) and appears to be valid and useful.

The model presents a necessarily multi-faceted view of safety performance:

1. What do deviation data (changes, errors, accidents) say as to:
 - a. the past?
 - b. system corrections needed?
 - c. program improvements needed?
2. What do audit data say?
3. What does the future hold:
 - a. judging from the past?
 - b. after changes in the system?
 - c. and after changes in program?
4. What more should be done to make risk tolerable?

As indicated in the model, deviations are believed to have degraded good performance. Can this be measured? After residual risk is accepted, can probable general performance in terms of non-safety measure be projected? Will performance measure up?

The model, then, may be useful in exploring ways of assessing non-safety sources of performance degradation.

Some aspects of risk assessment to be tested are reflected in the following kinds of questions which might be asked by top management or middle management:

1. What do you feel are our worst potentials for catastrophe (or major investment loss) in your area of responsibility?
 - a. What has been done to reduce these major potentials?
 - b. What more could be done, and what would it cost?
2. What are the provisions or standing instructions in your organization for hazard review of new or revised operations?
3. Participation and high-level influence seem to be fundamental to acceptance of safety procedures. What arrangements do you have for involvement of high-level personnel in the development and use of basic safety guidelines? Active committees might be an example.
4. What are you doing to audit the safety aspect of your operations?
5. Give examples of help given first-line supervisors so that they may fulfill their key roles.
6. Do you recall any recent incidents wherein you personally intervened to upgrade safety conditions?

Analysis of Project or System Risk

In this section we are concerned with evaluation and decision for a specific project, activity, machine, or system. Analytic methods can be more specific, less generalized. The broader goals of management policy and implementation do not have as great force (perhaps they should). Specific data seem to be more relevant. Cause-effect relations are more clear, and decision alternatives better defined.

Rhetoric still plays a part. "Let's be practical," is usually the slogan. Rhetorically induced "practicality" may have such effects as loss of life or plant, and may yield a maximum OSHA penalty, or may mean let's do it the loose, error-prone way.

It must be admitted that the intuitive approaches to safety assessment are usually early casualties in the battle, and deservedly so. The problem is to make a qualified protagonist of the safety proponent.

A well-defined and well-executed Hazard Analysis Process is the sound way to strengthen safety's role in decision-making. The relationships between defined risk assessment models and the Hazard Analysis Process described in the next Part are three:

1. The risk assessment models form a structure in which HAP's system analysis techniques operate.

2. The models are also the arena in which results of HAP will be assessed.
3. On the other hand, the risk models do not fully reflect the early, conceptual phases, which can do so much for safety, and they are weak in human aspect, and organizational contingencies and relations which too often result in unanticipated trouble.

The presentation of risk models does, however, seem to provide a helpful point of focus for the Hazard Analysis Process.

Three models are germane:

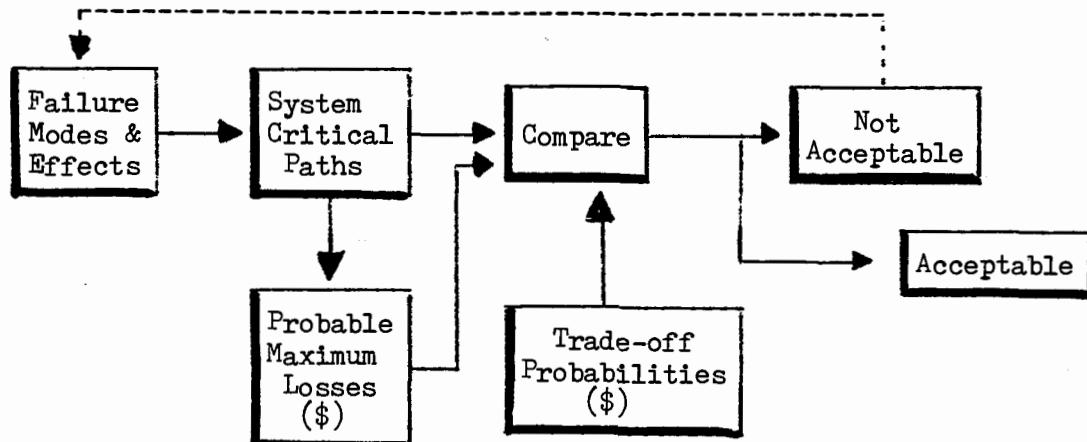
1. Simple--the elements shown in Figure 7-2 (page 90).
2. Expedient--a model developed and used with substantial benefit when more comprehensive techniques were not within resources.
3. A more Comprehensive model.

There is no need to comment further on the simple model, except to say that its essentials carry over into the succeeding two. The Expedient model will be described first. It is also quite simple, but some limitations should be apparent when the Comprehensive model is discussed.

Expedient Model. This can be called the Browning model--its use by Monsanto for analyzing petrochemical plant risks was reported by Browning (1969-70) as having great practical value when simplified, non-computerized techniques and the normal complement of engineering time must be used. (The term "expedient" is intended as descriptive, not derogatory. "Practical" would be a good connotation, although the comprehensive model is also practical. In any event, Browning's model is an order-of-magnitude improvement over the rather common intuitive approaches.)

The model, called Loss Analysis Diagram, uses some special terminology--partially translated into MORT language. The model can be seen as shown in Figure 21-2.

Figure 21-2. Expedient Analysis of Project or System Risks



The failure-modes-and-effects and system-critical paths are derived from project staff (line management for existing projects) and employ a fault-tree format, except it is described as less detailed.

Probabilities are entered on the fault tree only by order-of-magnitude (exponents as used in the table below). Short-cut rules for developing the tree are employed.

The Probable Maximum Loss is derived by insurance underwriting estimate procedures, readily available, and includes business interruption.

The Trade-Off Probabilities are the critical (only stated) criteria, as follows:

<u>Size of Loss, \$</u>	<u>TOP</u>
Under 25,000	10^{-1}
25,000-100,000	10^{-2}
100,000-1,000,000	10^{-3}
1,000,000-10,000,000	10^{-4}
Over 10,000,000	10^{-5}

As indicated in the model, if the probable maximum loss exceeds the trade-off value, the risk is unacceptable and is returned for improvement.

The references provide practical examples, loss estimating procedures, and typical failure rates.

The short-cut, expedient and practical aspects of this risk assessment method, validated in practice, seem substantial. Aerojet safety and reliability personnel are testing the technique for use on risks below those which employ Aerojet's detailed, computerized techniques referred to elsewhere (e.g., Vesely, 1971).

For those safety professionals who have had difficulty venturing into the field of system safety, this technique appears to be a "best bet."

Comprehensive Analysis of Project or System Risk. This model was derived from one prepared by the National Transportation Board entitled "Framework for Analysis of Risks Created by Dangerous Goods Movement" (1971). The model has been modified to fit the occupational situation, and a few aspects found to be substantial in occupational accidents have been added. (The term "comprehensive" is used only to distinguish from Browning's "expedient" version. Note that NTSB aptly called the model a "framework," which term correctly implies that there is more to be said!)

In publishing its document on risk concepts the NTSB said that the lack

of a framework for analyzing risks gives rise to several deficiencies in solutions:

1. Lack of clarity and uniformity of stated purpose,
2. Unrecognized variations in risk and costs of precautionary measures,
3. Vagueness in statements of hazards, risks and consequences,
4. Uncertainty as to weights given various aspects of risk and risk reduction, and
5. Uncertainty as to identity and nature of trade-offs between alternate solutions.

The comprehensive model (Figure 21-3) seems largely self-explanatory. A few comments may help understand the concepts, the elements added and the extensions of Browning's model. Also NTSB's text is very helpful to those who use the model.

System definition is made more explicit. Conceptual grasp and benefits, and research and measurement may be enhanced.

This model (Figure 21-3) inserts four explicit factors:

1. Initial development of performance and risk criteria.
2. Some consideration of possible/probable changes--a major source of trouble.
3. Explicit provision for life cycle and numbers--a powerful support for preventive measures.
4. A role for standards--necessary by law, and important. (NTSB takes an understandably jaundiced view of ad hoc, consensus standards.

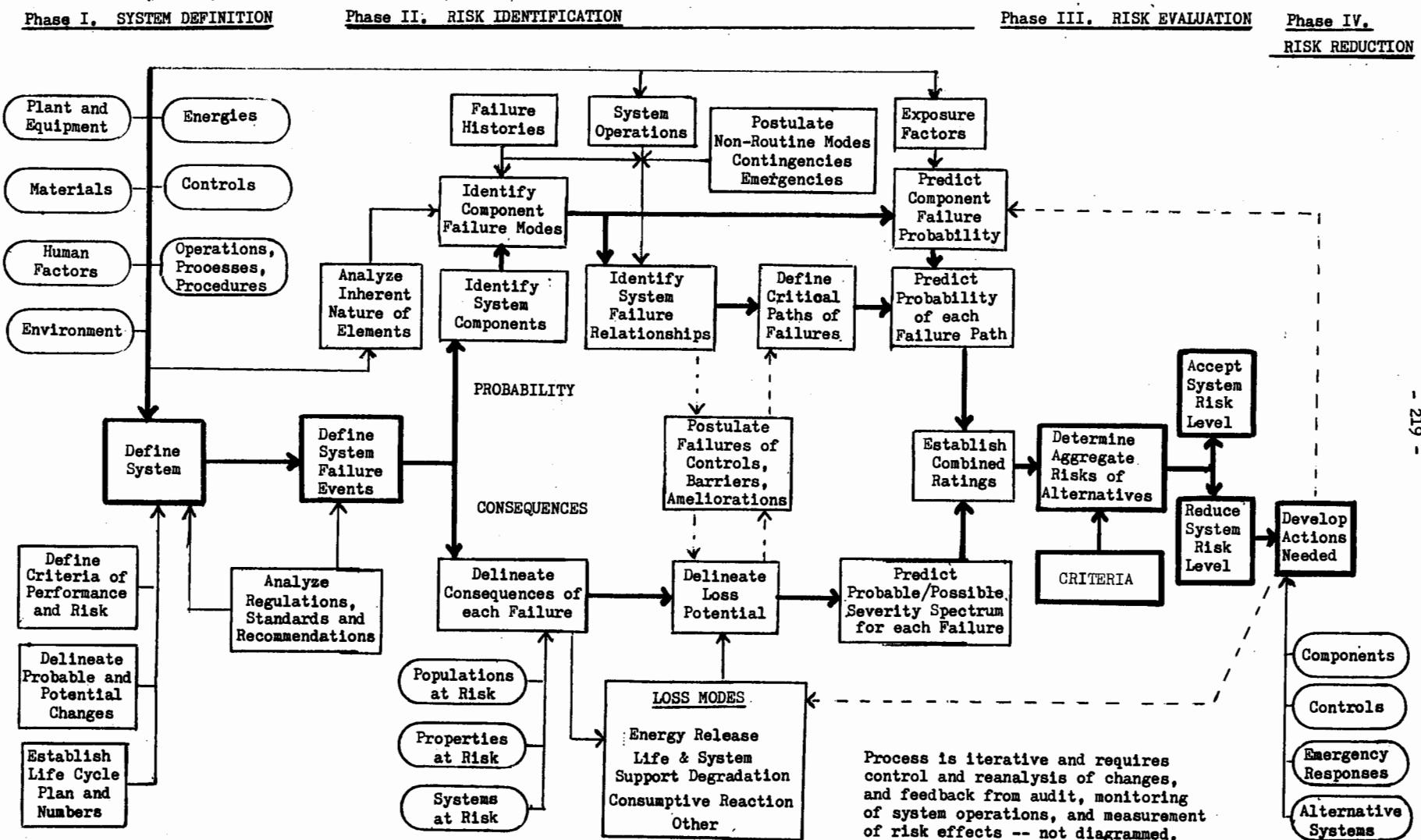
They can be good, and are present constraints.)

Probability analysis elements are specified in some detail.

"Unconventional events"--non-routine modes, contingencies and emergencies--have been specifically called out in the model. Types of chronic problems were described on page 81, and contribute to the exasperating difficulty of detecting and defining the set of events which will confound the routine calculations. Browning dealt in order-of-magnitude probabilities--the histories of unconventional modes suggest that normal failure probabilities have a factor of safety ($\times 10$ or 1 order) to compensate for unanticipated sequences, particularly when analysis is expedient. A taxonomy of unconventional events might be helpful in developing a project-specific inventory of possible (even probable) events. Certainly interaction (particularly damage to the system being considered) from adjacent facilities, and the possible role of malevolence could be examined.

Failure of Barriers is shown in a special role because of the frequency with which events in the probability chain interact with the consequence chain.

Figure 21-3. Comprehensive Analysis of Project or System Risk



Elements At Risk and Loss Modes are intended to be comprehensive, and would substantially expand Browning's model.

Criteria. NTSB did not insert a role for goals at the decision point. The role of goals analyzed at the outset of this chapter warrants their specific inclusion. Certainly Browning's goal, while practical and valuable for physical loss potentials, fails to consider other major goals. A subproblem in analysis or goals is suggested by the comprehensive model's reference to a spectrum of consequences--an integration of minor-major results (a format for \$ losses was suggested on page 43). Thus, both analysis and criteria can be expanded in coverage and detail to estimate the spectrum (or as an expedient, the value of any probable maximum loss perhaps should be increased by an order-of-magnitude to account for the proportionate number of lesser events likely to occur from subsidiary sequences).

Wilmette (NASA, 1971) provides a revealing analysis of the factors in risk assessment, particularly the attrition of safety values under conflicting pressures.

* * *

It would be extremely valuable to have data on the relative roles of the various types of risks in the histories of serious accidents. The individual cases analyzed in this study strongly support the proposition that:

It is uncertainties in the analytic-decision processes which produce the serious events, rather than named calculated risks.

Thus, the Specific (left hand side) of the MORT diagrams can be used to detect the risks that management assumed, knowingly or unknowingly. If knowingly, and risk assumption is a proper and necessary function, the accident can be said to be due to calculated risk. However, the risk more frequently was unanalyzed and perhaps unknown, or an "uncertainty" due to a defect in analytic or preventive process.

All of the risk assessment system is a part of management implementation. However, for convenience, discussion of the remaining portions of the system is in the following sections:

Part VI - The Hazard Analysis Process

Part VII - Work Flow Process

Part VIII - Information System

Part IX - Safety Program Review

The Hazard Analysis Process is largely unstated in most organizations, DOD, AEC and NASA being the exceptions, and we shall borrow liberally from them.

Information and measurement systems are mostly primitive, and even where well developed, seem to fail to provide types of data critical for decisions.

The meaning of the standard accident rates is ambiguous and misleading, and present data on circumstances and causes is questionable and has little decision value. Much accident data now stored in computers is so little used it could as well be stored in 18th century ledgers.

Some ideas for improved use of data for predictive or decision purposes are emerging. Ideas for better computer-based use of data are being tested. However, many tests will be needed before even present accident data are used fully and properly; development of new, more useful data is even more difficult.

Safety program review is sporadic and unorganized in most organizations (until after disasters). A partial exception is audit and appraisal of subsidiary plants, but even here criteria are weak. Most organizations lack a simple outline or list of what the safety program is. Where a safety manual exists, major elements of actual program are often omitted.

Juran has an interesting class exercise: Design an "Executive Instrument Panel" for a major problem. This is a statement of the safety program measurement problem.

This page intentionally blank

VI. HAZARD ANALYSIS PROCESSES

The Hazard Analysis Process must be conceptualized and defined. The failure to do so is probably the most glaring single weakness in present-day professional safety work.

Cookbook recommendations, while useful and needed, fail to clarify the analytic process or method and therefore may unnecessarily inhibit performance or fail to control potentially hazardous innovations.

The lack of concept definition results in a failure to educate management, scientists, and engineers in the intellectual disciplines of the safety process.

A hazard analysis should be required for every activity. The scope will encompass the full range of potential injury-producing energies. The depth of the analysis should be scaled to the magnitude of energies and other concerns, such as program impact.

This page intentionally blank

22. SYSTEM SAFETY AND HAZARD ANALYSIS

Two complementary system safety processes are implicit and intertwined in the MORT diagrams of the Hazard Analysis Process (HAP). They are Life Cycle phases and Safety Procedure Sequence (SPS). These processes have been detailed in many ways in the literature and are frequently alluded to in this text, but a specific enumeration of the two processes as reflected in MORT analysis is warranted.

Life Cycle Phases are considered to be:

1. Conception (including definition and requirements)
2. Design/Development
3. Manufacture/Construction/Installation of system components
4. Operation--procedures, personnel, maintenance, etc.
5. Disposal.

Recognition of the phases in the life cycle is frequent in the literature, including AEC guidelines, but implementation of the concept is "LTA". Even after the life cycle phases are recognized, there is a tendency to do safety analysis too late. Consequently, some NASA requirements (1970) are pertinent:

1. "Preliminary hazard analysis involves a comprehensive qualitative study of planned systems and equipments in the intended operating environment. Energy sources and inadvertent release of materials should be areas of emphasis... provide the basis for establishing safety criteria for inclusion in the performance and design specifications."
2. "Detailed hazard analyses employing suitable analytical techniques must be employed in the definition and design phases to further identify potential hazards and to determine methods for the elimination or control. These analyses must cover the planned systems and subsystems with emphasis on the interfaces between these systems and subsystems. The results of reliability, timeline, human error, ... analyses must be used and extended wherever appropriate .."
3. "Operating hazard analyses must be conducted to determine safety requirements for personnel, procedures, and equipment used in installations, maintenance, support, testing, operations, emergency escape, egress, rescue and training. The results ... will provide the basis for design changes to eliminate hazards or provide safety devices. They also will identify potential hazardous operation time spans and determine the need for special procedures to be used in servicing, handling, storage and transportation."

Safety Precedence Sequence is here defined as:

1. Design
2. Safety Devices
3. Warning Devices
4. Human Factors review (recycling through previous three phases)

5. Procedures, including emergency procedures

6. Personnel

- a. Supervision
- b. Selection
- c. Training
- d. Motivation

7. Residual Risks.

Also from NASA, we have the following listing of five elements in the Safety Precedence Sequence:

1. "Design for Minimum Hazard. The major effort throughout the design phases must be to insure inherent safety through the selection of appropriate design features such as fail-safe devices, redundancy, and increased ultimate safety factor."
2. "Safety Devices. Known hazards which cannot be eliminated through design selection should then be reduced to the acceptable level through the use of appropriate safety devices as part of the system, subsystem, or equipment."
3. "Warning devices. Where it is not possible to preclude the existence or occurrence of a known hazard, devices should be employed for the timely detection of the condition and the generation of an adequate warning signal. Warning signals and their application must be designed to minimize the probability of wrong signals or of improper personnel reaction to the signals."
4. "Special Procedures. If the possible effects of an existing or potential hazard cannot be reduced through design, or the use of safety and warning devices, special procedures must be developed to enable crews to perform critical functions once an emergency has developed."
5. "Residual Hazards. The remaining residual hazards for which countering techniques are not developed, shall be specifically identified to line management for decision-making as to the acceptability of the associated risks."

It will be seen that NASA items 1-4 are included in the SPS sequence and NASA's item 5 is last in the MORT SPS sequence. Actually, NASA, in other documents, covers SPS items 4 and 6.

Review of the literature on the broad range of human factors and roles in accidents reveals a dearth of research, often conflicting findings, and real difficulty in developing any systematic views useful in arranging program priorities or measuring program and program effectiveness. However, there are topical areas which seem to proceed roughly in descending order of degree of certainty in knowledge, and this also seems to be, in part, a descending order of closeness to the operational errors and behavior which immediately precede

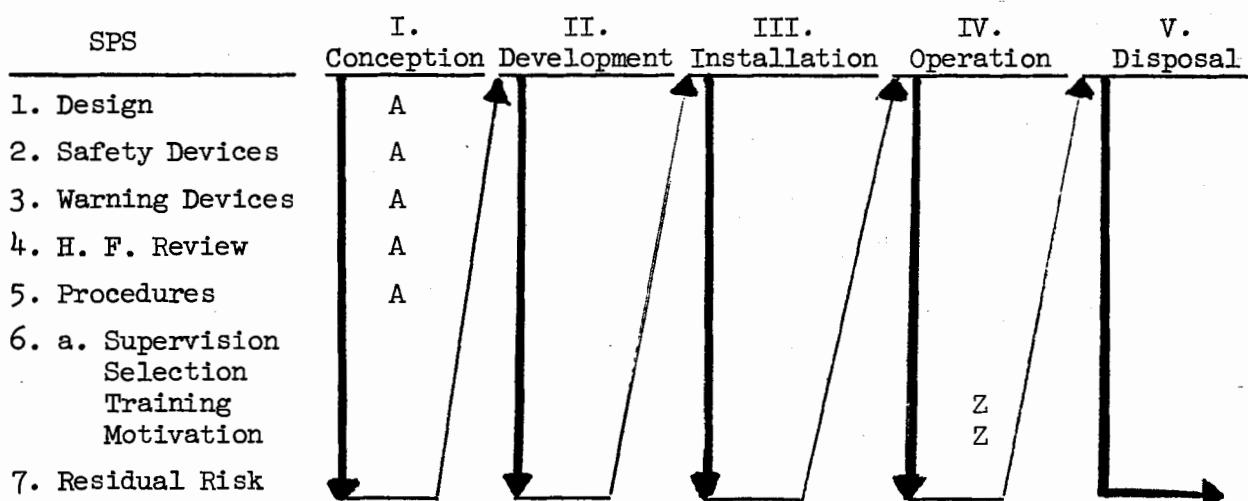
the accident. Thus, a useful extension of the Safety Precedence Sequence was postulated:

4. Human Factors Engineering Review
5. Procedures, particularly Job Safety Analysis (less sophisticated than HFE)
6. a. Supervision
6. b. Selection
6. c. Training, particularly J. I. T.
6. d. Motivation
 - a. Innovation Diffusion - attaining desired changes
 - b. Group and Social influences
 - c. Influencing individuals
 - (1) Human relations, mental health, alcohol programs
 - (2) Attitudes and personality
 - d. Safety Communication Programs
 - (1) Planning models
 - (2) Communication guides
 - (3) Program analysis.

The details of these sequences of the human elements are worked into the MORT analysis.

It seems useful to express the two principal concepts of the scope and nature of Hazard reduction as a matrix with a succession aspect, left to right:

Figure 22-1. Sequential Relation of SPS and Life Cycle



The figure suggests that safety enter the process very early and in fundamental ways (AAAA) rather than very late and in inferior ways (ZZ).

In general, the MORT diagram proceeds from left to right for both the life cycle and the Safety Precedence Sequence.

The principles of review at various life cycle phases are sufficiently important to provide a quotation from an earlier report on the Bevatron at Lawrence, which also exemplifies other doctrine outlined in this text:

During the visits to Lawrence, considerable interest centered on the Bevatron because it provides a practical example of use of system safety principles. and thereby may offer insight as to how general laboratory or general occupational procedures may be upgraded.

Lawrence gave important assistance in the development of the "Safety Guidelines for High Energy Accelerator Facilities" (AEC,1967) prepared by the National Accelerator Safety Committee. The Guidelines have been detailed, expanded, and specified in "Rules and Procedures for the Design and Operation of Hazardous Research Equipment at the Bevatron and 184-inch Cyclotron," April 9, 1968, a substantial looseleaf manual.

The management of the Bevatron exemplifies its personal concern and activity on behalf of safety, even as the looseleaf manual visibly displays concern. Lawrence personnel are also professionally active in laboratory safety.

Probably most significant is the oral expression of policy and practice by Bevatron management.

Manual provisions worthy of at least brief comment include statements fixing policy and responsibilities, authority to stop hazardous operations, and discipline; a lab safety organization which includes Hazardous Equipment Safety Review, Engineering Safety and Electrical Safety Committees; provisions for review early in the life cycle, design review and continuing review, and emphasis on procedures and checklists, as well as physical standards.

An engineer is assigned to work with an experimenter as soon as a project is approved. He and the operating group as a whole provide substantial services and equipment to help the experimenter do what he wants to do--safely. And the engineer monitors the experiment continuously, particularly for changes.

It seems almost superfluous to add that the Bevatron itself displays many built in safeguards. The experimental floor is, however, an area of continuous change which poses great hazard potentials of a less exotic nature, e.g., crane operation and tripping hazards. There was evidence of attention to high hazard potentials, such as the crane, and there was seemingly little statistical evidence that the minor hazards, such as tripping, were in fact causing trouble.

In Lawrence as a whole there is a system of "Building Safety Supervisors" appointed from among the scientific or technical personnel of the building. Thus, as well as in the three major committees, there is heavy reliance on "peers" to influence and guide research personnel.

The broad policy questions seemingly posed by the Guidelines and the Bevatron manual are:

1. Is research in the laboratory as a whole different only in level of energy and value of facility?
2. If the differences are relative only to the two above criteria, can the Bevatron plan and logic be applied in the lab as a whole?
3. How would the above criteria determine change in the degree of control over hazards?

4. What additional criteria are relevant, e.g., cost?

A more specific comparison of Bevatron plans with the MORT tree may serve as a two-way test.

Responsibility fixed. The experimenter is responsible. However, the building supervisor has authority to shut down operations or require higher standards of protection.

Triggers. The major trigger is a newly-approved experiment, for which a formal hazard review process is established. Engineering surveillance on the experimental floor provides change review. In addition, periodic review is required.

Knowledge. Both knowledge and technical assistance (such as an assigned engineer) are provided to experimenters. Lists of applicable codes and criteria are augmented by lists of resource persons for special problems. Some equipment, e.g., hydrogen bubble chambers, is furnished.

HAP -- defined.

Early review is required. In the conceptual stage a Lawrence physicist reviews the experimenter's stated requirements to help screen and limit energy as feasible, and thereby reduce subsequent control problems and emergency procedures.

Independent review of experimenter plans is provided for conception, design, pre-operation, and operation.

Procedures, checklists, schematics, logs, maintenance plans, and emergency procedures are required.

Training is required where necessary.

Monitoring is provided by engineers.

Documentation is required (as it is on design and test of pressure vessels in general).

Some forms of safety analysis - e.g., fail safe, redundancy, and test and qualifications are specified.

Other Aspects:

Goals for accelerators have been conceptualized (Hernandez, 1969).

Maintenance of the accelerator itself is planned and schedules computerized. The maintenance schedule is adjusted by experience. A 90% operating efficiency has been attained, and the preventive program has caught potential generator failures of critical significance. The skills required for maintenance ("heads not hands") have been defined.

Redundancy and Fail Safe principles are evident in the design of the machine itself.

Audit Plans by a Lawrence internal group representing all accelerators were recently instituted and provide an interesting confirmation of some industry findings, namely, the most rigorous inspections are those of peers expert in the operations.

Catastrophe Potential. The explosion (and fire) potential for chemical plants reflects the same kinds of considerations which led to system safety in aerospace work - new exotic processes in larger and larger magnitudes. The precautions already taken and the causes of accidents which do occur reflect in some degree the same general principles and approaches used in system safety,

for example: provision of successive layers of defenses; automatic monitoring; shut-off, and deluge systems; research on material characteristics with particular need to simulate operating conditions for such concerns as pressure, temperature, corrosion, etc.; automatic metering; consideration of relief and venting coupled with safe disposition of vented materials; better design of emergency procedures; etc. The histories of some chemical plant explosions reveals inadequate attention to the "What happens if ... ?" question. Also, the literature is silent on such aspects as design protocols, information search, and independent review.

One British chemical company has reported use of the Fault Tree method and a quantified level of risk as a criterion in chemical plant design. Browning's expedient fault-tree method was reported in Chapter 21.

Some highly regarded safety engineers in the chemical industry have reportedly said that system safety is not needed, and is just a new name for what is already being done (Santos, 1967). Neither view is believed to be correct.

Certain catastrophe potentials (e.g., in chemical plants) appear to be relatively discontinuous with the incidence of minor events. Fires, on the other hand, appear to be more continuous. This frequency-severity relationship for fire should be explored with matrices, because if such analyses are valid, they offer a new way of showing management the long-term potentials.

The transportation of hazardous materials is an area of increasing national concern, and it seems correct to say that the pace of improvement in U. S. Department of Transportation (DOT) programs is too slow - the problems are growing more rapidly than controls. (NTSB, 1971)

Four aspects of the transportation problem can be identified for appropriate study and action:

1. Package design criteria should be improved and modernized. Crash resistance is a criterion hardly recognized.
2. Emergency procedures are not effectively transmitted to a site of an emergency. Talk of educating small town fire departments is largely nonsense. A rapid information system for identification and recommendations on a 24-hour basis is required, as well as placards and instructions accompanying the vehicle.
3. Transportation hazards sometimes sky-rocket when incompatible materials are transported together and interact in a crash. Subdivision of magnitudes can be employed, as well as separation.
4. Plants are exposed to two types of hazards:
 - a. Materials being delivered.
 - b. Exposure to
 - (1) Adjacent plant potentials
 - (2) Materials in transit on adjacent traffic ways.

The National Transportation Safety Board has emphasized system safety in its work from its inception. For example, in a report (1971) of a liquefied oxygen tank truck explosion, NTSB concluded a listing of numerous factors with:

"the absence of a requirement for a systematic search for hazards during the development of the vehicle;

"gaps in the scope of the different kinds of hazards addressed in existing codes and standards."

The system safety approach would imply that management at each level has "most serious residual risk" lists in order of severity and criticality available at all times.

During the MORT Trials at Aerojet, a problem on the "priority problem list," namely, overhead crane operation at reactors, was chosen as a class exercise in application of the MORT hazard analysis process. Various aspects were investigated by class members. Although the cranes are already high-reliability cranes, participants and managers felt the study quickly revealed, and in an orderly way, the serious gaps in crane technology and operation. Many of the factors, e.g., human factors engineering, are difficult to rectify at a local level. A need for national study along similar lines was indicated.

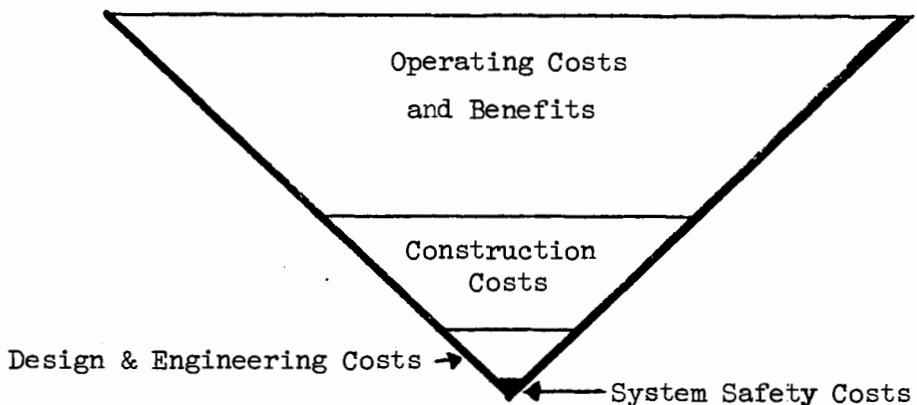
General design literature shows increasing concern for devices and methods which help prevent oversight and optimize solutions. Many such methods parallel safety-related techniques, e.g., criteria-solution matrices, cyclic or iterative processes, failure modes, and provision for feedback. Some design concepts or methods are, however, less formally structured, and are intended to develop open-mindedness as well as the search for oversight, e.g., the use of the six fundamental questions: What? When? Where? Who? How? and Why? And these historic search questions can be used in a three-dimensional examination of Media (information channels), Meaning (purposes and action values) and Matter (the physical factors) to produce a structured search (Turner, 1968). From the literature it appears that the more open-ended forms of inquiry have gained favor in England, and the more disciplined, but narrower, analytic forms have been used in the U. S. Each approach has its merits and disadvantages, both should probably be used.

Whether design is done internally or by outside contract, it is increasingly clear that the customer, the user of designs, will be dissatisfied with the products he receives, unless he has specified the Hazard Analysis Process he wants. Failing this, the quality of what he buys is highly variable and produces later troubles.

Since the costs of a thorough, complete hazards analysis are a recurrent problem, it is well to place system safety analysis costs in perspective - as a general matter, successive cost layers may approach a 1 to 20 ratio in terms of long-term operations, as suggested by Figure 22-2.

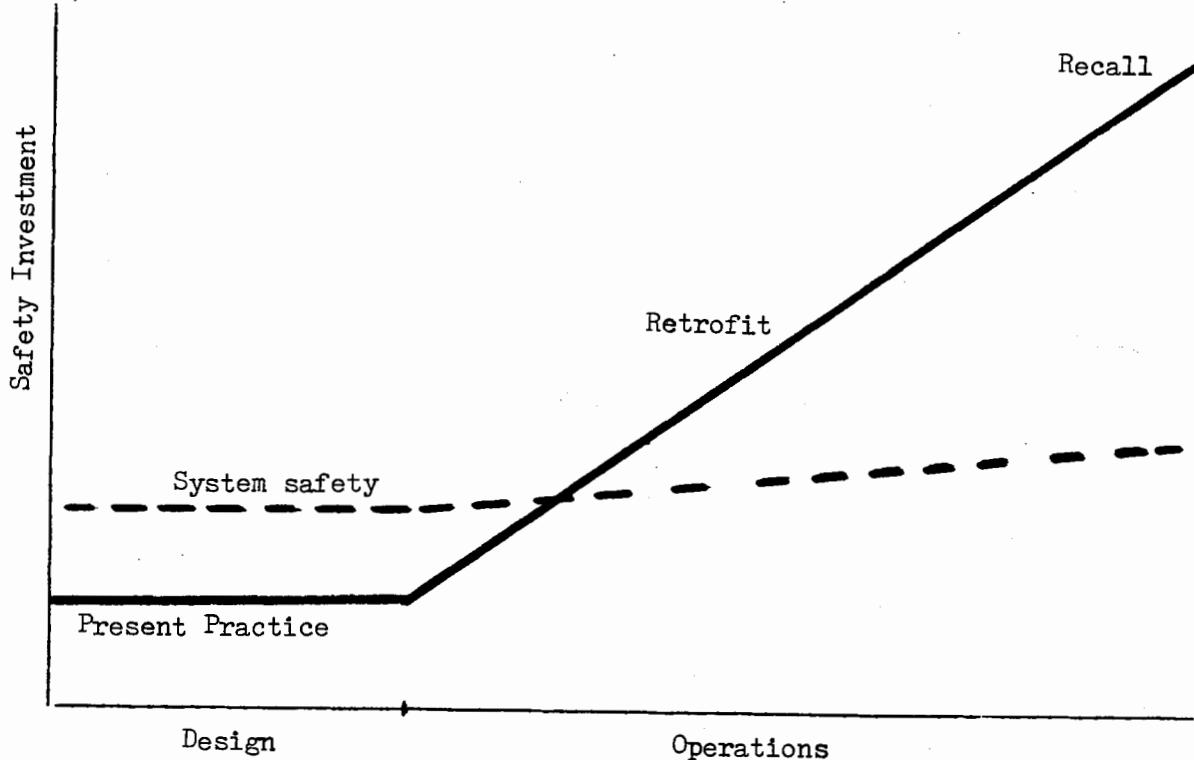
The difficulty of optimizing long-term operating costs and benefits without thorough system safety analysis is comparable in difficulty to balancing one of the Great Pyramids of Egypt on its apex!

Figure 22-2. Costs of System Safety in Perspective



The results of a practice of stinting the design phase and making later corrections are shown below:

Figure 22-3. High Costs of Retrofit and Recall



23. A HAZARD ANALYSIS PROCESS DEFINED

In the third generation MORT diagrams, the "Hazard Review Process" was defined to include the "Triggers" for use of hazard analysis. The fourth generation MORT list postulates the triggers coming from the Monitoring and Information Systems discussed in Part VIII. However, the original discussion of triggers, as such, is helpful in seeing how the Hazard Analysis Process works.

G1 Triggers. Stimuli for the Hazard Analysis Process are needed.

a1 Planned Changes. Historically, planned changes, such as new construction, alterations, new processes or machines, new materials, and new employees have triggered accident prevention processes. The logic and accident experience suggest an expansion of these opportunities for safety improvement, and increased formalization and detailing of such triggers in approval channels.

Clearly the rather common safety review of plans and designs (after completion) should be preceded by the vastly more profitable review and input at, conceptual stages. (Strangely, not all safety engineers are eager to get in at the conceptual stage.)

Management should also be aware of the common complaint that the safety group is not told of plans until too late. Management can easily correct this by withholding project approvals.

There are real problems in upgrading safety programs. But there seems to be little or no excuse for failing to at least try to apply HAP in full to the next few larger planned changes. These are opportunities.

Accident investigations should always cover the hazard analysis procedures in effect when facilities or equipment were installed. If documents relevant to hazard analysis are lacking (as they often are), the lack should be noted.

a2 Unplanned Changes. Unplanned changes (normally unreviewed) in people, machines, work and environment commonly show up as factors in accidents. Better change detection techniques, especially for supervisors, and monitoring for change is essential.

Periodic review requirements can detect unplanned, unreviewed changes.

a3 HIPO's. High potential situations, whether actual or potential incidents, should be screened and collected from all possible sources. In line with the "Pareto Principle" a small number of incidents will prove to have the large potential for loss. A search-out plan for such incidents should be in effect.

Allison (1965) has written extensively on experiences with HIPO reporting and analysis systems. However, the point that all available data sources be screened for HIPO characteristics seems more valuable than any specific method of reporting or analysis. Small numbers of HIPO's are reported in actual systems, for example, 3 HIPO's were reported as compared to 1,000 first aid cases at Sandia.

a4 Critical Incidents. Critical incident reporting has yet to be proven practical for trend analysis. However, the reports collected have proven to be extremely helpful raw material for the hazard reduction mill, and are probably second only to serious accidents as an information source. (See Chapter 37 and Appendix D.)

a6 New Information. Results of research, incident reports, new standards, all provide triggers for the review process. A test, retrospective in accident investigation, is whether a literature search would reveal that new information was published but was not detected or not used.

a7 Priority Problem Lists. Management should, at all times, know what its most significant assumed risks or worst potentials are thought to be. The usual second order effect of such a list is action to reduce risk.

The recent "Fire Safety and Adequacy of Operating Conditions" reports prepared at AEC sites are good illustrations of the value of "worst potential lists," and much is being accomplished in eliminating the hazards revealed.

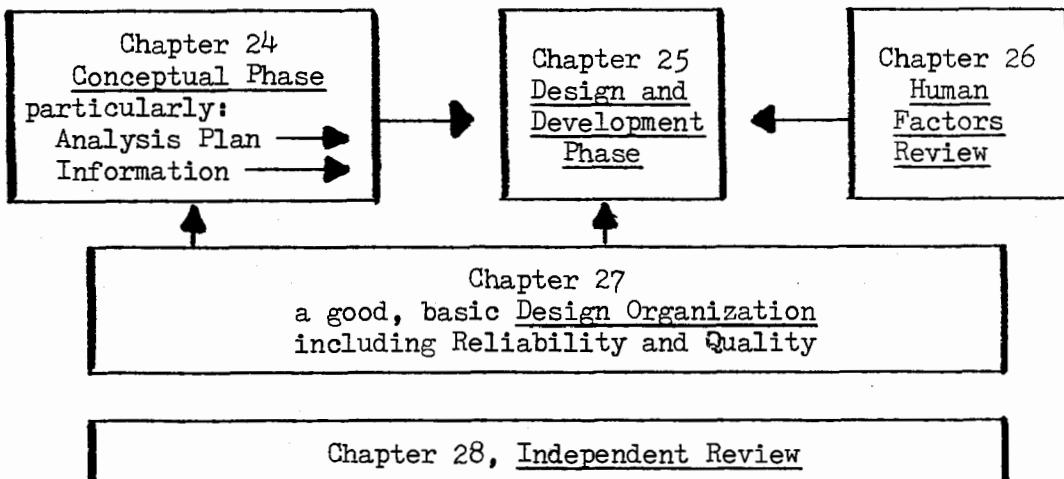
This study contemplates the preparation of PPL's on a continuing basis, and as a two channel process through the line organization as well as the safety department. (Such a process avoids some of the problems associated with a crash project.)

The PPL's obtained informally from safety engineers at two AEC sites did, in fact, consist of matters deserving of management attention, and subsequent exercises at Aerojet and in a seminar confirm their value.

The absence of PPL's results in major problems going without formal review, until an accident occurs. (PPL is not the same as "worst credible catastrophe" used in AEC nuclear safety plans for advance planning and review. PPL is the residual after review and reduction.)

The fourth generation of MORT lists the Hazard Analysis Process (HAP) as shown in Figure 23-1.

The material explaining the Hazard Analysis Process is organized as follows:



Introducing Improved Hazard Analysis Processes.

Even in an effective organization the introduction of a higher level Hazards Analysis Process is likely to consist of a moderately large number (5-10) changes in the HAP. If too many changes are made at the same time, there may be risk of disrupting the existing system which has been working well.

Figure 23-1.

HAZARD ANALYSIS PROCESS

1. Concepts and Requirements

a. Specify Goals & Tolerable Risks

- (1) Safety
- (2) Performance
- b. Safety Analysis Criteria
- (1) Plan
- (2) Scaling Mechanism
- (3) Analysis Methods
- (4) Require Alternatives
- (5) Specify safety precedence sequence
(e.g., priority for design)
- (6) Analyze Environmental Impact

c. Specify Requirements Criteria

- (1) AEC
- (2) OSHA
- (3) Other Federal
- (4) State and Local
- (5) Other National Codes, Standards,
and Recommendations
- (6) Internal Standards

d. Specify Information Search

- (1) Nature
- (2) Scope

e. Life Cycle Analysis

- (1) Specify Life Cycle Scope
- (2) Require Life Cycle Use, and
Failure Estimates
- (3) Require Safety Factors for
Extended Use

N.B. The basic design process
must meet such criteria as RDT
Standard F2-2T, USAEC.

2. Design and Development Procedures

a. Energy Control Procedures

- (1) Unnecessary Exposed Hazards
- (2) Under Design
- (3) Automatic Controls
- (4) Warnings
- (5) Manual Controls
- (6) Safe Energy Release
- (7) Barriers

b. Human Factors Review

c. Maintenance Plan

d. Inspection Plan

e. Arrangement

f. Environment

g. Operability Specifications

- (1) Test and Qualification
- (2) Supervision
- (3) Procedures Criteria
- (4) Personnel Selection
- (5) Personnel Training & Qualification
- (6) Personnel Motivation
- (7) Monitor Points
- (8) Emergency Plans (including
amelioration)

h. Change Review Procedures

i. Disposal Plan

j. Independent Review

- (1) Technically Competent
- (2) Method & Content

k. Configuration Control

l. Documentation

n. Fast Action, Expedient Cycle

WHAT ELSE ? WHEN ANALYSIS ENDS, ALL ELSE IS HUNCH !

The approach used has been to perform an evaluation of present practices and list the improvements needed to attain the higher standards. Then the improvements are ranked in an estimated order of importance. The most important one or two are introduced. When these are running smoothly, and have justified themselves, one or two more can be considered.

An outline for innovation follows:

1. Select a potentially important facet.
2. Develop a protocol as to how the improvement might be made.
3. Try out the protocol on one or two projects in each area.
4. Assess results and values as necessary, and revise.
5. Try again, now including the protocol as an independent review criterion.
6. Based on experience, prepare appropriate directives.

An alternative is to apply in detail a high-grade Hazard Analysis Process to one major new project.

24. CONCEPTS AND REQUIREMENTS - THE CONCEPTUAL PHASE

The importance of introducing safety in the initial stages of concept and definition of requirements simply cannot be overemphasized. All too often energies to be used are not limited or altered, and substitute processes are not utilized. Further, the common practice of safety review of completed plans gets too little safety because it is too late in the design process. Case histories of positive contributions of safety in the conceptual stages should be systematically collected (a few are reported from Lawrence).

MORT analysis of serious accidents confirms the values in the conceptual functions:

1. Unspecified "tolerable risks" turned out to be intolerably large!
2. Safety input was often nil.
3. Energies used were greater than were needed for performance, and the extra, unneeded energy raised both costs and trouble potential.
4. Substitute safer processes were not used.

"Openmindedness," a criterion once suggested by C. O. Miller of the National Transportation Safety Board, is often not evident. Rather the opposite, "We've always done it that way."

In the conceptual stage it is helpful to look at the widest possible range of considerations. For example:

1. Does "reliable control of work" assure that energy is controlled and directed to maximize performance? Are work controls also safety controls?
2. Would substitute processes (e.g., material handling equipment) help performance as well as safety?
3. Do safety criteria play a proper part in decision information, for example, would a plant site selection create commuting hazards? Would people drive into the sun coming and going? Is terrain hilly? Are roads poor?

The conceptual phase offers the greatest opportunity for most safety at least cost.

(The numbering system in the following section conforms to the revised MORT, Figure 23-1.)

1a. Specify Tolerable Risks and Goals

- (1) Safety (see previous discussion of Goals)
- (2) Performance--what output over what time, with what reliability and quality?

The set of values, e.g., minimizing adverse public or employee reactions, concern for public or customer protection, minimizing system disruption or

failure, long-term effects (rather than short-term) may be given desired emphasis in the goal statement.

1b. Safety Analysis Criteria

(1) Plan. The primary system safety requirements are defined as:

1. A system safety plan,
2. Hazard Analysis (defined),
3. Safety Precedence Sequence.

The system safety plan is essentially "who does what and when" in analysis, study and development. A detailed listing of specific safety tasks to be performed and scheduled milestones to measure performance are provided. Specifically, there is provision for safety assessment in all program review.

An excellent overview of analysis plans is provided by three figures from the NASA System Safety Manual (1970):

Figure 24-1. Safety Interfaces and Typical Data Flow

Figure 24-2. System Safety Activities Functional Flow

Figure 24-3. Safety Analysis - Program Activity Relationship.

It is clear from figures 1 and 3 that system safety, as with design generally, is an iterative process.

Despite the thoroughness of system safety work, the cost of system safety is reported to be only $2\frac{1}{2}\%$ to 4% of engineering costs in DOD.

(2) Scaling Mechanism. We do in practice scale the seriousness of events and possible events. And indeed we must scale events by some criteria in order to put a major portion of available resources into major problems.

From a humane view, we would like to prevent all accidents. But it simply is not practical to put a "gold-plated" effort into each of the numerous accident problems which frequently result in minor injuries. By some indefinite, but very real, yardsticks, we try to put major efforts into prevention of deaths, crippling injuries, and catastrophes.

Methods of scaling the amount of effort, analysis, or risk are presently quite imperfect. Were it not that we do and must scale magnitudes mentally, and largely without reference standards, as an everyday requirement, the problem of improving scaling mechanisms could be cast aside as too difficult and troublesome.

In practice there appear to be at least five types of scaling mechanisms:

1. Scaling by frequency (probabilities) and severity of effects on people or things (essentially a matrix).
2. Word descriptions of severity (e.g., the DOD classification of system effects).

NASA Figure 2

Figure 24-1

SAFETY INTERFACES AND TYPICAL DATA FLOW

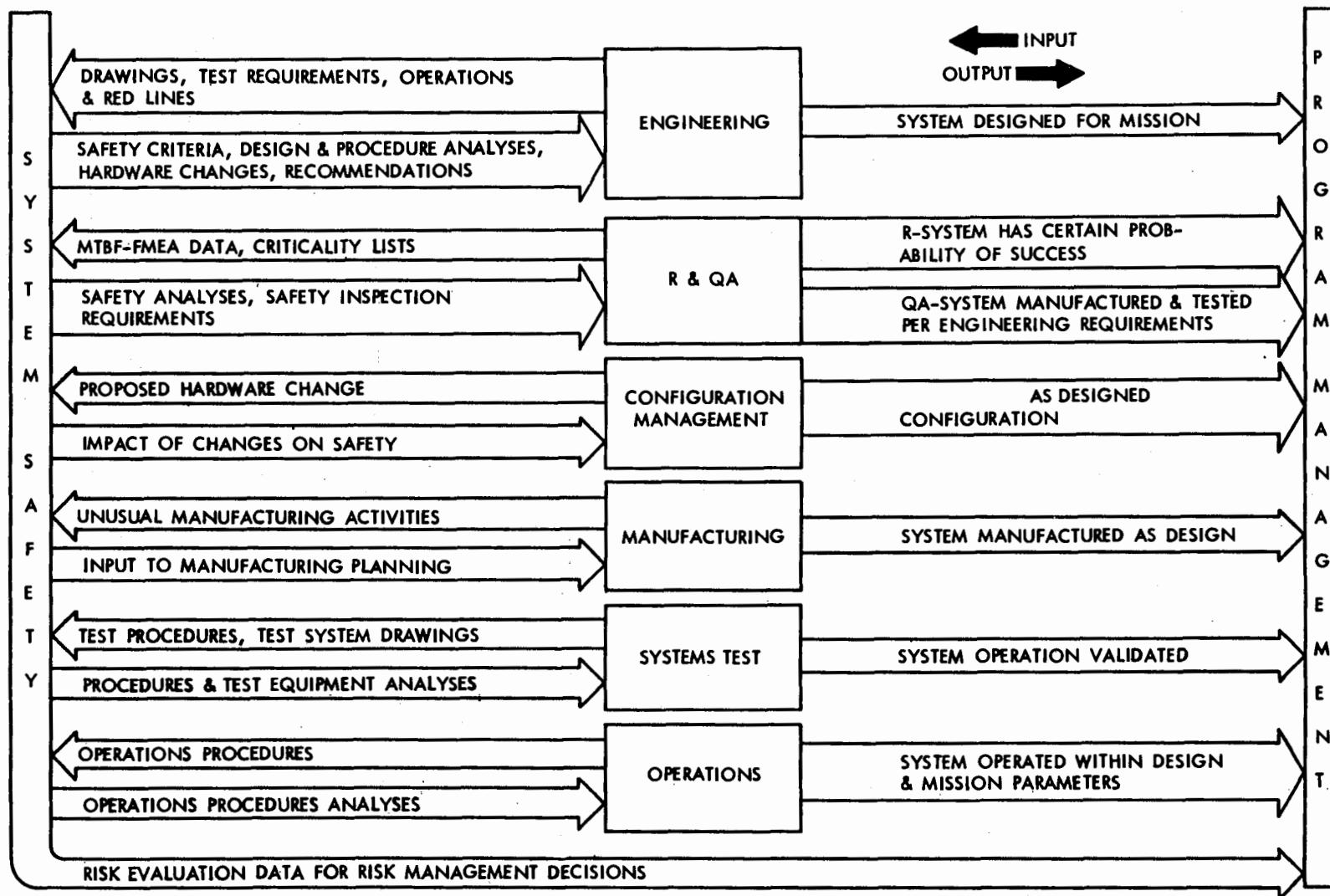


Figure 24-2

SYSTEM SAFETY ACTIVITIES FUNCTIONAL FLOW

IDEALIZED FUNCTIONS FOR NEW PROJECTS

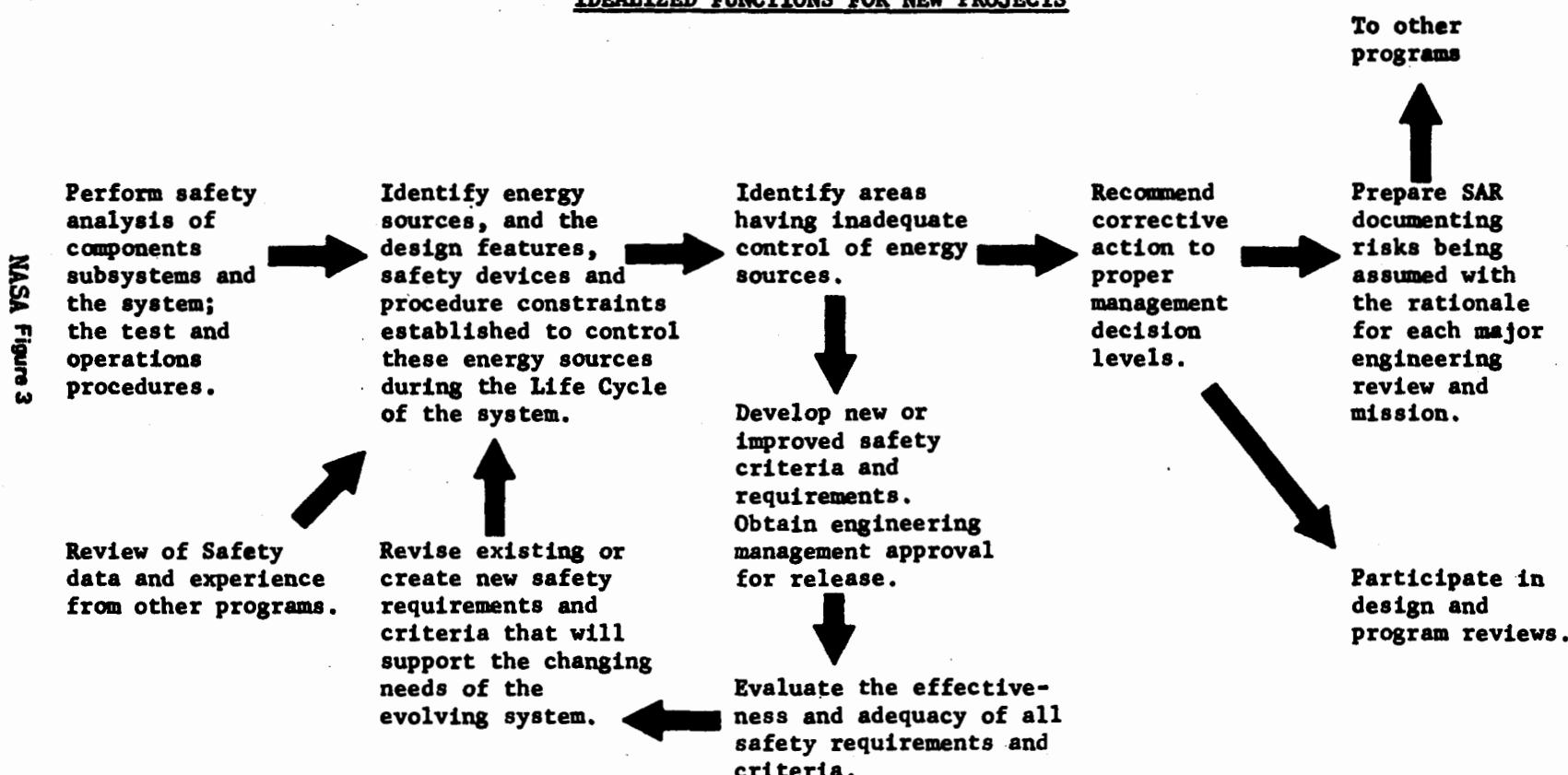
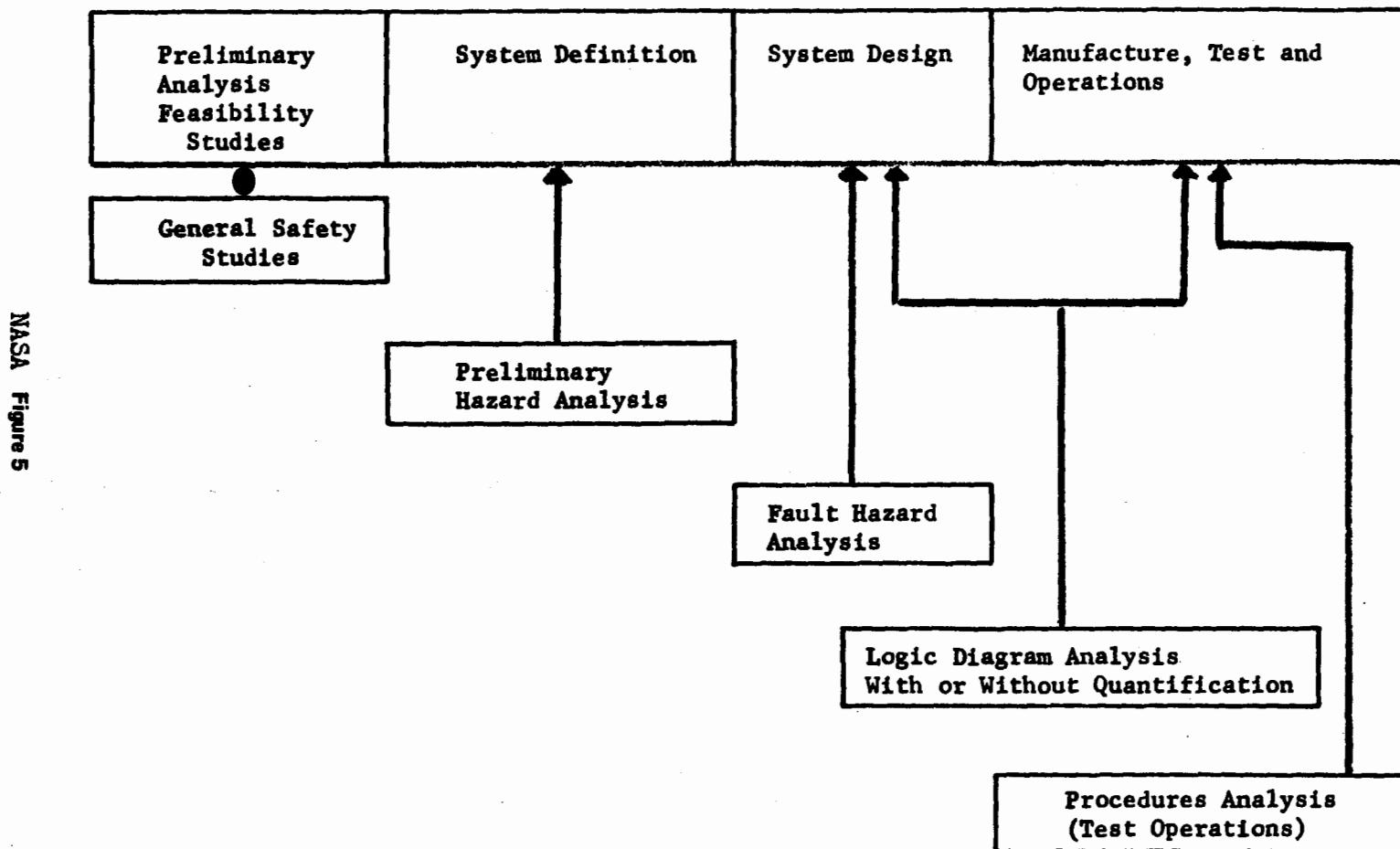


Figure 24-3
SAFETY ANALYSIS - PROGRAM ACTIVITY RELATIONSHIP



3. Categories of hazards (e.g., explosives, flammable, high voltages, pressure vessels) get major study in contrast with lesser study for non-enumerated hazards. New construction or alterations, new chemicals, or welding are examples of other activity scaling.
4. Some special hazards can be categorized numerically by the amount of energy (e.g., voltages, temperatures, pressures or amounts of toxic material).
5. Experience, or intelligent hunch, may be used to scale seriousness, and therefore, amount of preventive effort.

Certainly none of these kinds of criteria has been an entirely satisfactory scaling mechanism. Shall we use one or another, or examine the feasibility of articulating and then correlating or combining the various bases? The latter seems preferable, if it can be made practical, and if it expresses some consensus.

As examples of scaling of preventive effort, we have at one extreme the almost unbounded Safety Analysis Plans for thermonuclear weapons and reactors; at an intermediate level, Sandia's requirement of written SOP's for special named hazards; and essentially no defined requirement for non-repetitive, "low potential" operations.

These scalings, in turn, are the basis for requirements for review, procedures, etc., which are scaled as to amount. However, inquiry has shown that the thresholds above which safety program features are invoked are often vague, and the program application is proportionately vague, sporadic, and inexact. The consequence is, of course, that accidents occur in part because of differences in views as to the criteria to be used to judge amount of study or review. Another consequence is friction over who (e.g., professionals vs operators) is entitled to proceed with work without independent review, or friction over "too much red tape." Other consequences may be excessive cost for study of minor injury sources, or an organizational headache from the practical need to violate management directives, such as a requirement for analysis of "any hazard."

The absence of criteria is untenable - that is, it leads to loose or improper scaling of efforts and at the worst, to a vagueness which tends to de-energize the thrust of the hazard reduction process itself.

Only order-of-magnitude classes are needed to scale requirements for preventive effort, and probably four to six classes will ultimately be adequate. However, in attempting to categorize presently used thresholds, sub-classes A and B will be employed. As an opening effort for discussions and

development we have, by accident results:

<u>Category</u>	<u>Typical Potential</u>
I "Safe"	Scratches \$10
II "Marginal"	Medical \$100
III "Hazardous"	Lost Time less than 10 days \$1,000
IV "Critical" or "Dangerous"	More than 10 days, or Permanent \$25,000
V "Catastrophic"	Deaths, or 5 injuries \$100,000
VI "Super Catastrophic"	Multi-death \$1,000,000

This table is intended only as a first approximation to categorize the thresholds in use.

The DOD definitions (preceded by a code from the above scale) are:

- I-B "Safe: Failure will not result in major system degradation, and will not produce system functional damage or contribute to system hazard or personnel injury."
- II-B "Marginal: Failure will degrade the system to some extent without major system damage or personnel injury, but can be adequately counteracted or controlled."
- III "Critical: Failure will degrade the system causing personnel injury, & substantial system damage, or result in an unacceptable hazard necessitating immediate corrective action for personnel and system survival."
- V "Catastrophic: Failure will produce severe degradation of the system which will result in loss of the system or death, or multiple deaths, or injuries."

However, it is reported that such types of word definitions are not discriminating in actual practice.

The AEC scale for accident/incident reporting uses the following thresholds:

III	Type C	Disabling injury (ANSI Z16.1)
II-A		Damage - fire, explosion, over \$50
III-A		Damage - other - over \$500 } under \$25,000
II-A (or I-B)		Any motor vehicle accident
		Radiation - 3 rem to whole body
IV	Type B	\$25,000 to \$99,999
		radiation - 5 rem
V	Type A	Fatal, 5 injuries
		\$100,000
		radiation - 25 rem

The radiation energy levels, as well as some other AEC reporting thresholds, reflect public reaction and sensitivity as well as non-trauma concerns (protect genetic material) - another variable in evaluating hazard and preventive effort, and one which can be worked into a system of categories.

Sandia's guidelines for underground nuclear tests employ the following classification of hazardous conditions:

- | | | |
|-----|---------------------------------------|--|
| I | <u>Class 1 - Safe</u> | Activities, conditions, etc., such that the physical properties or functional characteristics do not present any hazards to personnel or experiments. |
| II | <u>Class 2 - Marginal</u> | Activities, conditions, etc., such that the physical properties or functional characteristics do present hazards to personnel or adjacent experiments which can be controlled by containment fixtures, special handling and/or by a minimum amount of protective clothing. |
| III | | |
| IV | <u>Class 3 - Dangerous</u> | Activities, conditions, etc., such that the physical properties or functional characteristics could result in injury to personnel or extensive damage to other experiments unless controlled by limiting personnel access, providing special safety devices, using special equipment such as protective clothing and equipment (face shields, respirators, etc.) and/or using remote handling devices. |
| V? | <u>Class 4 - Critically Dangerous</u> | Activities, conditions, etc., such that the physical properties or functional characteristics are so hazardous to personnel, experiments, and/or other test-event operations that no preventative measures can be taken to reduce the hazards to a Class 3 level or less. (Stop the operation!) |

Examples of thresholds described by subject matter include:

- VI AEC reactor safeguards, essentially unbounded.
- V Sandia's requirement for Safe Operating Procedures with independent safety review for "operations and tests involving explosives, pyrophoric materials, compressed gases, mechanical or physical hazards."

Aerojet uses a threshold "potential hazard" (II) to require detailed Operating Procedures or Safe Work Permits. But such a low threshold seems unenforceable and impractical. This suggests need for a more flexible hierarchy of preventive measures:

- I & II Pre-Job Analysis by operator
- III Pre-Job Analysis by supervisor or engineer
- IV Job Safety Analysis (from the operating department)
- V Safe Operating Procedures with review.
- VI Safety Analysis Reports and other reactor safeguards, unbounded.

The AEC guidelines for electrical safety in research employ several thresholds:

- I $\frac{1}{4}$ joule
- III 15 joules, 300 volts
- IV 50 joules
- Lasers (no power specification).

Nuclear criticality safeguards use weights of fissionable material as criteria.

Allison's HIPO analysis method uses AEC reporting criteria, in part, and has interesting differences and additions:

Type D - Not High Potential

III Injury less than 2 weeks
II Damage \$500-\$1,000

IV Type C - Injury greater than 2 weeks
III \$1,000 damage

Type B- 2 or more injuries

IV permanent injury
IV damage greater than \$25,000, plus
 Pressure - 150,000 pounds total

IV Type A - comparable with AEC Type A, plus
 200 gallons flammable
IV pyrophoric, explosive, toxic
 300,000 pounds pressure

Aerojet uses pressure-temperature criteria to guide types of protection in working on reactor loops.

A report prepared for the National Commission on Product Safety provides discussion and data on "biological tolerance to various environmental challenges." (Weiner, 1969.) The models and data are too complex for simple, yardstick use (but valuable to designers and safety engineers working on a specific product). However, the material can be helpful in visualizing gross yardsticks.

Fine (1971) has scaling methods as a portion of his analytic method. His formula and scoring ranges are: Risk = Consequences (1 to 100) x Exposure (frequency) (.1 to 10) and Probability (of sequence completion) (.1 to 10).

Expansion of the probabilities shown in the earlier section on Goals will likely be a factor in scaling, as will life cycle estimates of injuries or deaths. Certainly one object used for one year is different from 1000 of the same object used 10 years, at least as far as practical supportable safety analysis and precautions are concerned.

During the pilot phase of this study it was proposed that the wide variety of present scalings be studied and a "simple" scaling device be tested in organizational practice. The foregoing material permits at least a schematic model of a proposed mechanism, Figure 24-4.

In any organization many more pertinent examples of kinds of activity should be compared with accident data, which should permit filling in large numbers of activity titles. Further, a particular supervisor (and his unit) would only have to know pertinent parts of the array. A "fail safe" require-

ment could provide: If in doubt, move the classification up.

Figure 24-4. Possible General Scheme
For Scaling Potentials and Preventive Action

Class	Words Defined	Results (P values)		Kinds of Activity	Energy (by type)	Preventive Action
		Persons	Property			
I	Safe	scratches	\$10	Walking Sitting	To be detailed	
II	Marginal	medical	\$100	Lifting 5' Height		PJA
III	Hazardous	lost time 10 days	\$1000	5-20' Height Welding		JSA or SWP
IV	Critical	10 days permanent	\$10,000	Vehicles 20'+ Height		JSA or SOP
V	Catastrophic	Death 5 injuries	\$100,000	Explosives Flammables		SOP
VI	Super	Multi-death	\$1,000,000	Reactors		SAR unbounded

The scaling mechanisms provide both a level of effort in design and development, and a level of approval. For example, for reactors the Safety Analysis Report, Operating Limits, and Technical Specifications are essentially unbounded, and must be approved by AEC Washington, and then only after independent review.

At Aerojet, a five-tier documentation system, with successively higher approval requirements, is used to implement scaling. The first tier is corporate-wide Policies and Procedures (ANPP). Under this tier, the Reactor Operations Division has a "Standard Practice" (SP) (second tier) which specifies criteria for requiring a "Detailed Operating Procedures" (DOP) (third tier) or using an "Operating Manual" (fourth tier). For example, a DOP is required for "moving fuel that could cause criticality hazards and which is not covered by an SP or ANPP," and this means obtaining approval of an independent Procedures Review Board, which has published and enforced its criteria. "Work Instructions and Information" (fifth tier and uncontrolled) may be used only when criteria for use of the higher tiers do not apply. This type of scaling seems to work well for highly proceduralized reactor work with its own definitions. However, it operates with less precision in non-reactor work.

Consequently, Aerojet personnel have conducted a number of interesting explorations during the trial. The status of the work is about as follows:

1. A Frequency-Severity Matrix is used.

a. Frequency varies from common (6 months) to rare (1,000 years of facility life)

- b. Consequences follow classifications above.
- 2. Scoring has been preliminarily validated by having various persons rate named occurrences.
- 3. Levels of effort have been defined in terms of:
 - a. Line management approval level,
 - b. Level of analysis - formal SAR, checklist, or no formal requirement,
 - c. Independent review - scaled from a multi-discipline board review to field approval by safety engineer,
 - d. Reliability and Quality Assurance level,
 - e. Safety Department level of effort,
 - f. Subsequent monitoring, level of effort.

The mechanism was then exercised on a specific problem - which of a long list of operations and aspects should have priority in an intensified monitoring program. Ratings again showed an adequate degree of consistency. (Exhibit 2)

The present status suggests that two kinds of mechanisms will be needed:

- 1. Subject matter or topical rules (flammable, explosives, fissionable materials, ladders)
- 2. Matrices for use by scientists-engineers in more probing studies of relative importance.

And, each of these must be tied to a level of effort system.

The dilemma of AEC is probably typical.

- 1. A requirement for formal, intensive Safety Analysis Reports is being extended from reactors to other kinds of facilities,
- 2. It is desirable that any activity be analyzed.

How can we broaden the coverage of all analysis without lowering the requirements for the most serious hazards? Certainly every activity cannot have a Safety Analysis Report of the depth that AEC term implies. On the other hand, there are significant indications that injuries of minor consequence - bumps, bruises, and scratches - may be overanalyzed at the expense of study of critical and catastrophic potentials.

In summary, the explorations to date suggest that each organization develop its own scaling mechanism. The effort will be worthwhile because proper analysis will prevent accidents which may otherwise be shown to result from vague scalings. The essence of a usable scaling mechanism seems to be:

- 1. About six categories of events to be defined in several ways:
 - a. By words, such as "critical",
 - b. By examples of most common results, such as "medical care (w/o lost time)",
 - c. By activity, especially those hazardous activities in the organi-

zation, such as welding, explosives, flammables, etc.

- d. By energy types and levels, as appropriate, such as pressure, or temperature.

2. Level of effort and approval.

Although the problem of developing such a scale is troublesome, to say the least, the absence of such a mechanism is seemingly causing greater trouble in the form of accidents/incidents, and subsequent recriminations.

(3) Analysis Methods

This criterion has at least two dimensions: (a) were the appropriate analytic skills available in the organization (or from a consultant), and (b) were they used?

Hazard Identification has been said to be "Number One." The task can be seen as having three elements:

1. Practical experience in the operation, and in search-out.
2. Information on "known precedents," references.
3. Systematic analysis.

There is no substitute for practical experience in the operation. No amount of library information or systems analysis can substitute for the knowledgeable man who analyzes and inspects and observes carefully. Levens (1969) described the present day safety man as "almost intuitive" in detecting hazards, and this is both a compliment and a limitation. The compliment is justified because the skilled professional is so highly effective. But the limitations pointed out by Levens are:

1. Analytic process is not monitorable, cannot be documented.
2. Analytic process usually cannot quantify the relative merits of alternatives, no cost/benefit data.
3. Process breaks down in complex situations (some interfaces are omitted).
4. Graphic analytic forms are unavailable; teaching and persuasion are weak.
5. Thousands of combinations of potentials must be learned.

Krikorian gave an eight point summary of ASSE's Search I (1970):

"1. The term 'hazard recognition' ... a more-correct term would be 'identification and evaluation of accident-potential' ...

"2. ... concerned with the man/machine/environment interactions resulting from change/deviation stress as they occur in time/space ... physical harm to persons, but also functional damage, and system degradation.

"3. 'Things' are not hazards, or potential hazards. Events or a sequence of events are hazards. They interact within a system and are caused by the stress effects or the characteristics of people ... Events have both a probability of occurrence and a time-sequence.

"4. When identifying accident-potential ... look at the big picture, at the interactions in a system and its input/output, constraints, and controls. (Then small sections one at a time) and look for selected events that might produce an undesirable outcome... 'the vital few' instead of the 'trivial many.'

"5. We are looking for events and patterns (including behavior) in order to detect changes beyond the normal - such as changes during start up or shut down, or when a process goes wrong. ... Processes usually move along in a state of dynamic equilibrium; but when something does go wrong, the hazard increases - due to the interaction of people to correct the hazard.

"6. The use of 'check lists' is valuable, ... as 'topical guides.'

"7. ... a machine is merely an extension of the biological unit (man) and various human characteristics must be considered ...

"8. The safety-professional must use his natural sense-organs for recognizing accident-potential. .. The safety-professional should always remember (a) that he can ask questions concerning problems or situations that he doesn't understand, and (b) that those problems most likely to occur will not be present when he is present."

A statement of Preliminary Safety Tasks from NASA (1970) is helpful:

- "a. A review of pertinent historical safety data from similar systems.
- b. A continuing review of the gross hardware requirements and concepts, to maintain an understanding of the evolving system.
- c. A review of the proposed mission objectives.
- d. Completion of the planning for follow-on safety activities.
- e. The completion of preliminary hazard analyses to identify potentially hazardous systems and to develop initial safety requirements and criteria.
- f. Participation in trade studies with the result of the preliminary hazard analyses identifying highly hazardous areas, with recommendations as to the alternatives.
- g. Identification of the requirement for special contractor safety studies that may be required during system definition or design.
- h. Estimation of gross resource requirements for the system safety program during the complete system life cycle.
- i. Preparation of an index document that identifies all pertinent safety data developed during the life cycle of the system ... updated at the conclusion of each major increment of the system development ..."

In attempting to describe analytic methods, a difficulty is that many forms of analysis have been given different "trade names" and it is somewhat difficult to perceive the generic forms.

Peters (1968) (as well as MacKenzie, 1968) listed some principal analytic techniques as:

1. "Gross-Hazard Analysis. Performed early in design. Considers overall system as well as individual components. Called 'gross' because it is the initial safety study undertaken." (Stein and Cochren (1967) suggest a "Hazard Manifestations" classification to be used in a matrix with hardware (or other) system components.)
2. "Classification of Hazards. Identifies types of hazards disclosed in step 1 and classifies them according to potential severity (would defect

or failure be catastrophic?) Indicates actions and/or precautions necessary to reduce hazards. May involve preparation of manuals and training procedures."

3. "Failure Modes and Effects. Considers kinds of failures that might occur and their effect on the over-all product or system. Example: effect on system that will result from failure of a single component (a resistor or hydraulic valve, for example)." (Sometimes called "Hazard Modes and Effects." See Figure 24-5 for Recht form and lists of Aerojet captions. FME Analysis is probably the most basic system safety technique and a good point of departure in venturing into detailed system analysis.)
4. "Hazard-Criticality Ranking. Determines statistical, or quantitative, probability of hazard occurrence. Ranking of hazards in the order of 'most critical' to 'least critical.'"
5. "Fault-Tree Analysis. Traces probable hazard progression. Example: If failure occurs in one component or part of the system, will fire result?" (Also Recht, Hixenbaugh, Ericson, Browning, Driesen.)
6. "Energy-Transfer Analysis. Determines interchange of energy that occurs during a catastrophic accident or failure. Analysis is based on the various energy inputs to the product or system, and how these inputs will react in event of failure or catastrophic accident."
7. "Catastrophe Analysis. Identifies failure modes that would create a catastrophic accident."
8. "System/Subsystem Integration. Involves detailed analysis of interfaces, primarily between systems." (Miller says by mock ups, simulators, and tests ... not well defined and a challenge! In this study such factors as lack of interdepartmental coordination repeatedly show as causal factors. Other interface problems are also common.)
9. "Maintenance-Hazard Analysis. Evaluates performance of the system from a maintenance standpoint. Will it be hazardous to service and maintain? Will maintenance procedures be apt to create new hazards in the system?"
10. "Human-Error Analysis. Defines skills required for operation and maintenance. Considers failure modes initiated by human error and how they would affect the system. Should be a major consideration in each step." (See Chapter 26.)
11. "Transportation-Hazard Analysis. Determines hazards to shippers, handlers and bystanders. Also considers what hazards may be 'created' in the system during shipping and handling."

Miller (1968) used nomenclature differing from the above: preliminary hazards analysis rather than gross hazard analysis, and a grouping of "trade name" techniques under Hazard Modes and Effects, but also introduced more consideration of procedures, personnel, and job safety analysis.

Trees. The uses of Fault-Trees and adaptations thereof is increasing rapidly. Even when modified forms are used, as in Browning's expedient form or in MORT, the assumptions and logic are still made explicit and visible for review. These qualities seem to give considerable flexibility without destroying

Failure Modes and Effects Analysis

Formats Used at Aerojet

For Reliability:

Design Characteristic
Failure Mode
Failure Probability
Effect on System
Essentiality Code
Control to minimize:
Frequency
Effect

For Priority Problem Lists:

Energy Sources:
 Kinds
 Amounts
Potential Targets
Barriers, Controls
Residual Risk
Failure Mode
Failure Mechanism
Consequence Potential
Frequency, Consequence Matrix Class
Action-Decision Classes
 Authority level
 Type and date Action Due
(For samples of the last two approaches
see Figure 42-3 on page 442.)

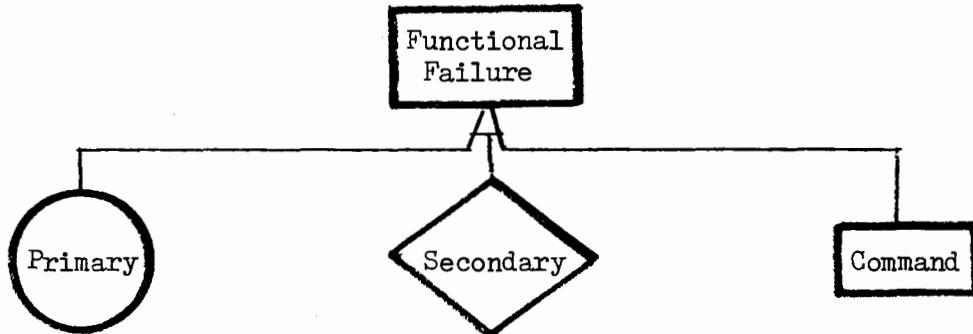
Figure 24-5

FMEA Form

the disciplined character of the analysis, when the dictum is observed that causal factors must be both "sufficient and necessary" for the chain of events.

(The basic logic and the symbols used in MORT are given in Part IV.)

The detection of complex fault paths, while always difficult, is aided by Fault-Tree logic. A common analytic device is:



Primary failures are those occurring under normal operations under designed stresses.

Secondary failures include natural catastrophic exposures (e.g., wind) and a termination symbol is used. But, the substantial number of damaging impacts from nearby exposures--other processes, missiles, or even malevolence, suggests that a fair proportion of the complex events require careful attention to neighboring potential.

The so-called command failures occur when controls, relief devices, and signals (including human) direct the stress which results in failure.

NTSB's (1972) "A Systematic Approach to Pipeline Safety" provides an example of Fault-Tree Analysis.

Hammer (NASA, 1971) suggested a Safety Consideration Tree (and provided an example) to be issued by the procuring agency for guidance of design work.

The General Services Administration (1972) has developed a comprehensive Fire Fault Tree to analyze fire safety. This tree becomes a format for performance standards in new building construction.

Nielsen (1971) used two trees to show the logical connections of causes and consequences:



Nielson also gives particular attention to repair or other special situations and to role of delays in operation of protective systems.

In accident analysis, the prevention of second accidents is viewed as an ameliorative step. But in preplanning and design, such events are best treated as parts of the energy sequence. An example was the introduction of a hydrogen-using experiment into a reactor building. Nielsen's tree is useful in this regard.

The Positive Tree (Figure 9-1) has seemed to have more force in attracting interest and in persuasion than did the same recommendations in text form.

The basic building blocks of system safety analysis are Failure Modes and the Fault-Tree. The suggestion is that these with Schematics-Steps-Criteria (Figure 20-3), which is also a tree, be frequently and consistently used as they have in this text.

Other Analytic Methods. Appraisal of the more common analytic methods suggests needs for additional devices.

Change Analysis. Kepner-Tregoe (1965) suggest analytic forms to search for cause, and potential problem and decision analysis worksheets. In the Role of Change (Chapter 5) Change-Based forms for use in accident investigation were described. Developments in Aerojet trials make it possible to specify in more detail what might be required in simple Change-Counterchange displays in analysis. Two recent serious incidents resulted from uncontrolled change. Thus, in both conceptual and design stages, a display should be required along the lines of Figure 5-3.

Nertney Wheel. Dr. R. J. Nertney of Aerojet developed the wheel concept shown in Figure 24-6--a provocative method of examining the successive phases in hardware-procedure-personnel development, and also examining the all-important interfaces between those three elements.

Without deprecating the sophisticated forms of system safety analysis (as briefly described by Peters, et al) there are strong indications in the Aerojet trials that very simple change analysis of the type described in Figure 5-4, or Dr. Nertney's Wheel, will catch large numbers of common oversights.

Hazard Type. There is an emerging concept that types of hazards, cross-classified by subsystems and components is a desirable approach, prior to the use of the various analytic methods. Miller (summarizing Adams and Hammer) (NASA, 1971) and Stein and Cochran (1967) provide various lists which could be combined as follows:

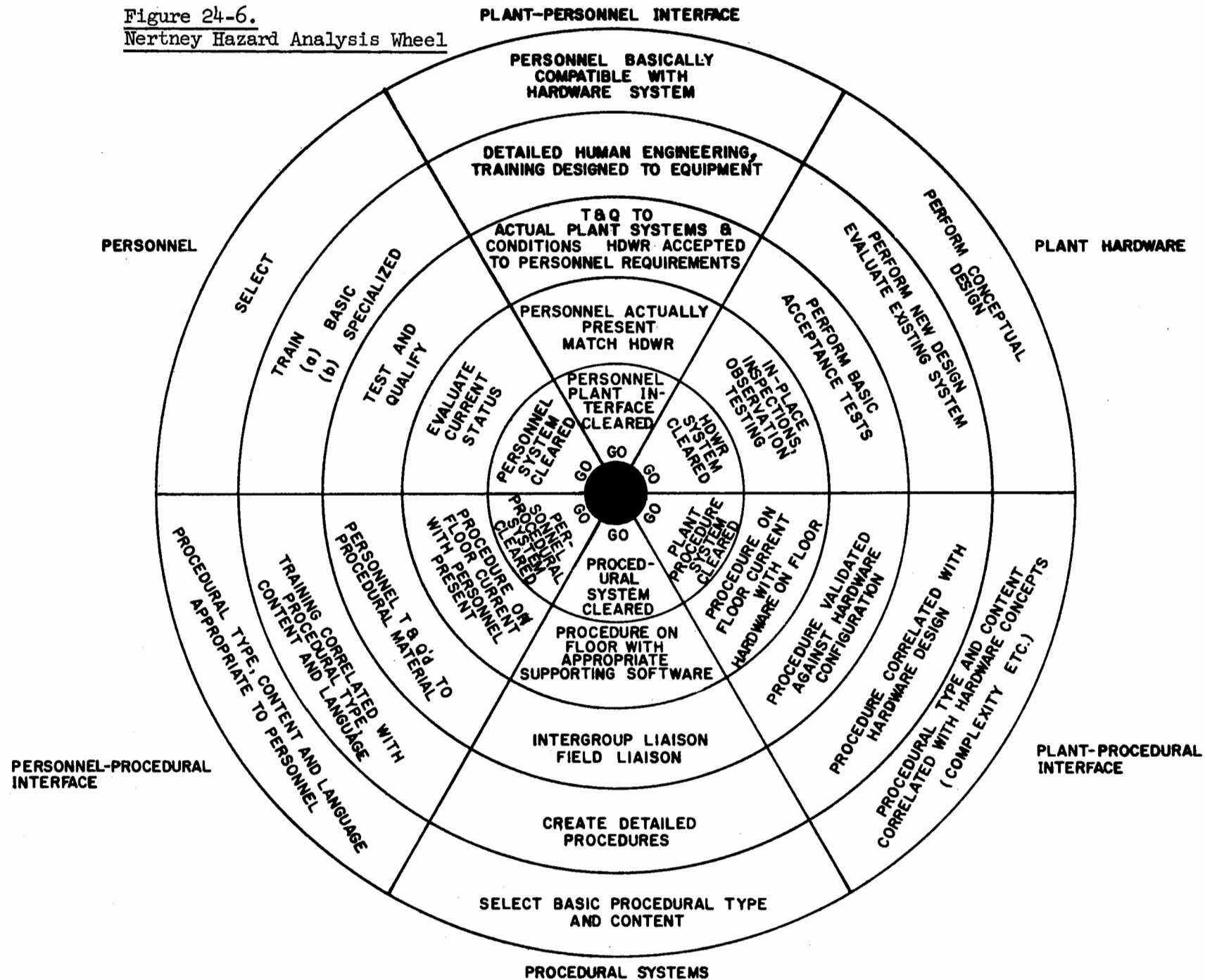
Acceleration	Moisture
Chemical disassociation	Noise
Chemical replacement	Oxidation
Contamination	Pressure
Control anomaly	Radiation
Corrosion	Shock & impact
Electrical	Signal data anomaly
Environment (physiological effects)	Stress concentrations
Explosion/implosion	Stress reversals
Falling objects	Structural aberration
Fire/smoke	Toxic
Heat & temperature	Vibration
Leakage	Weather
	Human Error

Such a list, when reviewed against each subsystem or component, and against a life cycle diagram, is reported to be provocative and searching in early hazard identification.

Greene and Cinibulk (1971) developed a "criticality matrix" for personnel safety based on a failure-mode analysis of personnel hazards and using probability and a "hazard index" as the two dimensions. The hazard index considers time available to correct conditions, as well as long-term time of exposure.

Figure 24-6.

Nertney Hazard Analysis Wheel



Failure Analysis. Currie (1968) lists typical elements to be examined in a scope broader than the usual FMEA (Figure 24-5).

"Operating Condition
Failure most likely
Failure most critical*

Impending Failure
Symptoms/Recognition*
How to inspect for it*

Actual Failure Mode
Symptoms/Recognition*
Troubleshooting to isolate failure source

Action by Operator(s)
Recommended Procedure
Possible Alternatives
Possible Errors *

Effects

On immediate conditions (correct action and incorrect action by operator(s))*
On continued operations (correct action & incorrect action by operator(s))*
Of subsequent additional failures within same system*
Interfaces/potential effects on other systems"

*items emphasize preventive viewpoint.

Hazard Vector. Canale (1966) proposed a new technical definition of safety:

"The safety level of a system is the probability that human and material resources are conserved by the control of all potentially hazardous system input, output, and internal energies."

His model requires estimation of failure rates for various types of controls for each source of potentially hazardous energy. Through a "hazard vector" (probability and magnitude) a cost basis for examining additional controls is established.

Time Line. Analysis of system interactions in the operating period, and on an extended time scale for wear-out, repair, change, etc., is helpful in detecting specific hazards of a "worn-on-worn" relationship of components, as well as the abnormal and non-routine operating modes so productive of trouble.

Double-failure Analysis. Single failure analysis is the primary task, followed by double failure analysis for severe consequences. These are quantified in the Fault-Tree if detected. Special review for double failure potentials is a specific aspect of any good analysis.

Hazard Inventory. The list of hazards identified, but perhaps not all countered, is essential.

Human Factors Review--see Chapter 26.

Perhaps the most difficult aspect of analysis is identifying the sequences or combinations of failures in advance. Accident investigations often show lengthy sequences, but analytic methods tend toward "single failure analysis." A good deal of human ingenuity and a good historical information system are required, in addition to analytic method.

Throughout all of the forms of analysis, it is important to retain visible record of aspects examined and found non-hazardous, at least in the working papers used for review. In a failure mode analysis, for example, when severity or frequency approach zero, show the numbers. In a MORT analysis, leave the satisfactory aspects in the diagram colored green. Otherwise a review agent must play a guessing game as to what has been studied.

Investment/Benefit/Value/Threat. The costs of a hazard countermeasure are easier to estimate than the benefits. But technical difficulties in cost estimation are numerous. After detailed examination of the Planned Program Budgeting System of the Department of Defense, the National Safety Council recommended (1968) a "break-even method." This would provide management with a judgment of the percent reduction in a class of accidents which would be necessary to cover countermeasure costs.

"This simple technique is seen as an interim approach to evaluation of alternative ... countermeasures ... Using this simplified method will expose the analyst to many of the basic problems ... and will yield quantitative information for the decision-maker."

Most occupational accident cost data are so conceptually weak as to provide low, inadequate estimates of potential benefits to be derived. An exploratory study (Stanford, 1964) for public accidents provided some useful concepts, but little follow up research has ensued due to lack of funds.

There is great need for a usable "state of the art" summary, in particular for results of numerous studies financed by the Department of Transportation.

The term "Investment" seems in some ways preferable to "cost" since costs of a countermeasure become confused with accident costs, the reduction of the latter being a "benefit."

Unless the non-monetary values, positive or negative, (e.g., participation or repression) associated with a measure are made explicit, cost/benefit studies may be misleading. Also, if there are threats to the use of the countermeasure, they should be noted.

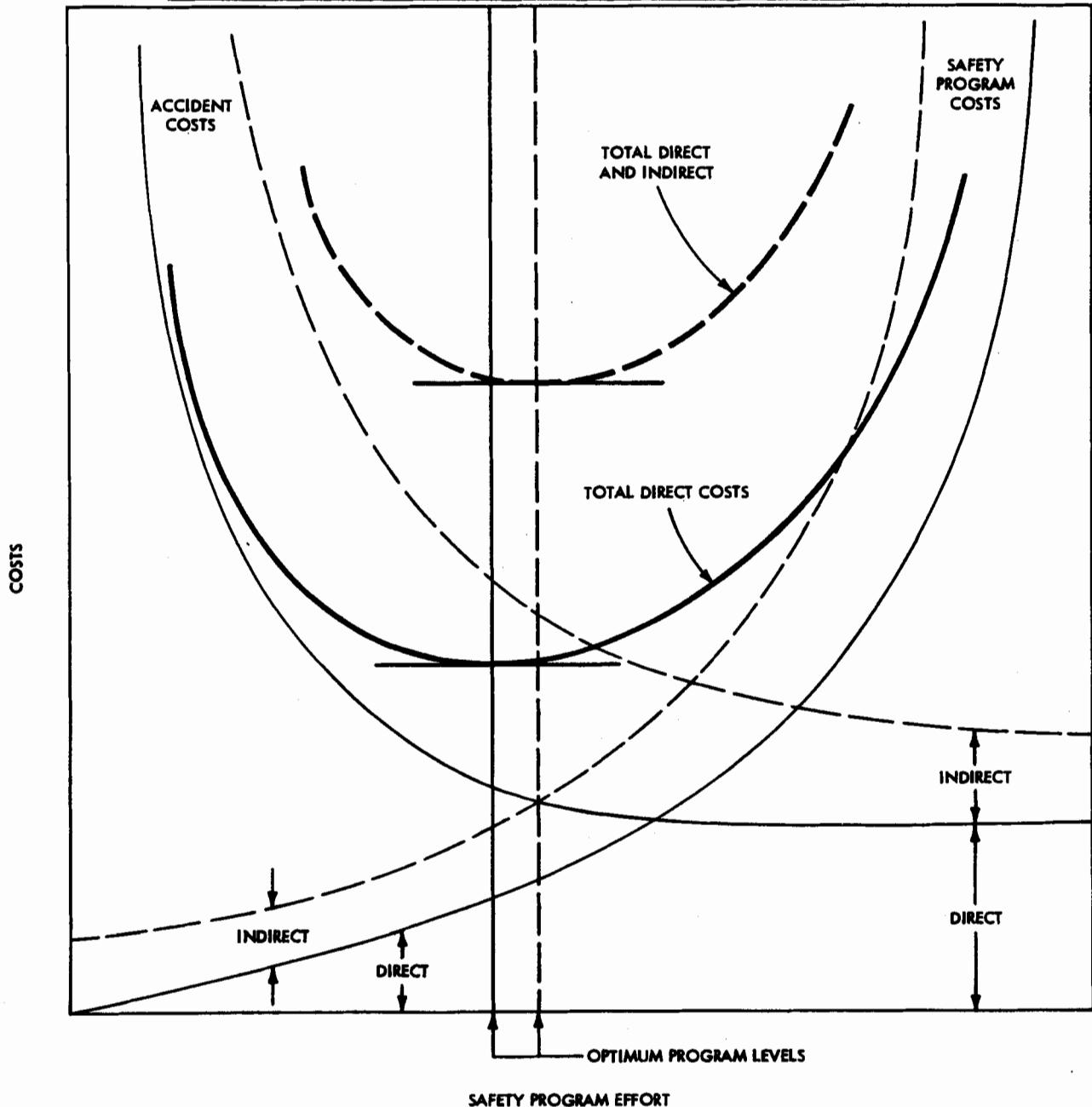
All of these aspects should be required by a format so they will routinely be handled, and the "break-even" percent in accident reduction benefits can be shown.

The Stanford Research Institute study (1964) used a figure (24-6) to show the theoretical optimum of safety in terms of aggregate costs of accidents and prevention.

This curve shows that an optimum is at the lowest point on the Total Cost curve. SRI, however, went on to make the important points that (1) some costs of accidents are born outside the organization (in this case by employees

or the public), whereas (2) most costs of prevention will be within the organization, and (3) the point of optimization of total costs for the community will therefore be at a substantially higher level of safety than for the organization only.

Figure 24-6. Optimization of Safety Program Effort



Regulation is partial, but far from complete, route to minimize costs to the community. Therefore, the entire cost concept seems likely to fail to justify our ideals, unless the interaction of safety with performance and efficiency is used to strengthen management motivations.

In short, cost/effectiveness measures may do more harm than good if effectiveness is measured only by tabulatable costs.

Fine (1971) developed a cost/benefit weighting formula based on scaling five factors: consequences, exposure, probability, cost of measure, and degree of correction. However, data needed for the calculations are often not available, and the method omits some of the considerations immediately above.

* * *

References to the growing literature on system safety analysis techniques (e.g., Miller, Gates and Scarpa, Kanda and Anello, plus others previously cited) suggest that it may perhaps not be so important which brand name of analysis is used, as that appropriate new forms of analysis be used. All of them can greatly upgrade analytic processes.

Training in the new analytic techniques is increasingly available, for example, at University of California (UCLA), George Washington University (Washington, D. C.), and University of Washington (Seattle) and National Safety Council.

The above short discussion of analytic methods extends beyond the conceptual phase and through design and development phase into the operational phase. However, it seems important to introduce these analytic techniques early in the conceptual phase so that the full scope of the analytic work to be undertaken will be understood and planned.

Gnawing through all the touting of system safety analysis techniques is the question, "Why do things still go wrong?" The answers seem to be somewhat varied:

1. System safety is a special (potentially discontinuous) aspect of the project-oriented aerospace effort. If the system safety analysis effort is not funded, it will not be done. Industry is more continuous than project oriented, and therefore well-organized design and other functions hold a greater potential for continuous action.
2. Allocation of resources may be too small or too late.
3. Project constraints may put hazards not solved in the discard pile, since project managers are so heavily measured on budget-schedule performance. The docket or inventory of hazards and disposition being considered by NASA is an effort to control this phenomenon.

The probability of system failure probably varies as the square of the delay in injecting safety into concepts and design.

Notwithstanding the obvious failures, the analytic techniques have demonstrable value.

The greatest strength of modern analytic techniques is complemented by the idea that all analysis should yield a choice of alternatives, with an analysis of trade-off cost/benefits. A simplistic single solution may be a trap which eliminates better or cheaper alternatives. Therefore, a hallmark of good analysis is the display of alternative solutions, particularly those which give the manager the option of buying greater protection.

1. b. (6) Analysis of Environmental Impact

The scope of the hazard analysis should include environmental impact, and pertinent requirements must be inserted in the Safety Analysis Plan, and fulfilled in subsequent stages of Conception, Design, Operation, Disposal, etc. Hayes (1971) reported as follows (abbreviated):

The National Environmental Policy Act requires Government agencies to administer their affairs in accordance with its policies relating to conservation and use of the environment, and assuring safe, healthy, productive, esthetic and culturally pleasing surroundings, and other purposes. These requirements will fall on industry to an increasing degree.

To accomplish these purposes agencies shall -

"utilize a systematic, interdisciplinary approach which will insure the integrated use of the natural and social sciences and the environmental design arts in planning and in decision making which may have an impact on man's environment;

"identify and develop methods and procedures ... which will insure that presently unquantified environmental amenities and values may be given appropriate consideration ... along with economic and technical considerations;

"include in every recommendation or report on proposals for legislation and other major Federal actions significantly affecting the quality of the human environment, a detailed statement ... on

- (i) the environmental impact of the proposed action,
- (ii) any adverse environmental effects which cannot be avoided should the proposal be implemented,
- (iii) alternatives to the proposed action,
- (iv) the relationship between local short-term uses of man's environment, and the maintenance and enhancement of long-term productivity, and
- (v) any irreversible and irretrievable commitments of resources.

"As written, those requirements paraphrase quite suitably the basis for a systems analysis. The objective of a systems safety analysis is to avoid an undesired event, in this case one which will pollute the environment. In a systems analysis of a piece of hardware this event is equivalent to a failure resulting in damage or loss of a mission.

"The methods available such as Fault Tree, FM & Effects, Gross Hazards Analysis could be used to identify the events which will bring the pollution about.

"The selection of available alternatives to the proposed action as required in this law will become possible when, in the analysis, they are pin pointed.

"The usual hard requirement in a system analysis is that each step is documented, and that the whole analysis provides for sound management decisions."

Aerojet Nuclear Company does, of course, include a requirement for an environmental impact statement in its review criteria.

1. c. Specify Requirements Criteria

It is sound practice to specifically call out the codes, standards, manuals, recommendations, etc., deemed applicable to a project. Accident histories not infrequently show failure to use such material, and prior documentation fails to show whether the failure was oversight or a considered decision.

OSHA and other federal, state, local regulations are primary. Regulations are normally definitions of error in specific, pre-analyzed situations where (a) a consensus process has defined needed precautions, or (b) research has defined harmful limits.

Since the available literature covers a large proportion of accident factors it is unfortunate that there are seldom data on the documents actually used in analysis prior to accidents. For example:

1. What documentation was relevant?
2. Was it known at the points of design and operation? If not, why not?
3. Was it adequate? If not, why not?

Also, the question of need for a higher degree of protection than standards is warranted (and is alluded to in AEC Manual 0550-034C).

Complicating the reliance on standards is the generic standard - i.e., "improved risk" in fire protection - not amenable to easy code definition.

A major problem in some standards and manuals is the failure to make visible method of analysis (AEC guidelines for accelerators and electrical safety in research, are positive and constructive examples of good practice), A code defining the Hazard Analysis Process could be a proposed positive force by requiring listing of documents deemed pertinent.

There is widespread criticism of the consensus process for developing codes, manuals, and recommendations, but no data on accidents resulting therefrom. The prior questions on codes, etc., would make it feasible to analyze the possible failure of the consensus process, particularly for very serious accidents. "Drawbacks to Standards" has been a topic of concern. (Journal of American Insurance, 1969.)

To some extent consensus standards are "political" rather than "scientific." Consequently, any organization with the capacity should examine the basis for standards, rather than follow them slavishly.

The pace of development of standards has been too slow under the voluntary system, and there are strong governmental pressures for improvement, especially OSHA. At the same time, the leading corporations, whose personnel perform do most of the work on the standards, meet many of their own needs with internal standards capable of more rapid development and modification. Further, they use their internal standards nationwide and are little concerned over low minimum public standards in a great number of states, because their internal standards are so much higher.

U. S. Steel's plans (1964) for attaining physical safety are typical of the past best practice. They say:

"Safe physical conditions can be established and maintained only if three basic requirements are met:

- (1) Safety standards are established and enforced in the design specifications of equipment and facilities;
- (2) Newly installed or changed facilities are inspected and approved for safety before they are released for operation or use; and
- (3) Specific responsibilities are established for periodic inspection, and for prompt correction of deficiencies or immediate shutdown of equipment if a serious hazard is found."

Then follows a lengthy listing of standards relevant to corporate operations and covering such areas as ventilation, sanitation, lighting, explosion and fire, and toxic materials.

Some organizations, such as AEC, have adopted all applicable public standards, published internal standards, and have gone so far as to promulgate NSC's comprehensive Manual as an internal guide (although it is not written in standards fashion). Larger organizations frequently publish internal guides closely related to their operations, e.g., Sandia's Laboratory Guide.

Provision is customarily established for safety engineering review of all plans, but such review of completed plans is too late to have maximum benefit.

The previous "best practice" should be augmented with the analytic process emerging.

The long-term role of standards is called into question by system safety analysis. The goal is a desired degree of safety, rather than simple conformance with some standard. The day is not near when standards will not be needed, but the day is here when they can be seen as minimal.

It may also be wise to conceive of levels of standards--provide ultra-high reliability standards for special needs, as for example for cranes around such locations as reactors, space equipment or steel furnaces.

In general, performance standards are to be preferred over specification standards, because the former are less likely to inhibit improvement. Performance standards of certain types, such as AEC's radiation standards and OSHA's ceiling and exposure values for hazardous materials, are capable of being steadily raised as evidence warrants, and thus can be in the nature of goals, steadily rising minima. Thus, an organization's internal standards should specify values higher than legal minima.

It would be interesting to see what would happen if a buyer asked a machine manufacturer to not only conform to legal codes but also supply a Failure Mode and Effects analysis for his product!

1. d. Specify Information Search

The failure to require an information search is probably the most glaring single weakness in a typical hazard analysis process.

During the Aerojet trials, a variety of information search methods were tried, some with considerable success, others handicapped by weaknesses in both national and local systems (as discussed in Part VIII).

Developments by May 1972 made it feasible for the Aerojet's ROD Manager to specify to engineering divisions that future proposals must contain the following presentations on information search:

1. Incidents - a search of, and use of:
 - a. RDT Incidents (already key-word coded)
 - b. RSO Incidents (RSO #15 is now key-word coded)
2. Codes, Standards, and Recommendations: List those found applicable and applied.
3. Change and Counterchange Display.

The last item derived from the proofs in two accident/incidents which clearly resulted from uncontrolled and/or uncompensated changes.

The work thus far suggests the following draft protocol for information search:

1. The design unit originates an information search document which includes:
 - a. Description of the project in sufficient detail to include likely key-words to retrieve prior experience. Where appropriate, this includes life cycle use estimates and accident and error projections.
 - b. List of known controlling documents:
 - (1) AEC, including Operating Limits and Tech Specs.
 - (2) Corporate documents, policies and procedures.
 - (3) ANSI, OSHA, ASME, ASTM and other codes and standards.
 - c. Preliminary Gross Hazards Analysis
 - (1) List problems and prior experience in solutions.
 - (2) List recognized information gaps for search at NSIC, NASA, NSC, internal sources, customers or other sources.

2. Safety utilizes the above document to produce:

- a. Copies of relevant accident/incident and error reports of any nature. Analysis thereof.
- b. Notations of additional relevant codes, standards, and other documentation.
- c. List of JSA controls available to supplement the procedures.
- d. Other comments and suggestions, including internal sources of expertise, where pertinent.

Where necessary, conducts information search on non-nuclear, non-reactor task components, as well as nuclear aspects.

3. R & QA performs similar review, in particular providing lists of relevant incidents.

4. Line Management review supplies three needs:

- a. Incident reports not elsewhere available,
- b. Safety operation anomalies, requirements, and needs from use of similar equipment,
- c. Liaison designees for the life of the project.

5. Upon completion of project, the information search record is forwarded as an appendix for management and independent review.

In order to maximize the scope and value of the information search, as much as practical of the Conceptual phase should be included above, for example:

1. Specification of tolerable risks:
 - a. Safety - probability goals.
 - b. Performance - essentiality classes, failures and error rates and goals.
2. Energy reductions and limitations, where practical.
3. Substitute processes and energies.
4. Problems to be listed include those of:
 - a. Installers, constructors, fabricators,
 - b. Adjacent employees,
 - c. Downstream users, including transition to new methods,
 - d. Environmental impacts, including results of abnormal operations.

Quantification of selected variables in failure analysis is useful, but also fraught with danger when variables omitted are of substantial significance. If the effects of "no information search" and "no critical incident studies" are taken together, the risk from unrecognized causes approaches certainty of failure.

l. e. Life Cycle Analysis

The life cycle concept has to be used for a time to fully appreciate its tremendous potential for changing action. Essentially it guards against two weaknesses:

1. Failure to see subsequent events as a design and plan responsibility, e.g., reliability of components, maintainability, and safe disposal.
2. Failure to see the true size of a hazard over time.

We have all met designers who say, "It's not my fault, it's the damn fools who use them." But the new concept (and it is finding its way into law) says

the designer or the decision-maker can do something about hazards throughout the life cycle.

The life cycle also produces numbers of potential accidents which are an order of magnitude larger than the so-called normal expectation, or the "hunch," or the uncalculated risk. And, if we equate action to magnitude, as we try to do, we'll get a lot more action out of life cycle estimates.

Interestingly, one of the management policies originally assembled by NSC includes the following:

"... Safety starts with planning and continues through design, purchasing, fabrication, construction, operation and maintenance ... "

Besides life cycle phases, the scope of life cycle would include, not only the prime mission equipment, but also check out and test equipment and procedures, facilities for operations, procedures for operation, selection of personnel, training equipment and procedures, maintenance facilities, equipment and procedures, and product support.

The power of life cycle numbers can be illustrated in two ways:

Probability of trouble, this machine, today	=	P (a small number)
100 machines	=	100P
for a year	=	25,000P
for the life cycle	=	100,000P 200,000P 500,000P

Estimates of uses form a basis for error rates.

The "life cycle par" for 1,000 employees for 20 years for certain industries would amount to:

<u>"LIFE CYCLE PAR"</u>	All Industries	Manufacturing	Electric Utility	Construction
Dead	4	1	8	15
Permanent Injuries	31	25	23	62
Disabling Injuries	575	1,300	500	500
Other medical Injuries	2,500	1,800	2,000	4,500
Direct Costs	\$900,000	\$800,000	\$900,000	\$2,600,000
Total Costs	\$2,050,000	\$1,800,000	\$2,000,000	\$4,500,000

And for high rate companies, the totals would be two or three times as great.

It is not uncommon for large facilities to be used longer than originally planned, or to maintain good performance with stretched out maintenance schedules (Davidson, 1970). Therefore, careful attention to potential or likely extremes in uses will dictate augmented safety factors.

1. f. General Design and Plan Criteria - see Chapter 27

The conceptual phase terminates in internal and/or independent review to ensure that the project is ready to move to the design and development phase.

* * *

Some future standards and information needs are difficult to fill within short-term constraints of a project. Long-term R & D is needed, as has been recognized in reactor development.

Two examples recently supplied by a British petroleum engineer are illustrative:

Blanketing tanks with inert gas was experimentally applied to small tankers and tested methods were then available for super-tankers.

Off-shore oil drilling should anticipate the probability of deep water wells and initiate developmental research.

These illustrations suggest that an organization formally initiate the conceptual phase of long-term projects NOW, so that needed R & D gets started.

This page intentionally blank

25. DESIGN AND DEVELOPMENT PHASE

The conceptual phase provides major safety inputs--analysis plan and methods, requirements and information. Design and development are the processes of using these inputs.

When things go wrong, we can be protected by redundancy, fail-safe devices, and monitors which signal, but was there full-scale application of such principles? Basically, risk reduction principles are identical with present occupational safety content, but were techniques and principles fully applied? If the analytics are properly executed at least partial answers will be supplied in the detailed logic and quantification.

Analytic logic for evaluating Design is shown in MORT--page 3 (GC3) for design system and page 5 (SD2) for accidents, as well as in the revised list form in Chapter 23. Note that barriers and amelioration, analyzed separately in accident investigation, are part of the design process.

2.a. Energy Control Procedures *

(1) Unnecessary exposed hazards.

(2) Design.

Analysis of "Structure Failed" usually involves three elements of stress:

(a) Energy Supply (which may be limited in the conceptual stage or by certain classes of automatic controls), Energy Control (which is diagrammed), or (c) Safe Release and Barriers and Amelioration (which are shown as separate operations in this analysis).

Note that stress is produced when supply changes, and control and relief are inadequate. Were there changes in energy or structure?

(3) Automatic Controls. (Also see MORT, page 5.)

Note that controls must be checked as to concept and design. A point frequently made by the system analysts can be illustrated here:

If a safeguard has a failure probability	1/1,000
and a redundancy is added with	1/500
we attain a Pf of	1/500,000.
Then, if another redundancy is added with	1/800
we attain a Pf of	1/400,000,000.

They make the point that more can probably be gained by skipping the second redundancy and going to another part of the system, where pure oversight may be the problem.

* See ASSE, Bibliography (1967) for extensive references on control techniques.

Since good accident analysis will often show a number of possible safe-guards at several points, the above concept is helpful in bringing final recommendations down to an optimum course of action.

(4) Warnings. (Also see MORT, page 5.)

In the hierarchy of the Safety Precedence Sequence, the third item, "Warnings" seems relatively weak. However, the frequency with which accidents are followed by recommendations concerning signs, labels, etc., suggests that the presence or absence of warnings at the point of operations be a consideration in hazard analysis and JSA, and be systematized and quantified in accident investigations. Warnings can be categorized as physical or human, and dynamic or static.

Dynamic warnings include:

1. signals, lights, bells,
2. gauges with red lines,
3. lock out or tag outs,
4. change sheets.

Static warnings include:

1. Labels, colors,
2. Data on magnitudes, capacities or operating limits, energies,
3. Procedural steps,
4. Requirements, such as goggles.

Accident histories suggest that red lines be more liberally used, as simple sometimes as a stripe of red finger nail polish.

Jigs, etc., may be classed as warnings because they prevent error as well as facilitate performance.

(5) Manual Controls (Also see MORT, page 5).

(6) Safe Energy Release.

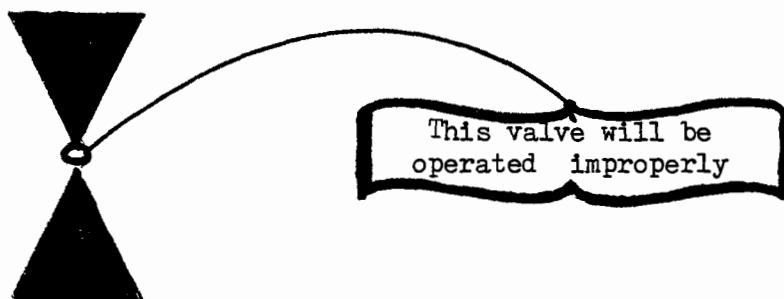
(7) Barriers.

Review Chapter 2 on the barrier idea. The first four barriers are definite parts of Concept and Design. What about the next four? They, too, can be handled in Design. Consider each kind of barrier separately for potential use, and consider barriers between energies as well as for people and objects.

Note the HE Press Explosion in Appendix A. It shows a check of Barriers for different classes of persons and objects. Don't overlook questions of shock absorption and how shock could be cushioned.

The notion of Barriers, both to separate energies and to protect people and objects should be most carefully considered for each point in the energy sequence. This analysis tests the skill and imagination, and has already been shown to be a provocative and critical series of questions in accident investigation.

What might be called the "valve comedy" illustrates a number of ideas. A valve is, of course, one example of possible barriers. However, from a design standpoint the standard symbol for valves should have a tag attached:



Labeling, signalling, shape as well as color coding, operating mode flags, locks and interlocks, and automation are all examples of possible outputs of processes above and below to counteract frequent and seemingly inevitable error.

b. Human Factors Review (See Chapter 26).

c. Maintenance Plan (See MORT, page 6, SD3; also see Chapter 31.)

Design for maintainability and inspectability should be given careful consideration, as should the specification of maintenance and inspection methods, schedules and competencies.

d. Inspection Plan (See MORT, page 6, SD3; also see Chapter 31)

e. Arrangement. This possible deficiency is like Human Factors Engineering. If there is no study, the failures may not be apparent. Here we consider space, proximity, crowding, convenience, order, freedom from interruption, enclosures, work flow, storage, etc.

f. Environment. Here we consider particularly the physical stresses (such as those cited in human factors reference material) as they may affect people or things.

g. Operability Specifications in the seven areas specified in the MORT diagram, and emergency plans. A few of these items need comment:

(1) Test and Qualification. The "dry run" or demonstration proves out, not only all associated hardware, but also procedures - checks for oversights, adjusts to final arrangement, and should provide some participation.

(3) Procedures Criteria. In general, engineers and designers are not aware of their limitations in writing procedures for operating personnel, nor of the need for selection and training criteria for operators (not the same as the engineers), nor of supervisory problems. Therefore, liaison with operators and independent review (and inputs) are needed. (See Chapter 32.)

(8) Emergency Plans are shown on pages 4 and 6 of the MORT diagrams and discussed in Part VII.

h. Change Review Procedures. The authority for changes and the review procedure to be followed should be specified. Accident reports give shocking evidence of the important role of unauthorized and undetected changes in equipment (see for example Appendices A-1, 2 and 4). It seems just plain nonsense to wait for a serious accident before specifying change review requirements. Aerojet has extensive analytic and review requirements for modifications or changes in its reactors, and extends the same or similar requirements to non-reactor work. The latter is effective on projects costing \$2,000 or more, and many below that level.

Change dockets on engineering drawings are a routine requirement. A consulting engineer reports the docket is his first step in trouble shooting. There is considerable indication that change dockets at the point of operation would be a redundant safeguard and an aid in inspecting and trouble-shooting.

In system parlance, change review should cover "form, fit and function" up the part-component-subsystem chain to a point where no change is demonstrated. Figure 5-3 will help in change review.

i. Disposal Plan. Disposal plans can include criteria for aged, obsolete equipment, as well as safe disposal.

j. Independent Review (see Chapter 28).

k. Configuration Control. As normally understood, configuration control is expressed by Aerojet in the following terms:

"Establish uniform procedures which will assure:

- a. The proper review and documentation of modifications to the reactors and associated facilities.
- b. The proper review of the procedures used in the operation of the plants.

"Use a controlled release design drawing and specification system to document design changes to the reactors and associated facilities.

"Accept, for use with the reactors, sponsor furnished systems and equipment on the basis of specifications and design drawings provided by the sponsor and approved by the Manager, Test Reactor Operations Division."

The broader problem of maintaining actual control over plant configurations at all times extends across all problems of design implementation of requirements, through manufacture, transportation, installation, maintenance, changes and field operations. A Configuration Control Analytical Tree (Exhibit 3) was developed by R. J. Nertney. This type of tree is, in effect,

a double-check on the adequacy of the entire system for controlling hardware. Exhibit 3 can also be useful in accident investigation to pin-point failure modes. Manufacture and transportation (covered by Aerojet in design specifications for manufacturing control, traceability of parts, pre-installation inspection, etc.) are not shown. If needed, the analytic processes for manufacturing and transportation are the same as is shown for initial installation.

l. Documentation. We find in NASA plans this statement:

"Effective application of System Safety requires careful planning and the preparation of appropriate documentation."

Is this different than the emphasis on written instructions which we have seen in outstanding safety programs? Yes, it is. The documentation of safety criteria and decisions by stages (preliminary analysis, definition, design and preliminary development, and development and operations) is more likely to expose assumptions (or hunches) which get lost in the final document or plan. Additionally, there is greater emphasis on the importance of detailed documentation.

During this study, serious accidents have often shown very weak documentation on design and test of the equipment involved. Investigators must then guess as to what went wrong in the design and test process.

m. General Design Process (See Chapter 27).

n. Fast Action, Expedient Cycle. Seemingly the more that is prescribed regarding hazard analysis, the more is the compulsion to emphasize the need for the kind of quick, expedient hazard removal which has characterized the effective safety engineer. This extends to the "stop operation" authority which safety staffs should have, acting through line authority, but cutting across channels as hazard warrants. However, fast action expedients are far from a substitute for the improvements which result from a well planned hazard analysis cycle.

"Fast Action at the trouble spots" has been said to be the mark of a good manager. Certainly it is also the mark of a good safety professional. Prompt and aggressive pursuit of an important hazard reduction is a necessary ingredient. "Before the fact" action is cheapest in the long run, even if organizational procedures are short cut.

Time delay between hazard detection and reduction is a quantifiable item for safety program measurement.

Questions on Planning and Hazard Review. From the preceding material the following kinds of specific questions develop:

Date of last thorough hazard review? By whom? Review and approval, by whom? Documentation?

1. With respect to physical design:

- a. Was the hazard identified?
- b. What methods of control were utilized?
- c. What methods of control were studied but found impractical?
- d. Was any research felt necessary? Had it been initiated?
- e. What public or private standards were applicable? Were they followed? If not, describe the process of approval utilized for exceptions?
- f. If process was hazardous, was remote operation possible?
- g. Could manual handling be replaced by mechanical handling?
- h. Could the task (or steps in the task) be eliminated? How?
- i. If equipment or components were purchased, describe hazard review procedure required of, or utilized by, the manufacturer.

2. With respect to safety devices (fail-safe, redundant, guards, etc.):

- a. What safety devices were provided?
What safety devices were studied and found impractical?
- b. What standards were applicable? Followed? Exceptions, how approved?

3. With respect to warnings (gauges, instruments, audible and visible signals, operating limits, etc.):

- a. What dynamic signal devices were provided? Were red lines clear?
- b. Were critical operating limits clearly posted? Were operating limits controlled automatically or manually?

4. With respect to human factors evaluation:

- a. Were the task and controls analyzed for error possibilities? When? By Whom? Describe experience or training in human factors engineering.
- b. Were controls, instruments and procedures the same for all similar equipment? If not, had differences resulted in errors?

5. With respect to procedures:

- a. Were the procedures written, or oral?
- b. Were they adequate and complete? Were they correct?

6. Were emergency procedures:

- a. Written or oral?
- b. Adequate and complete?

WHAT ELSE ?

WHEN ANALYSIS ENDS, ALL ELSE IS HUNCH !

26. HUMAN FACTORS REVIEW

Error was stated to be a major causal factor in accidents in Chapter 4. The further purpose of the early material was to suggest by discussion or examples some specific approaches to error reduction--for example, Rigby's categories of error tolerance limits (page 52) and Swain's work situation approach (page 51).

The organization's policy posture regarding error and human performance was discussed in Chapter 11, pages 122-24. Extending the policy discussion:

The reduction of errors in the design, manufacture, transportation, storage and use of thermo-nuclear weapons is a matter of such overwhelming importance that the Sandia Laboratories of AEC have a "human factors" group which is in the Human Factors and Quality Control Division of the Reliability Department. They make quantitative estimates of the influence of human performance on the reliability and safety of nuclear weapon systems. The philosophy and practice of this group, sometimes called the "work situation approach," as contrasted with a "motivational approach," is consistent with findings of human factors specialists in other areas of work. Yet, the approach, which is more or less a policy aspect of weapons work, is not widely, explicitly, or consistently used in AEC programs. Some major safety gains could, therefore, be anticipated from a conscious application of Sandia-AEC practices to work in general.

In this chapter we consider possible expedient ways in which human factors criteria can be applied to planning and investigation in the absence of a corps of experts and specialists.

Identification of situations which might have been improved by Human Factors Engineering or Review is one of the most difficult analytic problems, given the lack of professional HFE review in most situations. Experience indicates that accidents previously attributed to "unsafe acts" are often reduced after human factors review and correction. This implies that the previous description of "unsafe acts" was largely incorrect, and that we really had an "error-provocative" situation, and therefore an "unsafe condition." However, in the absence of HFE professional review, how can the real situation be appraised?

The obstacles to simple approaches to human factors (ergonomics as it is known in England) were recently shown graphically by Dukes-Dubes (1972). He charted an ergonomic process whereby:

1. Four basic scientific fields
2. Break down into eight relevant major fields, which in turn feed
3. Twenty-two scientific specialties, which in turn are synthesized into
4. Six major areas, and in turn
5. Create a science of ergonomics or human factors
6. Applicable in thirteen industrial areas and eleven non-industrial areas.

Quite a "ball of worms" for threshold or minimal entry into the field.

On the other hand, large numbers of specific applications are extremely simple, for example:

1. Design of connectors in error proof ways,
2. Shape coding of controls,
3. Numerical registers rather than dials,
4. Controls convenient to the small, fifth percentile users.

Some other recent examples of human factors faults may be helpful:

1. A small dial was cheaper than one with a larger face, so the small one was chosen.
2. A new dial in an old location was installed without any red flag to signal the change.
3. Instrument and control were separated by 20 feet, and around a corner.
4. Spurious signals foster disregard for alarms.
5. Unnecessarily tight control limits create undue stress.

The HE Press accident in Appendix A poses some human factor and error rate questions.

Are there any simple questions which can be asked about an accident (or a work situation) which would trigger an initial grasp of the role of human factors? There is a major task in reducing HFE to some simple key concepts which managers, scientists and supervisors can use as they analyze work situations. The material in Chapter 4 provides some insight and guidance.

Garrick (1967) reports some general guidelines and criteria:

- "1. Human error rate increases as a function of the constraints and demands imposed on the operator.
- "2. Human error rate is directly proportional to the length of tasks and procedures; the number of controls and displays to be operated; and the number of communications, decisions, and calculations required by a system.
- "3. The failure of system elements, both human and equipment, should be evaluated by failure mode and effect analyses. Such analyses not only evaluate the effect of human error but point out how it may be eliminated or reduced in effect.
- "4. Although the trend is to automated systems to remove the human factor (the less predictable element), it is generally desirable to incorporate human backup and consider it in reliability evaluations.
- "5. The greatest source of human error is generally found to be in the design, fabrication, and inspection of equipment (up to 80%). Subsequent to start of normal operation, human error rate can be expected to be relatively low as a direct cause of equipment or system failure. Experience indicates this to be the case in view of many design modifications, repairs, and adjustments made during pre- and post-acceptance testing.
- "6. Experience indicates that human initiated failures should decrease with completion of acceptance testing and become completely random with onset of normal operation.

"7. Human errors of a given type do tend to repeat themselves if the factors responsible for them are not corrected. These errors are symptomatic of underlying defects in design, procedures, or personnel policies."

Garrick's third point is of critical importance in system safety analysis, particularly since so many analysts fail to study the human role.

Increasing Human Factors Capabilities. We can conceive of three levels of skill which ought to be equated to size of the problem:

1. Human factors scientists--for example, those working in the weapons and some reactor programs.
2. Engineers and psychologists with HFE training--e.g., the short courses at University of Michigan or at Sandia. (Sandia also has a one semester, college level course, once a year.)
3. Other professionals without special training, but using checklists, etc.

Aerojet has one scientist in the first category, and has begun a program of training in the second category. The scientist has, over the years, given literature and information, and some training to many personnel.

Swain (1970) has also spoken of the need for a team in human factors analysis of systems or tasks - human factors specialists, engineers, operations researchers, and others. The actual use of such a team would depend on the importance of the task and mission, but the competencies involved can be brought to bear at a low level of hazard to support longer-term mission fulfillment.

The criterion for minimum good practice seems to lie in the compilation and improvement in use of design notebooks relevant to the particular organization. The costs should quickly be returned in reduced error.

For present purposes some references likely to be available to safety professionals seem to fill that need: Brody, Currie, McFarland, Tarrants, Surry, Vilardo, plus two NSC manuals--for Industrial Operations and for Industrial Hygiene. A longer, more general bibliography is provided as Appendix F, as well as in ASSE Bibliography (1967).

Within the AEC complex, a variety of studies have been produced by Swain and associates at Sandia and Nertney at Aerojet. See, for example, Description of Human Factors Reports, Sandia Laboratories, 1970. In the past year, Swain produced a new text, Design for Improving Human Performance in Production, a most useful summary of his "work situation" approach (but the text is unfortunately only available from London).

It is hard to conceive that any repetitive task of even moderate importance should not have at least minimal, checklist review--this should be an analytic criterion. How could even an amateur use of checklists do harm?

During the trials an incident demonstrated that preventive action is often quite simple. An instrument technician put a repaired instrument package into place in a panel, but plugged the package into the wrong socket, thus shutting down the process. Corrective action: shorten the cord. Many situations seem to be of this common sense type, rather than needing an in-depth study. Therefore, a simple sensitivity to the role of human factors may be helpful.

The analytic process shown in the MORT diagram, page 6 (and reproduced as Figure 26-1), confirms to some key elements described in HFE literature. Its value in investigations by other than HFE specialists has been only partially tested.

What is certain is that specific task analysis (as contrasted with more general analysis), estimation of error rates and diagnosis of error causes, can be constructive and successful in reducing errors.

a1 Professional Skills LTA. From the above defined levels of skills, determine whether the minimum level of capability is present and has been used.

a2 D/N Describe Tasks. Step-by-step analysis is a feature of even Job Safety Analysis at the craft level. But, of the designer, we can ask such questions as:

For step 1: How does operator know when to act? What to do? When he's finished? What to do next?

For step 2: Repeat.

By this analysis we begin to deal with the great range of variability in tasks, and the concept that errors are task specific.

a3 Allocation man-machine tasks LTA. Man excels at some tasks, and is flexible; machines excel at other tasks. Checklists and analytic processes exist to help allocation. Was anything done at this stage?

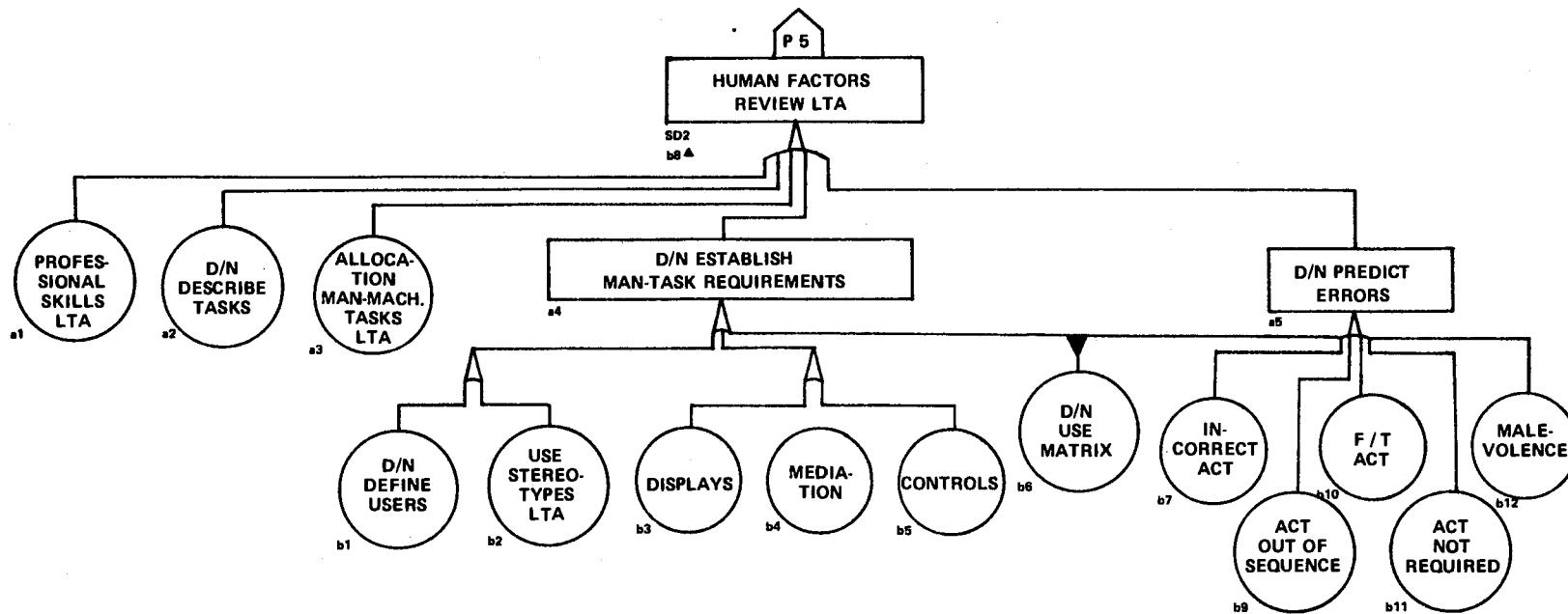
Juran (1964), speaking of business functions generally, provides a useful set of criteria (broader than the usual man-machine checklists) as to where various kinds of tasks can best be assigned in visualizing a job analysis. As modified, his list is shown as Figure 26-2.

Swain (1970) presents a number of man-machine analytic formats to be used in conjunction with a table of criteria for man-machine trade-off consideration.

a4 D/N Establish Man-Task Requirements. (See Rigby's definitions, page 2). The lack of usable task definitions has been most revealing when Rigby's criteria are applied.

Figure 26-1.

MORT Analysis of Human Factors



277

Figure 26-2. Allocating Work Functions.

MACHINE, Etc.	SUPERVISOR
Repetitive	No standards
Standardized	Changes
No judgment	Human relations
Hardware reliable	Coordination
Rapid, certain actions	Cooperation with others
OPERATOR	Violations
Work stable	Failures
Problems foreseen	not correctable
Procedures established	major
Criteria simple	Responsible agent (less bounded)
Training practical	MANAGEMENT
"Self contained"	Process under control?
Failures	Budgets
correctable	Risk decisions
minor	Responsible agent (unbounded)
Pattern recognition	
Responsible agent (bounded)	

Much human factors study has been concerned with relatively simple tasks. The tasks of a highly skilled professional or technician when operating complex process equipment present some unusual problems reported by Rasmussen (1969). From analysis of accidents in nuclear industries and air transport, he offered the following observations:

"Most of the accidents are initiated during periods with non-routine operations (e.g., initial operation, experiments, maintenance). Only a few are related to operational conditions that have developed into routine, and they are all initiated by technical failures.

"Accidents initiated by human maloperation amount to roughly three quarters of the total number of reported cases, and only in a few cases do simple accidental operations or manipulations seem to be of essential consequence, presumably because such simple maloperations have been foreseen and taken into account during system design.

"In nearly all cases the operators would have been able to make an appropriate decision and carry through the action if the actual state of the system had been known to them.

"In approximately one third of the cases ... a prescribed procedure has not been followed. ... As such procedures are not operationally optimal in normal circumstances, they are very likely to be 'improved' by the operator during his normal work at the expense of safety margin.

"The majority of the failures can be attributed to the human operator in complex, non-routine situations when he has to adjust his procedures while taking many parameters into consideration.

"..the critical task of the display system will be to support the operator in the identification of his working conditions during abnormal periods." (Emphasis added)

During this study, incidents involving complex equipment in non-operating modes (i.e., no organized data display) showed that supervisors failed to collect, organize and use available data, and further had had little guidance on such tasks.

Personnel selection criteria, where valid, will emerge from this function.

Few errors were found to be emotionally cued in a laboratory exercise, (Ammons, 1957) suggesting that objective analysis of tasks and better definitions may have strong bases.

b1 D/N Define Users. There is a great range of human variability. Was what was known about the employees who would be users, or what could easily be found out, defined and used in design?

b2 Use of Stereotypes LTA. Here we begin use of the checklists in literature already cited. Were the checklists used? Do any of the conditions in the accident violate the stereotypes? For example, do we turn a control left to move the device right? Were controls coded by size, color, or shape?

b3, b4, b5 Display, Mediation, Control requires the distinction of three components of errors. This helps identify the specific remedy.

a5 D/N Predict Errors. All tasks seem to have a basic human error rate which is relatively consistent between tasks requiring similar behavior elements. The error rates have components of the types shown in the MORT diagram, and the types help determine corrective action. Some typical error rates from Garrick (1967) are also provided in Appendix E to illustrate their nature and range. Sandia has urged increased government support for central error data stores.

The general dimensions of the error problem may be seen from (1) error rates from 1/100 to 1/10,000 per task, (2) 80-90% detected and corrected, (3) 20-30% of remainder significant, thus yielding (4) thousands of significant errors per day in larger establishments.

a4 b6 D/N Use Matrix is a cryptic allusion to the THERP method, originally developed by L. W. Rook (and reported in Recht). The matrix as further developed is shown in Figure 26-3.

The nature of the error, as classified in the matrix, becomes a guide to the nature of corrective action. And, if input and mediation are seen as information and information processing, and control as energy transfer operations, the analysis becomes provocative for preventive measures.

Figure 26-3. System of Human Error Categories

Due to acts:	Behavior Components of:		
	Input (Displays)	Mediation	Output (Controls)
Intentional - incorrect			
Intentional - out of sequence			
Unintentional - act not required			
Omitted			
Malevolent			

Rigby further suggests a classification of errors with preventive implications:

1. Random - personnel selection, training, or supervision may help.
2. Systematic - one-sided limits, or inadequate feedback, may be factors.
3. Sporadic - our most difficult type, infrequent, not seemingly related to variables in the work situation, not correctable by training or indoctrination. Relations to controllable conditions must be found.

* * *

Hopefully, an organization's human factors skills will rapidly be upgraded. However, in the interim the above analysis should produce useful ideas for plan review and accident analysis.

In Part VII, the Work Flow Process, we examine procedures, and how they may be less error-prone, and also the role of supervision in error reduction.

Part VIII tries to integrate tabulatable aspects in data collection.

27. DESIGN ORGANIZATION, RELIABILITY AND QUALITY

Much of the safety analysis described in the preceding three chapters is usually carried out by the basic design and engineering staff. In aerospace, system safety is sometimes a separate contract, subordinate to the primary design contract. In any organization, the safety group may have specific defined functions, particularly in information search and always in independent review.

During the Trials at Aerojet safety was powerfully aided by competent, well-organized design and engineering functions, and by the strong reliability and quality assurance program. As a matter of fact, it is difficult to conceive that Aerojet could have attained its present level of excellence without well managed functions.

The engineering general criteria in the revised MORT are based directly on an audit of the Engineering Division performed by R & QA according to the criteria contained in AEC's RDT Standard F2-2T:

Concepts and Requirements.

General design and plan criteria

- (1) Design planning techniques
- (2) Organizational and functional responsibilities
- (3) Interfaces with operations, maintenance, test organizations
- (4) Definition of safety-related criteria. (Operating considerations and availability, materials, fabrication, construction, test, operation, maintenance, and quality assurance requirements.)
- (5) Internal review.

Design and Development Procedures:

General design process

- (1) Procedures for code compliance
- (2) Procedures for use of new codes
- (3) Procedures for use of information
- (4) Engineering studies to assure compliance of criteria
- (5) Identification of weaknesses and analysis of "trade offs"
- (6) Provision for preventive design features
- (7) Standardization of parts
- (8) Qualification of non-standard parts
- (9) Design descriptions
- (10) Classification of items - essentiality and safety
- (11) Acceptance criteria
- (12) Identification of items
- (13) Interface control within design process
- (14) Development planning
- (15) Development and qualification testing
- (16) Test control
- (17) Development review
- (18) Failure reporting

It is not uncommon, in auditing or reviewing a design process (or a management or work process) to find that those doing the work are using some good practices not specifically provided for in their documentation. However, little permanent reliance can be placed on unstated, informal practices. They will be highly variable with different persons and over time. Therefore, specific criteria and audited performance are indicated.

The basic line responsibility for safety is carried out in the design stage by staff groups, largely engineering, but also R & D groups. Since the engineering groups do so much of the safety job and usually do it so well, the role of an independent safety function is sometimes in question.

It is argued that design engineers can understand or learn the techniques of safety, and this is in considerable part true.

Nevertheless, the independent safety function is believed necessary for management assurance:

1. Benefits of design solutions should not be permitted to obscure risk and uncertainty. The latter commonly have weaker data, and if the voice is also lost, unintended large risks will be assumed.
2. Designs and plans involve physical and human factors. The role of human, social and behavioral factors is usually better handled by specialists.

The close relationship of good design work and reliability is apparent in an excellent set of project review criteria prepared by an Aerojet reliability engineer for use in the independent review function. (See Exhibit 4.)

It must always be remembered that there are potential hazards in reliability-safety trade-offs. For example, upgrading reliability to continue to operate a process can impair protective systems. The goal must be protective systems which do not fail, and which always work when called.

The Reliability and Quality Assurance function is a strong complement to the safety program, and close mutual support is evident at Aerojet.

R & QA is also a preventive discipline--and uses problem reporting, modern analytic techniques for failure and hazard identification and is concerned with both engineered and human-based safeguards.

Safety and R & QA can mutually benefit from non-duplicative cooperation in design review, procedural control, construction/installation, operation/maintenance, and test (or test supervision) for critical equipment, e.g., cranes, pressure vessels, test equipment, etc. Recent AEC standards for R & QA include material handling (#6) and shipping (#7 in draft form). These have already stimulated problem analysis beneficial from a safety viewpoint.

28. INDEPENDENT REVIEW

Although design and production people perform major safety functions, there is ample evidence that safety will not get the attention it requires unless there is independent safety review at pre-established points, "milestones," in the life cycle process.

The independent review groups find that design and operations planners do a better job of safety when they know that there will be review, and that it will examine two facets - analytic method and technology.

Plans which are sent forward should document risk reduction trade-offs, and primary residual risks, and should state what happens in case of various failures.

One head of a nuclear criticality review group emphasized:

The review group's responsibility to search out, develop and specify analytic technologies, and cited examples.

Conventional safety approaches are negative, as compared with the positive approaches of providing analytic technology and requiring independent review.

Thus, the independent review (which is a redundancy) should have its internal redundancy - technology plus analytic method - and method is a safeguard of the true independence of the review.

AEC has placed great emphasis on independent review beginning with authorization of the reactors themselves, and extending in the field to operations, modifications, procedures and personnel. Extremely high standards are established for independence, objectivity and technical competence of the members of multi-discipline review boards and agencies.

The composition of such Boards may present a trade-off question if advanced technology is involved - that is, those who know the most may be the designers/operators of the process under review. Thus knowledge and objectivity may be conflicting criteria. (Again, prescribed analytic method is some safeguard.) Review Board membership of peers has also had great influence on the general safety climate at two sites, a collateral advantage. Group meetings are required, and unanimity is a requirement; one "No" vote produces a negative recommendation to management for a proposal. The role of the Safety Department is usually fulfilled by Board representation.

Aerojet policies require line management to show positive evidence of independent review, and a "water cooler" chat will not suffice. Aerojet has an extremely well developed independent review system. In Aerojet review the definition of "independent" has been raised from the original and usual concept of redundant safety analysis. The further effort is not to have the

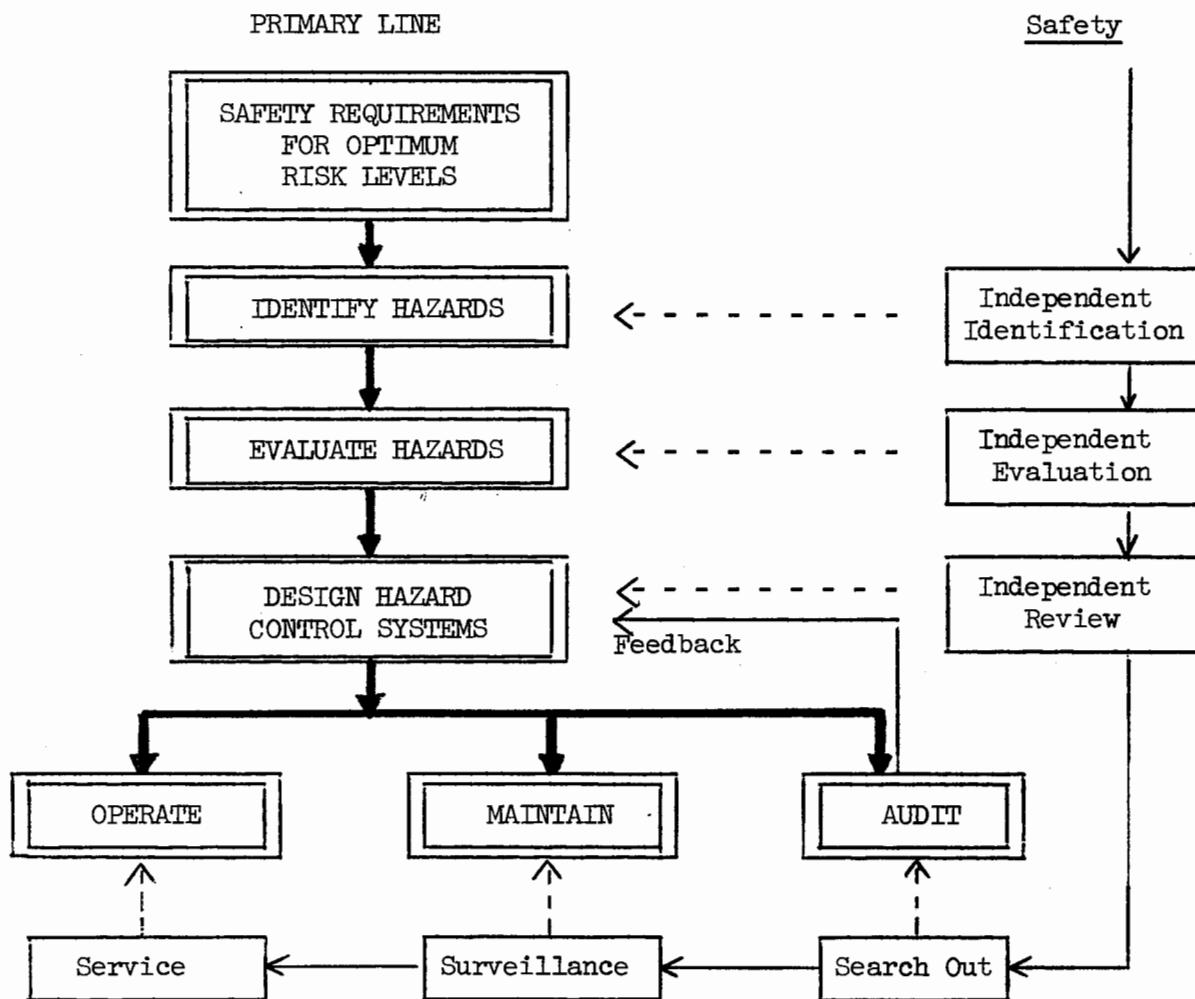
person who supplied the safety inputs involved in the review, and ideally not his associates. (This avoids "incest!") Such a procedure is difficult for a small staff. In fact, the question can be asked as to whether an independent review function can be overemphasized as compared with other essential functions in the Hazard Analysis Process - if HAP is not well done, e.g., if there is no information search, there may be too much to catch in review.

Aerojet has a short cut procedure - many changes which are improvements in safety can be reviewed and quickly approved orally, and documented later.

At Aerojet the Nuclear and Operational Safety Division reports directly to the Chief Executive Officer - it is independent.

An NOS section head at Aerojet had a useful overview of his independent review function:

Figure 28-1. Independent Safety Functions



In early work at Aerojet (successor to Idaho Nuclear) the relationship of various independent review plans to the life cycle was conceptualized in Figure 28-2. The abbreviations are:

T & Q	Training and Qualification
NOS	Nuclear and Operational Safety
R & QA	Reliability and Quality Assurance
SWP	Safe Work Permits
RDT	A reportable incident
FS & OC	Fire Safety and Adequacy of Operating Conditions list

The multiplicity of review points and mechanisms, including a triennial board to review the review system, is a truly impressive effort to create safeguards against oversight.

The Aerojet review system has elements much broader than simple, independent review of the Hazard Analysis Process. While some of these elements can also be seen as field safety engineering, annual audit, monitoring or accident investigation, it seems best to describe the Aerojet review system as Aerojet conceives it (See Figure 28-3). The Figure is explained as follows:

A. The Process

As indicated by the heavy blocks in the top row, the process to be audited and reviewed may be broken down into five subprocesses:

- (1) The personnel process which is designed to produce "reactor grade" personnel at the various work sites.
- (2) The procedural process which is designed to produce "reactor grade" procedures at the work sites.
- (3) The hardware process which is designed to produce "reactor grade" hardware at the work sites.
- (4) A reactor modification and experiment process which functions on an intermittent basis to result in modification of the reactor-experiment complex. This is not a separate process but represents a functional, coherent application of (1), (2) and (3) above.
- (5) Other activities which are related peripherally to nuclear or reactor safety and/or involve safety considerations other than nuclear and reactor safety.

B. The System "Gates"

The middle set of blocks indicate the independent review agencies which are interposed as "gates" between defined processes and field application of the processes or process products.

These review agencies consist of multidisciplined groups selected according to the nature of the subject under review.

They conduct independent review of the process and/or the process product and/or proposed activities prior to field implementation. Approval action may be associated with these activities as delegated by line management.

C. The System Audit Processes

These are on the left and consist of two basic sorts of audit processes:

- (1) Audit processes which audit preparatory work being performed upstream of the field activities.
- (2) Audit processes which audit actual field activities.

Based on
Idaho Nuclear

Figure 28-2

At the start Millions of Potential Mistakes

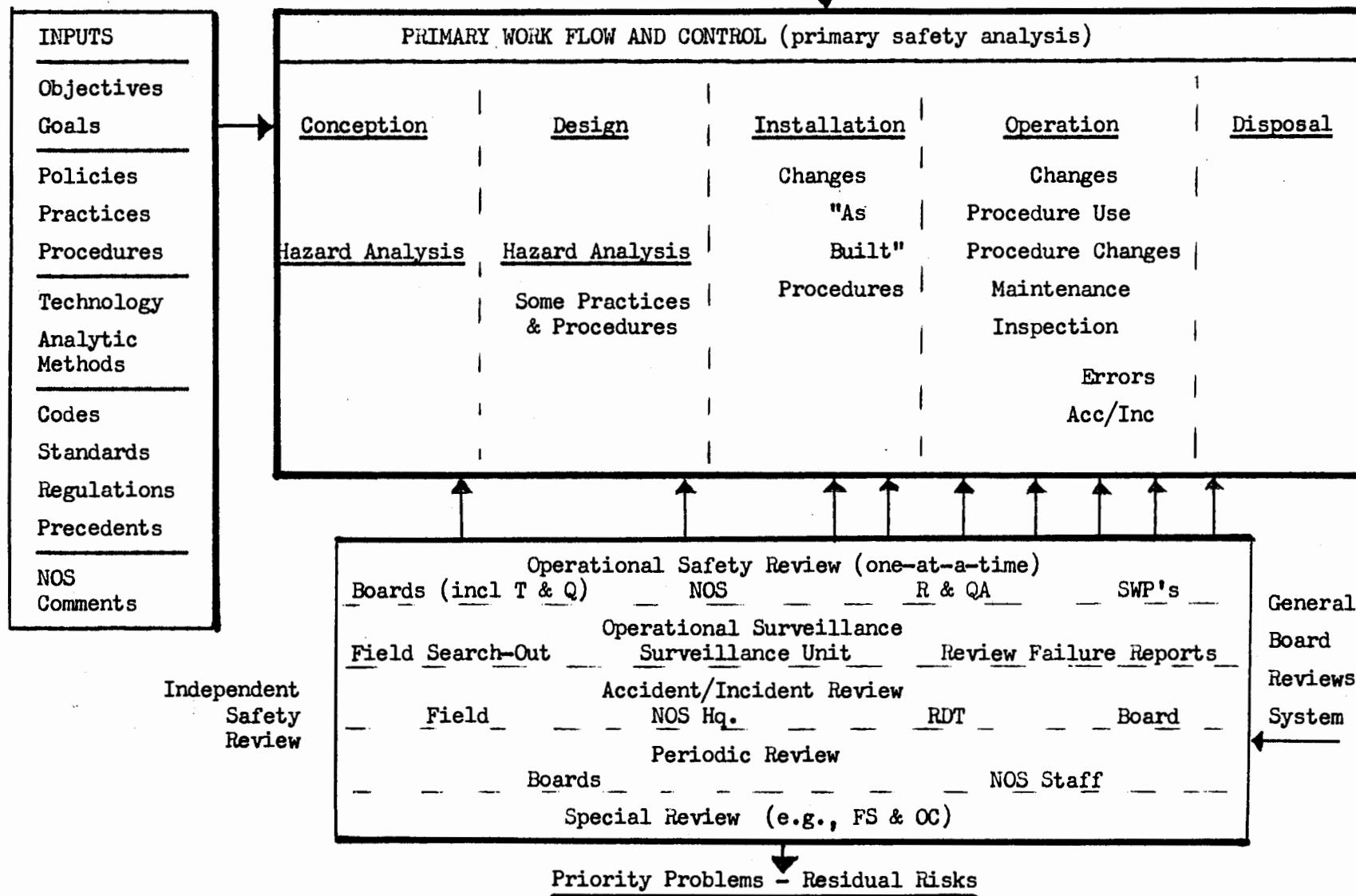
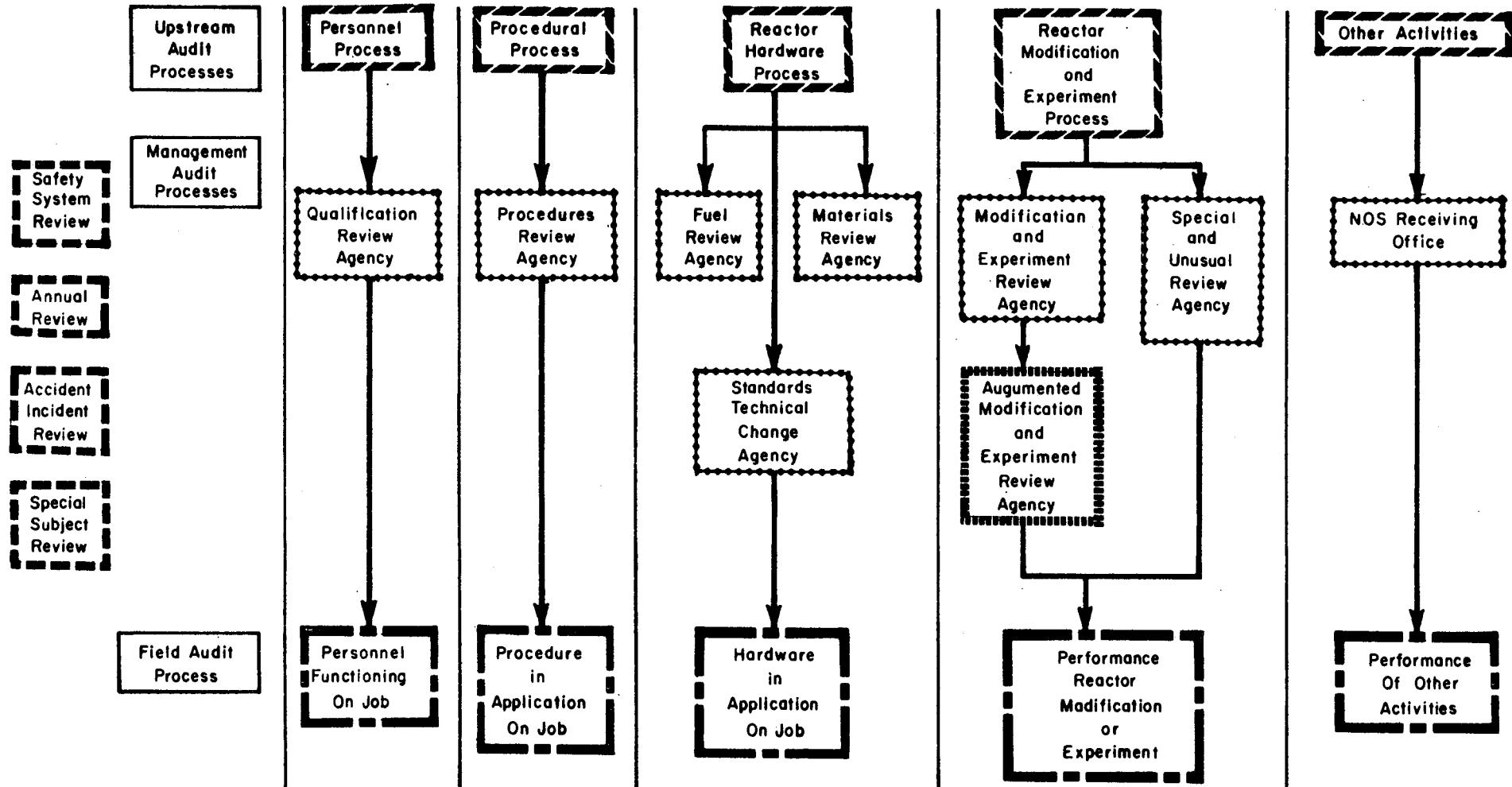


Figure 28-3. Aerojet Review System



- 287 -

ANC-B-850

D. Process Oriented Review Activities

These are review activities on the far left. They are designed to review overall process design, process function and certain types of malfunction (accidents and incidents).

These review agencies consist of ad hoc multidisciplined groups selected according to the nature of the subject under review.

There are four classes of process oriented review agencies:

- (1) The safety system review boards which perform management review of the safety review system itself.
- (2) The annual review boards which conduct annual reviews of the major company projects and activities.
- (3) The accident and incident review boards which conduct reviews of certain types of accidents and incidents.
- (4) The special subject review boards which perform reviews of selected subjects relevant to nuclear and operational safety, e.g., shipping of radioactive materials, electrical safety, monitoring systems, etc.

Most of the review agencies have published the criteria which they will use in review. Such publication has important effects on improving the prior hazard analysis. (See MERB Board criteria, Exhibit 5.) The criteria used by one review board member are shown in Exhibit 6. It will be noted that the form provides for scoring a proposal. This has had a marked effect on quality.

Dr. Nertney prepared Exhibit 7 to display some of the factors which affect redundancy and independence. Dr. Nertney also developed a detailed Fault Tree to facilitate analysis or development of a review system (Exhibit 8).

The safety department's "receiving office" is the focal point for review of projects other than reactors and critical facilities. Coverage of projects over \$2,000 is comprehensive due to internal controls, and much is reviewed below that level. The proposal routing sheet (Exhibit 9) will indicate the scope and depth of coverage. Each reviewer has criteria specific for his role. By way of example, the fire reviewer's criteria are shown in Exhibits 10 and 11.

The annual reviews and accident reviews are thorough and exemplify good audit and investigation procedures (part of what the author classifies as Monitoring).

The list of review topics for which special boards are appointed is interesting:

<u>Topic</u>	<u>Frequency</u>
Transportation of Radioactive and Fissionable Materials	1 year
Site Electrical Systems	2 years
Training and Qualification	1 year

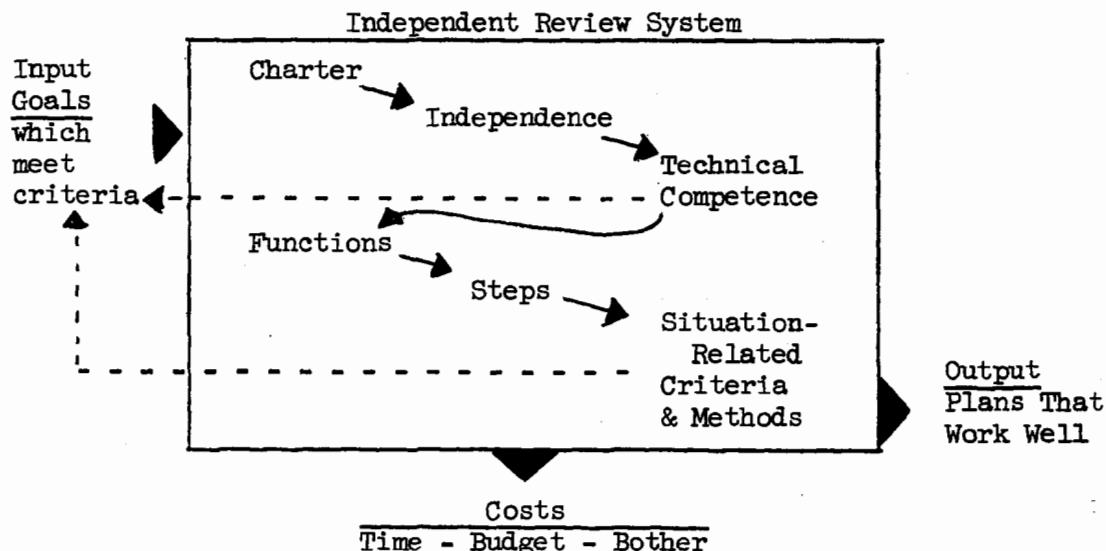
<u>Topic</u>	<u>Frequency</u>
Overall Safety Review Program	3 years
Waste Management	1 year
Radiation Monitoring and Detection System	3 years
Definition and application of AEC Codes, Standards and Regulations	2 years
Reliability and Q/A Activities	2 years
Internal Procedural Control Systems (including Surveillance and Audit)	3 years
Handling of Fissionable Materials (out of reactor)	3 years

Aerojet's superlative review system is the product of several years building and development. The system has a high degree of objectivity and independence. Despite its apparent complexity, it is economical; the work is spread widely among board member pools. The system is simple to use; refer a proposal to an appropriate Board or to NOS, the rest is automatic.

In 1972, as criteria were developed and were scored, it was most interesting to see high criteria and searching analysis increase spontaneously from those participating in the review process.

The major factors which can affect the quality of an independent review system can be expressed in a schematic, as shown in the Figure below:

Figure 28- . Factors in Independent Review



This page intentionally blank

VII. WORK FLOW PROCESSES

A schematic or model of a work flow process is used to analyze and suggest improvements and measures of supervision, maintenance and inspection, procedures, employee selection and training, and task performance.

A sequential approach to these factors in a work process permits an increasingly probing examination. Thus an incomplete hazard analysis process, or a faulty supervisory or procedural process must be examined before the roles of employee factors can be correctly assessed.

The discussion of supervision examines common failures in terms of the services and assistance provided by higher supervision, and thus reasserts management responsibility.

Last, employee motivation, participation and feed-back systems are examined.

This page intentionally blank

29. GENERAL SCHEMATIC OF WORK FLOW PROCESSES

During the Aerojet trials of MORT, as an offshoot of the major initial task of developing an adequate monitoring system, a need was seen for an overall concept of a work flow process, stemming from a management decision process and a hazard analysis process. Specifically, major monitoring resources had been focused almost exclusively on the work site, rather than the full scope of relevant events. It quickly became clear that the "upstream processes" (design, training, etc.) which produced the ingredients of work--hardware, procedures, and people--should be scrutinized, as well as actual work site operations. Also, some major ingredients of safety at the work site could be shown.

The schematic which evolved is shown in Figure 29-1. The hardware used at the work site proceeds from two major processes--(1) the original design (covered by a Safety Analysis Report, construction, and Test and Qualification, followed by documents on Operating Limits and Technical Specifications) and (2) Modifications and Projects (proceeding through a hazards analysis process, through a Configuration and Document Control unit, and then through one or more of several independent review gates, such as a Modification and Experiment Review Board, Procedures Review Board, or the Nuclear and Operating Safety Unit). Technical Support (scientific and engineering) is needed in both hardware processes. The hardware requires the kind of Maintenance and Inspection discussed below.

Procedures, for a highly technical operation, emanate from operations management, but are supplemented by craft manuals, job safety analysis involving work site people, and a Safe Work Permit issued by the safety unit for jobs which involve any hazard. The procedures become a basis for training of various classes of personnel.

The Personnel subsystem shows roles of higher supervision and certain categories of personnel. The aspects abbreviated are:

S = Selection

T = Training

T/Q = Test and qualification

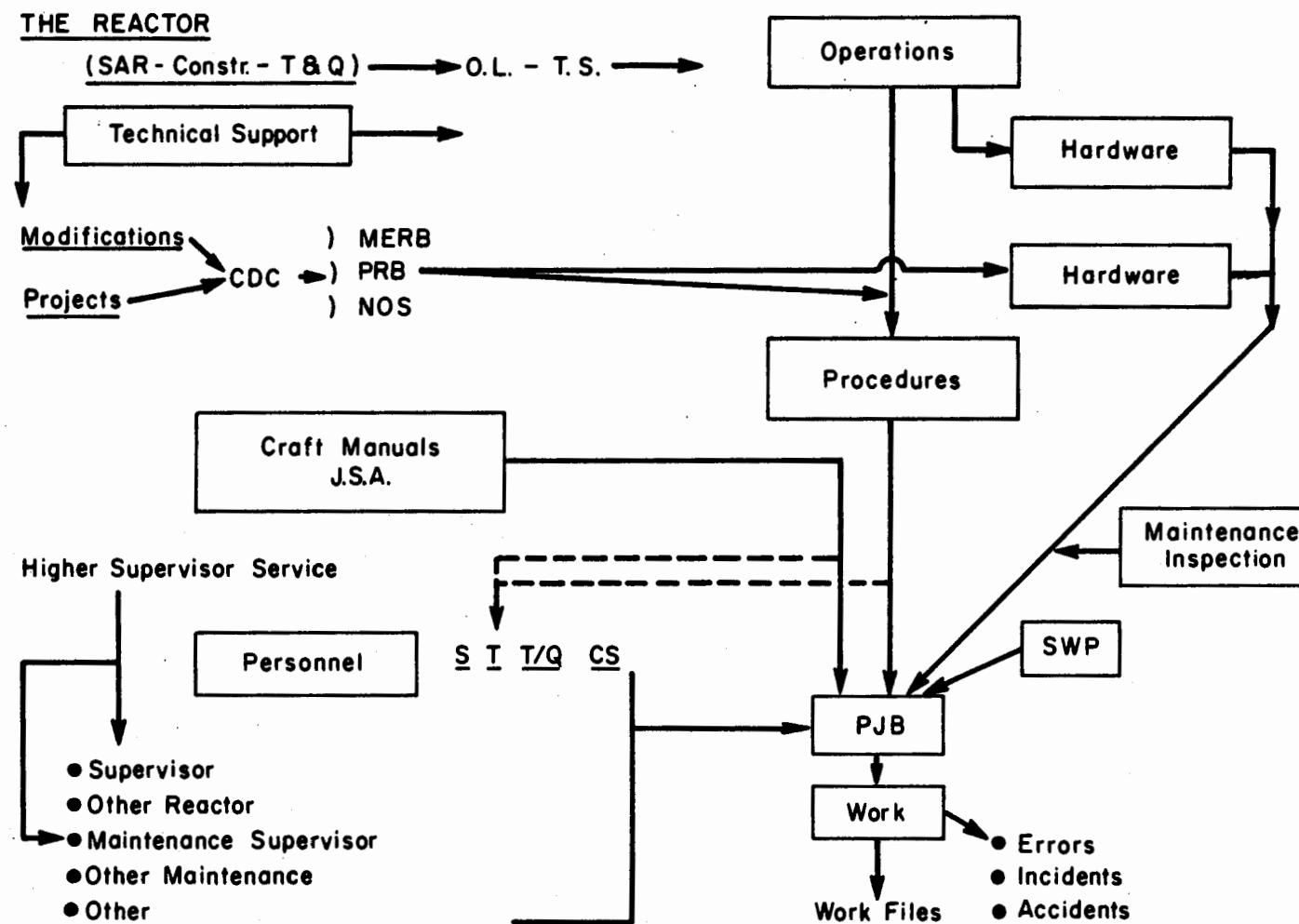
CS = Continuous surveillance, e.g., for errors, personal changes, or medical factors.

A Pre-Job Briefing (PJB) is shown as an essential factor in acquainting personnel with the particular job, changes from prior work, emergency plans, and operational readiness review at the point of operation.

Errors, accidents and incidents are shown as unwanted by-products or deviations.

Figure 29-1.

A BASIC SAFETY- RELATED WORK SCHEMATIC



See text for definitions of abbreviations.

Work files are shown simply as an audit point for monitoring procedures, review and sign off.

This basic, safety-related work schematic has proven to be a useful tool in designing monitoring programs, as well as up-stream and work site safety programs. The discussion in this Part follows the organization of the schematic, except that hardware processes are considered to have been fully discussed in the prior Part on the hazard analysis process.

All "upstream processes," including the Hazard Analysis Process, are susceptible to constructive analysis as "work processes" in themselves. That is, design, or training can be analyzed as to the hardware, procedures and personnel they utilize. Thus "work process" may be like a succession of mirrors extending back to an original idea or concept.

The remainder of this Part is organized as Chapters:

30. Supervision
31. Maintenance and Inspection
32. Procedures
33. Employee Selection and Training
34. Performance Errors.
35. Employee Motivation and Feedback.

Among the kinds of upstream processes for hardware analyzed during the Trials at Aerojet were such aspects as a tool room controlling inspection and maintenance of tools, and the plans and operations whereby such equipment as anti-contamination clothing and health physics instruments were delivered to the work site. In all of these kinds of supplementary operations, the finding in major operations was repeated - namely, that an initial walk-through audit of operations produced a schematic, steps, and criteria which immediately highlighted gross deficiencies. This was true even though processes were under direct management of the safety division itself. Plans and specifications were unreviewed, less than precise, and sometimes unknown to those in the process, and actual operations differed widely from the theory and the advertising. The need for auditing of upstream hardware processes was thus shown for both major and minor hardware, and for hardware under operations and safety management.

The general conclusion was:

Adequate work site control and safety cannot be achieved unless high quality of "upstream processes" which produce work site ingredients is audited and assured.

This page intentionally blank

30. SUPERVISION

The function of supervision has been so much examined, and from these examinations has come such a flood of literature, that one more dissertation might seem unnecessary and fruitless. Certainly supervisors have an adequate supply of advice on how they should do their jobs. What is not apparent in review of the literature is that factors beyond the control of the supervisor, namely under control of higher supervision and management, have had the attention they deserve.

The role of the first line supervisor in safety has been characterized as "the key man." While this may be good propaganda for supervisors, it is akin to the fallacious data which so often assign 85% of the responsibility for accidents to the "human factor."

There can be no doubt that the supervisor is a key man in safety.

The emphasis on supervisor training is appropriate and seemingly effective.* Large organizations have developed many such programs. Members of NSC use a tremendous amount of the Council's training materials. Recently, NSC has expanded its training function to make its "Key Man" course widely available through local safety councils. Other training programs are widely used; for example, Lateiner (1969) has been active in the field since at least 1947 when he and the author were assisting the New York Transit Authority.

The emphasis on the role of the supervisor is, however, probably just a step on the road to a superlative program. The supportive functions which emerge from this study (as well as the emphasis on management oversight and error) amount to a rather drastic change in the advertised role of the supervisor. If the supervisor is to fulfill his responsibilities, he must have the following kinds of supportive services, over and above general training and training in such subjects as Job Safety Analysis.

1. Top and middle management support and assistance as evidenced by specific actions prior to serious accidents,
2. Monitoring services which tell how his operation is functioning,
3. Data in usable form, such as Shewhart control charts for accidents and errors, diagnostic cause data, and access to national data or cases as relevant.
4. Finally (or first) equipment and work situations which have the highest possible degree of safety and reliability, including staff study of human factors. This implies upper management planning and audit of the "upstream process" which produce work site ingredients.

*See pages 195-97.

This list is suggestive rather than exhaustive, but seems to make the point.

An illustration may be helpful. AEC, NASA, and such industries as steel-making have need for ultra-high reliability in overhead and mobile crane operations. Yet when Clark of Aerojet examined crane operations and national data against MORT standards, he found gross deficiencies, including lack of human factors analysis. Now suppose a very serious accident occurs in a crane operation - is it due to an operator deficiency or a supervisory deficiency, or is it due to deficiencies at the national level, including crane manufacturers and purchasers?

There is a difficult duality in assessing supervisor responsibility after a serious accident. No one can argue against a searching and hard-nosed assessment, but the assessment of management's role in support and service to the supervisor should be at least as searching and hard-nosed!

The general framework of this chapter is, then, an examination of supervisor failures in a broader context, rather than a basic essay on supervision as such. The general framework also presumes that a competent hazard analysis process lightens the load on supervision, and that he has competent and useful advice and support on such matters as procedures, job safety analysis, and employee participation and support for the safety program. In brief, MORT traces supervisory failures to deficiencies in higher supervision, a seemingly unique way of viewing aspects of safety supervision.

The function of Supervision (not the individual supervisor) must be examined as one of the organization's primary methods of controlling Error, so-called "Unsafe Conditions" and "Unsafe Acts." The focus is on the organization for control, rather than the individual employee's unsafe actions.

The functions of supervisors are sufficiently numerous, time-consuming and divergent to deserve listing and study:

1. Basic Management functions:

- a. Production
- b. With safety
- c. Accountable for performance.

2. Special safety functions:

- a. Planning
- b. Procedure
- c. Employee selection, training, motivation
- d. Monitoring, inspecting and observing to detect deviations
- e. Hazard review and reduction.

Quite a load! And, as we begin to measure more precisely where this element in the system fails, the questions of adequacy of compensating assistance

to the supervisor functions will grow.

Most important, we must try to discover what in the management system failed - not who.

Roethlesberger (1968) described the many constraints and duties under the title, "The Foreman: Master and Victim of Double Talk." He said the supervisory position often embraced fourteen knowledge areas, many of which had a staff department to which the supervisor must relate. He found that, despite official doctrine, the supervisor commonly gave up and concentrated on performance - getting the work out on schedule. Thus, management assistance and the usable outputs of a safety program from the supervisor's viewpoint constitute the first dimensions to be examined.

The MORT analysis postulates an extremely high degree of supervisory control. Some might say it could be attained, for example, in steel making or at reactors, but not in other types of work such as maintenance. If this be true, the analytic method need not be changed; rather collect objective data on the deviations from high standards, and then make judgmental allowances in reviewing the data on degree of control.

In any organization, investigations should reflect the supervisory control criteria actually in effect in the organization, as well as MORT criteria. Thus, two kinds of measurements are made: against organization norms, and against MORT standards.

The first three basic problems (top left of page 7 of the MORT diagrams) are, in effect, questions about the institution of supervision. It is well, first, to ask some general background questions:

1. Were the supervisor's responsibilities clear? Were there any gaps or overlaps in the supervisory assignments related to the event? Was inter-departmental coordination a factor?
2. Describe the measures of general performance available for this work area (waste, quality, rework, etc.).
 - a. What was the most recent trend of such indices?
 - b. Have there been recent incidents in general performance which were less than satisfactory? Satisfactory? More than satisfactory?

Using the MORT diagram system of classification and notation:

all Help, Training LTA. The help and assistance given to supervisors to enable them to fulfill their roles may be grossly deficient.

Feedback is an all important need (cited in the literature and in MORT analyses). However, deficiencies in feedback systems seem to be frequent in three areas:

1. General feedback on a supervisor's performance seem LTA, judging from the literature.

2.. Specific feedback on safety performance is LTA.

3. The organization's triggers for HAP, or its monitoring and surveillance are frequently deficient. This puts a greater burden of hazard detection on the supervisor.

Examples of deficiencies in feedback service to supervisors are not hard to discover. If monthly charts of first aid or other injuries are supplied without assessment of statistical significance (e. g., quality control charts with judgement limits), the results are capricious and unfair, and put an undeserved burden on the supervisor to be his own statistician. At one site such charts were used, were effective, and yet were dropped for "budget reasons." Today such charts can be printed out by the computer, usually from data already stored in the computer.

At Aerojet, such control charts showed that supervisors were apparently able to control errors near the lowest limit of previous wide fluctuations by simply applying normal administrative controls; but the process took a year to implement. (This facet is further discussed in Monitoring Systems, Chapter 37.)

It is perhaps not so important what supervisor assistance program be used, as that results be assessed. For example, Lateiner (1969) discusses Modern Techniques of Supervision and claims reductions of injury incidence on the order of one-half in many organizations using his program.

Leverage for safety unquestionably can be focussed at the supervisory level. The principal question is the form of the program, and the assistance given the supervisor in implementing the program.

Hannaford (1965) outlines a "Supervisory Factor Analysis" wherein the supervisor's supervisor reviews, not only a Job Safety Analysis, but also the supervisor's general effectiveness in directing work operations.

Aids, forms and materials can help the supervisor. Some might see the recording procedures of U. S. Steel's Job Safety Analysis - Job Instruction Training - Safety Observation Plan (JSA-JIT-SO) as onerous, but no one could help but feel that the company had gone to great ends to help the supervisor carry out his responsibilities as outlined in Figure 30-1 on the next page.

Training. What training had the supervisor been given? In general supervision? In safety? Has the training program been evaluated? How does it measure up?

Since safety programs generally have emphasized subject matter rather than hazard analysis methods, we must ask whether safety training provided analysis methods, including practical handling of emergencies.

Figure 30-1.

BASIC ESSENTIALS



**PLANT SAFETY
PERFORMANCE
REPORT**

**MONTHLY
CORPORATION
REPORT**

**JOB SAFETY
ANALYSIS**

**SAFE JOB
PROCEDURE**

**AWARENESS
CHART**

**INJURY
EXPERIENCE**

**EMPLOYEE
RECORD**

**ACTIVITY
REPORTS**

**FACILITIES
EQUIPMENT
INSPECTION**

Basic Training Individual Contacts
Safety Observations

We could expect the supervisor should have had training in JSA-JIT-SO (by any local nomenclature). Had he?

Many supervisor training programs are understandably long-term - that is, a topic or a series of training meetings may be repeated only infrequently, or not at all. Therefore, it is important to ask the what and when of supervisor training as they relate to specific accidents. The immediacy of supervisor training needs is exemplified by Aerojet's provisions:

"Great stress is laid on the supervisor's responsibility for the safety of his employees and management helps the supervisor learn how to discharge these responsibilities.

"Each new supervisor (foremen included), whether promoted or hired in, must attend a safety indoctrination conducted by the Safety Section. This indoctrination covers responsibilities and procedures peculiar to the Company. In addition, this new supervisor is loaned a copy of the National Safety Council's Supervisors Safety Manual. Within four weeks, the supervisor must return the manual and pass a written test on the material in the manual.

"For a number of years, we have used successfully a Supervisors Safety Program patterned similar to the regular employee safety meeting program. It works in this manner.

"The Safety Supervisor selects several suitable subjects and discusses them with Management until four are selected for a years schedule. One subject is presented each quarter in a series of 30 to 45 minute meetings arranged to accomodate all Supervisors at all plants. A schedule of subjects, meeting times, dates and places is prepared by Safety and given to all Supervisors prior to the first meeting each year. The subjects are assigned to members of Health Physics and Safety to prepare, or if on a technical subject to a specialist in that subject field. A typed copy of the presentation is given each Supervisor who attends. A complete numerical analysis of attendance at each series is given Management with a list of names of Supervisors who failed to attend. Action by Management keeps attendance very high. Some subjects we have used included:

Psychological Needs and Importance of Safety in Supervision
ASA-Z16. Recording and Measuring Work Injury Experience
Hazardous Chemicals
Idaho Workmens Compensation Law
Selling a Safety Program and Conducting Safety Meetings
Movement or Handling of Radioactive Materials
Correct Use of Tools
Fire Prevention and Protection
Accident Follow-up
Enforcement of Safety
Hidden Accident Expense and Risks"

On the Job Help may be deficient. Since accident reports on relevant safety work of middle management are few, this remains to be assessed.

If directives for procedure development are LTA, unenforceably high, the supervisor's role may be unclear.

Thus, at least four general areas of supervisor preparation are presented for investigation and measurement.

The vigor and example of the supervisor will have important effects on employee behavior. People mirror the behavior of their bosses. Equally, the effects of the behavior of the supervisor's boss on the supervisor will be great. Therefore, objective questions should be directed to this point. What was the nature and frequency of middle management display of safety concern prior to the accident?

Continuing with the MORT analysis, we have:

a2 Time LTA. Accidents analyzed in this study suggest supervisors may have neither the help nor the time they need.

Objective data on the supervisor's degree of control will enable management to judge whether it has provided the basis for the degree of hazard control which it desires. How frequently can the supervisor thoroughly examine each job?

a3 Transfer Plan LTA. When experience in present or previous jobs was analyzed in some accidents, recent transfers of supervisors were indicated to be a common problem.

The transfer protocol was examined and found to be largely non-existent! In certain kinds of work, the safety documentation exists in the department; others, not so. In no case was there any requirement for orderly transfer of safety information, including information on personnel, from the old to the new supervisor. When one plan was described by the author as, apparently, "A slap on the back, and 'good luck'!", no contrary evidence came forth.

Where reactor supervisors must pass a T & Q Board exam, on the other hand, their supervisors take steps to see that they are qualified. This is an exception. What was the supervisor's experience in this department? In this type of work? How was he trained? Aerojet has a practice of maintaining hazard catalogues for various areas - this facilitates orderly transfer of responsibilities for both supervision and safety personnel.

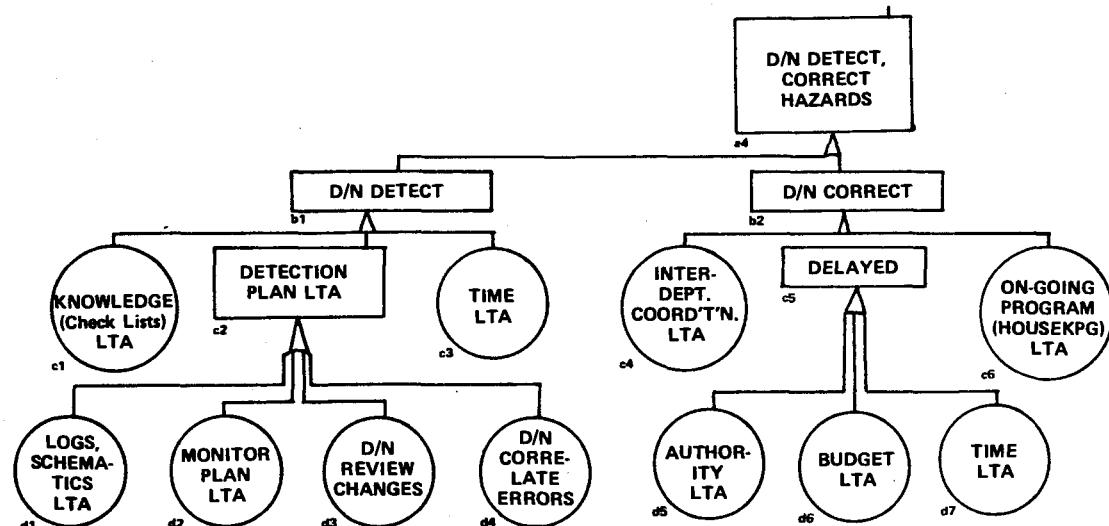
At this point it may be well to repeat a portion of the MORT diagram in Figure 30-2.

To a considerable degree knowledge of hazards reposes in the work force and must be elicited in suggestions or in formal "critical incident" studies. The skills of a supervisor in developing suggestions and innovative ideas are discussed in the Chap on Motivation. Certainly the supervisor must be receptive and accessible, and must display vigor in acting on suggestions if he wishes to have access to the knowledge which is all around him.

b1 D/N Detect Hazards.

Some questions which may be useful are: When did the supervisor last make an inspection of the area? Was a checklist used? Did it cover the factors in this accident? Was the checklist complete, correct, clear, up to date

Figure 30-2. Supervisor D/N Detect, Correct Hazards



and tailor-made for his department?

- a. Was any unsafe condition present in this accident, present at the time of inspection? Was the condition detected?
- b. When and why had conditions changed?
- c. When was the next inspection scheduled?

If Appendix A is consulted to see how many physical defects occurred in the environmental chamber case, or how many errors were made in the MAPP and Initiator accidents (and similar cases are in the file), the question of supervisor detection of hazards takes on new significance. These cases showed gross deficiencies in detection mechanisms, such as to warrant searching inquiry. The number of deficiencies was not such as could likely arise spontaneously, just before the accident. These findings also show clearly why "single cause" data may be harmful.

c1 Knowledge (Checklists) LTA.

This simple item opens a large area embracing the full content of all jobs in the organization. ASSE's Search I thoroughly examined the strengths and weaknesses of checklists, and concluded that a checklist specific to the operation was valuable provided it concluded with open-ended, general questions. So, in an investigation, we can ask about the availability and use of such lists, as well as the general competence of the supervisor in his area of work.

c2 Detection Plan LTA

d1 Logs, Schematics LTA. Significant numbers of accident reports recommend point-of-operation posting of schematics, procedures, warnings, emergency procedures, continuous test permits, change, maintenance and inspection logs, and lock-outs or tag outs. This finding is so frequent as to probably warrant

a generalized requirement:

Documentation should be conspicuously posted at point-of-operation for the kinds of events listed above.

Exceptions should be variances from the general requirement only after a finding of no need.

Accidents indicate a "change tag" should be attached to equipment when it is changed. Changes made for one job create surprises for the next user.

Not only will such a requirement be very helpful to employees, but their responsibilities for maintaining and reviewing documentation can be increased.

Note how the supervisor's job changes. Instead of relying entirely on detective skills to find out what's moving out of control, he is aided by on-the-spot, visible records! And monitors, too, can do a quicker, better job of monitoring.

d2 Monitor Plan LTA. What guidance was given the supervisor in inspecting and monitoring? Did he use the guidance? Was he required to have any given frequency of personal contact with employees? And, if so, was he given guidance on detection of such growing problems as alcoholism, drug use, or personal problems? The medical staff can assist the supervisor in four ways: (1) by giving training and advice on detection, (2) by its own alertness to symptoms, (3) as a referral resource, and (4) as the source of conclusions from general health monitoring.

d3 D/N Review Changes. What guidance was given on review methods and change detection? Did he use the guidance? Questions are:

- a. Were the changes involved known to the supervisor? If so, describe the hazard review given each known change.
- b. What counterchanges were made for the known changes?

d4 D/N Correlate Errors. Were there any chronic errors afflicting the process? Had the supervisor been told they might correlate with safety errors? Had he made the effort to correlate?

Were there any other signs, signals or warnings that the process was moving out of control?

c3 Time LTA. Objective data may be collected by the following kinds of questions: Where was the supervisor at the time of the accident? How far away? Was there an assistant supervisor in direct charge? Where was he?

b2 D/N Correct Hazards. Some facts about non-correction were dealt with in detection. But some basic factors remain to be examined.

c4 Inter-Department Coordination LTA. A seemingly significant number of accidents are "two-department" accidents. How many? Since this kind of

coordination is a key responsibility of supervisors (rather than operators) we should measure the factor.

c5 Delayed. These are risks supervisors may have to assume on behalf of management due to limited authority, budget or time. How frequently do they occur?

c6 On-Going Program (e.g., Housekeeping) LTA. Housekeeping in some laboratories is about as poor as can be imagined or tolerated. The Hilac report pointed out losses due to poor storage plans. The AEC's "Electrical Safety Guides for Research" (Paragraph 1b (5)) points out electrical hazards in poor housekeeping. On the other hand, the true role of housekeeping in the accident experience is unclear. Laboratory personnel may have developed a compensatory adjustment to gross housekeeping deficiencies. The situation suggests need for an evaluation of present practices, potential gains from improvements (e.g., salvage and reuse of equipment, research quality improvement from elimination of sloppiness, etc.) and enunciation and enforcement of realistic and appropriate policies and plans.

When asked for an estimate of how much material disappeared from laboratories during a clean up campaign, one safety engineer said, "About half!"

Parts stored in small laboratories become obsolete or deteriorate and create hidden losses.

Emergency Preparedness Plans.

As would be expected, the National Reactor Testing Station has well developed emergency plans. One feature is worthy of note - a computerized photograph retrieval system. This is used not just in emergencies, but to describe planned changes and to give instructions to designers or craftsmen. It helps avoid embarrassing mistakes.

Emergencies and Problems.

Accidents/incidents investigated during this study reveal a significant frequency of emerging events or sequences which were mishandled by supervisors. Such reviews are, of course, retrospective - that is, 20/20 hindsight! However, these events prompted a literature search on emergency problem handling, which produced almost nothing on the supervisor's role and conduct in emergencies (other than named events for which a solution was structured). The analytic and decision mechanisms to be used by supervisors in handling unnamed or unstructured emergencies and problems are not described, other than broad injunctions to "maintain control, not panic, and act wisely." Such advice to a man in trouble seems to have slight value.

An examination of a variety of training outlines for supervisors showed

a vast range of topical concerns, but nothing on the unstructured events which seem to get supervisors into trouble, and often with serious repercussions for the organization as well as the man.

Emergency Preparedness Plans as conventionally conceived are a valuable and necessary part of safety planning. Examination of such plans reveals that the emergencies conceived are on a "MACRO" scale, and highly structured, e.g., for tornado, flood, major fire or explosion, etc. Such plans are obviously good, but seemingly give little guidance as to what a supervisor should do in lesser, unnamed emergencies - especially when these occur on the graveyard shift, as they frequently do.

In consequence, Aerojet personnel and the author endeavored to construct a problem-solving routine which could be a basis for training, and hopefully subsequent, practical action.

In studying emergency action, one can distinguish "MACRO and MICRO" events - the former being large-scale problems of a defined nature and with pre-defined solutions. However this distinction blurs when procedures are highly defined and call out such emergencies as can be conceived and handled by pre-planned actions. A great deal of sweat should go into these definitions of pre-planned action. Simulation of conceivable emergencies is a valuable training approach.

However, after all MACRO and defined MICRO events are handled in this manner, there remains a substantial number of emergencies or problems to be handled by direct supervision.

The model of decision processes in an accident sequence (Surry, Figure 4-1) may be useful in studying emergency action, especially as it develops over a time period of at least several minutes, or perhaps a half hour or more.

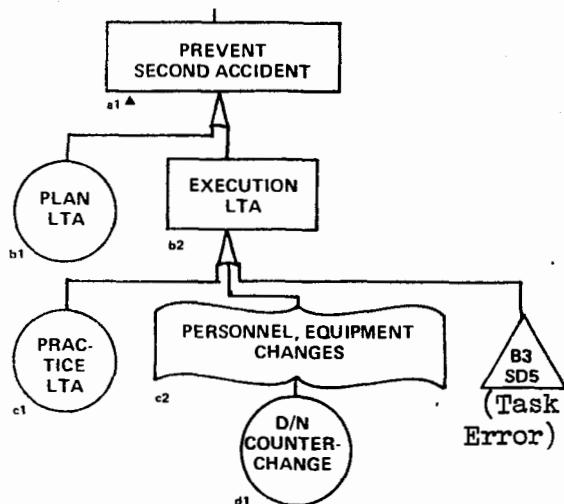
About two-fifths of the critical incidents (RSO's) reported at Aerojet were case histories of good solutions of incipient or emerging problems, but study of these to detect emergency problem handling mechanisms, other than frequent references to close monitoring and quick action, has not been carried out, and might not be feasible for cryptic RSO reports.

In discussion, it seemed that the Kepner-Tregoe method outlined in Chapter 11 was an ideal problem solving technique, but far too complicated for extemporaneous field use in emergencies. If these conclusions be correct, the problem is one of defining essentials of the K-T method in such brevity as might be woven into a set of guidelines for emergency action.

Emergency actions are analyzed in two parts of the MORT diagrams - on page 7 as to "emergency shut off" and on page 4, "Preventing Second Accident."

The first relies on the second for analytic method, and both rely on Task Error Analysis (transfer reference to process B3, SD5), Figure 11-3.. However, the Analytic format suggests some significant aspects.

Figure 11-3. Prevent the Second Accident



The guidelines which were developed at Aerojet and supplemental comments follow:

Emergency Problem Guidelines

NOTE: There is usually some prior indication of an approaching problem. Timely follow-up on indications of changing conditions can prevent or reduce the likelihood or severity of many emergencies.

1. Alarms and Signals.
 - a. Believe alarms and signals until proven false. DO NOT ASSUME signals are false.
 - b. Remember alarm setpoint values and the logic of the setpoints.
 - c. Take extra measures to monitor while the alarm condition exists, until the alarm is proven false, or when alarms are out of service.
2. Secure equipment and take action to prevent the situation from expanding:
 - a. Deenergize electrical power or other energy sources.
 - b. Isolate system or parts of system.
 - c. Isolate affected area - establish a perimeter, mark it, and place a monitor to watch it.
3. Avoid unnecessary haste.
 - a. If there is immediate serious danger, take prompt action to reduce the danger or correct conditions, e.g., call ambulance, call Fire Department, evacuate the scene or area, carry out specific applicable Emergency Action Procedures.
 - b. Go slow or STOP.
In the circumstances confronting a performance-oriented supervisor, the emergency injunction to "go slow" or STOP seems strange. However, examination of many accidents/incidents reveals this to be a critical, judgmental aspect of the process of handling problems.
One experienced safety engineer (Kling, 1969) said: "Newton's laws of motion, especially the one about a body continuing in a straight line unless acted upon by an outside force, seem to apply to the thought processes as well as to material masses."

The very human tendencies to "push on" and "bull through" are commendable, but fraught with possibilities for escalating trouble.

Whenever possible - STOP.

In an emergency, it's not very useful to say, "don't panic." But stress (and incorrect decisions) can be alleviated by a stop-to-think interval, almost regardless of need for fast action.

- c. If there is no immediate serious danger STOP -- COLLECT INFORMATION, THINK OUT and ANALYZE -- AND THEN ACT.
 - (1) Remember that the problem is due to some change in plant, equipment, personnel or procedure.
 - (2) Correction depends on a correct diagnosis of the relevant change, its nature and location.
 - (3) Then neutralize or counteract the troublesome change, or take action to counter the change.
 - d. Above all, remember the "no hero" rule - heroes are too often dead and wrong.
 - e. A potentially confusing finding is that in marine disasters there was a apparent failure to act in time. But these particular kinds of accidents, examined more closely, suggest that failure to slow down, or to change course, or to call for help was actually involved--nothing in these is inconsistent with the general notion of slowing down or stopping whenever possible.
4. Establish a command post, usually YOU.
- a. Be sure all know the location.
 - b. Don't inadvertently allow others to take over.
 - c. Keep the command post manned.
 - d. Check out communications with all manned stations.
5. Seek and disseminate information.
- a. Use all expertise available - use call out if time permits. (Previously indoctrinate personnel as to the importance of information in decision processes - which means, for them, volunteer information which is relevant.)
 - b. When possible, verify all reports of conditions.
 - c. Log all information received, if time permits. At least collect all information in one place, even if it's in your head.
6. Notify appropriate people of problem.
- a. Branch Manager or higher management if Branch Manager is not available.
 - b. Warning Communications Center if scale requires. If not, do not hesitate to use WCC as a communication medium, e.g., to contact other plants, request assistance or expertise.
 - c. Project Engineer, if an experiment is involved.
 - d. Get help - in terms of people and equipment.
7. Apply the concept that no decision can be made and implemented unless at least one alternative has been considered.
8. Take corrective action:
- a. Clearly communicate decisions and verify that personnel understand. Require "action understood" and "action complete" reports.
 - b. Monitor indications which could show action giving expected results - also those that could show the opposite.

- c. Log all action and results in sequence.
- d. Plan and initiate further corrective action based on initial action and results.
- e. If situation expands to Emergency Action Procedure level, declare so and implement appropriate Emergency Action Procedure.
- 9. Do no re-start or resume original process until cause is found, verified and corrected.

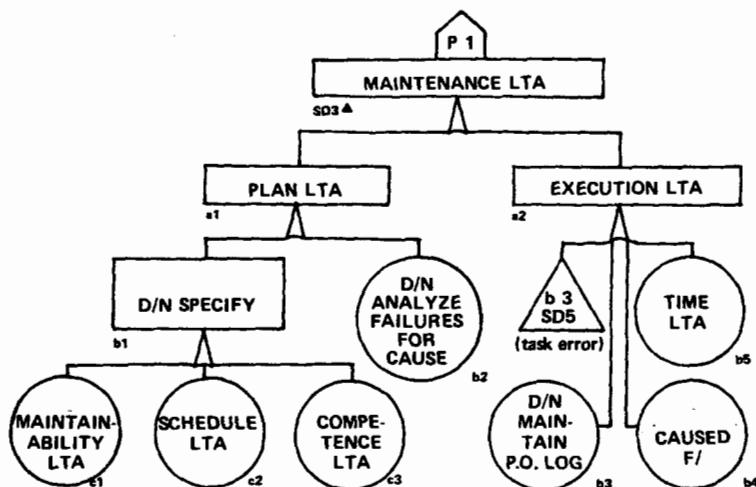
Even in the above cryptic form, the thought and command processes, while perhaps useful in training, become too lengthy to structure practice in actual emergencies. Therefore, a short version, possibly retrievable in emergencies, should probably be used:

1. Hear ALARMS and SIGNALS
2. SECURE
3. STOP when possible
4. Establish COMMAND
5. Collect INFORMATION
6. Get HELP
7. DIAGNOSE - consider ALTERNATIVES
8. ACT
9. Close out process when emergency has ended.

31. MAINTENANCE AND INSPECTION

The MORT diagrams postulate a method of examining maintenance:

Figure 31-1. Analysis of Maintenance



The same analytic process is postulated for inspection.

SD3 Maintenance LTA. The analytic diagram is largely self explanatory.

b1 D/N Specify. Requirements should emanate from the Development stage of the Hazard Analysis Process. Otherwise plans should be produced in operations as rapidly as possible. Standards may apply, for example:

"All safety and warning devices including interlocks shall be serviced and checked for proper functioning at intervals not to exceed six months." (American National Standards N43.1)

b2 D/N Analyze Failures for Cause, e.g., worn out through use, misuse, or poor maintenance.

b3 D/N Maintain P/O Log refers to needs for logs, labels, or color coding at the point of operation to show maintenance status, like the tags on fire extinguishers or color coded quarterly inspection tags on crane slings. Accident reports indicate that operators or supervisors need such warnings.

b4 Caused F/ refers to failures caused by maintenance mistakes and errors in the work. Some typical questions are:

1. Describe the maintenance procedures and standards established for the equipment involved.

- a. Were maintenance responsibilities allocated?
- b. Was actual maintenance in accordance with standards?
- c. Was the unsafe condition (if any) covered by maintenance procedures?
- d. When did the equipment last have periodic maintenance or repair?
When was it next scheduled?

2. Were lock-out or tag-out procedures applicable? Were work permits required?

3. Are work orders reviewed for:

- a. Maintenance employee safety?
- b. Other employee safety?
- c. Subsequent safety in use?

If so, describe findings and actions.

SD4 Inspections. Inspections are a routine method of hazard detection, a basic monitoring process, and the type and nature of prescribed inspections constitutes a major facet of a safety program. Essentially an inspection system is a method of detecting (1) oversights, and (2) changes occurring over time.

The common inspection systems can be categorized as follows:

1. Operational, by employee, at start up, during, and at change or shut down.
2. Supervisory, same characteristics.
3. Special - frequency and competence of personnel are usually specified for pressure vessels, elevators, cranes, fire, industrial hygiene, etc.
4. Periodic
 - a. by supervisor - internal to department,
 - b. by safety department, committee, etc., - external to department.

To these should probably be added:

1. New, changed or restarted equipment.
2. Sampling techniques to audit the inspection systems.
3. Detailed, in-depth thorough inspections - less frequent than (4) above, but more searching, and comprehensive. Accident reports suggest that routine inspections too often become superficial.

Checklists are generally considered desirable, but there are important qualifications:

1. The checklist should be specific for the department or operation.
2. Checklists should be, at least in part, "topical" to suggest exploration of content and such topics as maintenance procedures, frequency of process review, etc., as well.
3. Checklists should be made clear (by any needed explanations) and equated to competence of inspectors.

The checklist is, then, a written retention of the wisdom of past experience, and will be no better than that wisdom. It is a reminder. It must also ask, "What Else?"

Perhaps the biggest weakness in inspections is to see them solely as methods for detecting (and correcting) hazards. These they most certainly are. But always the "cause behind the cause" is the vital thing. Why did

the change or unsafe condition come into being? What should be done about the "why?" A common weakness is failure to analyze inspection reports for causes of defects, that is, corrective action stops with item fixes rather than system fixes. Thus we have a number of criteria useful in measuring the inspection aspect of a safety program. The Environmental Chamber Case in Appendix A shows problems of both maintenance and inspection.

Two generalizations seem supportable:

1. Any piece of equipment or process should, upon acquisition, have an established period and method of inspection (and maintenance).
2. The schedule should be shown and monitored in two ways:
 - a. By a record on the equipment or at the process, e.g., color tags on slings.
 - b. On a master schedule.

Some useful questions are:

1. Describe the inspection plans (other than by supervision) applicable to this area.
2. When was the area last inspected? By whom? Attach report.
3. Was the equipment, etc., involved in this accident inspected? What was found?
4. If there was an unsafe condition in the accident, did it apparently exist at the time of the inspection. Why did the inspection miss the change or condition?
5. When was the next inspection scheduled?
6. Was an inspection docket maintained on the equipment? In the work area? Very recently, an analytic tree for thorough examination of the inspection function was developed by Dr. R. J. Nertney of Aerojet (see Exhibit 12).

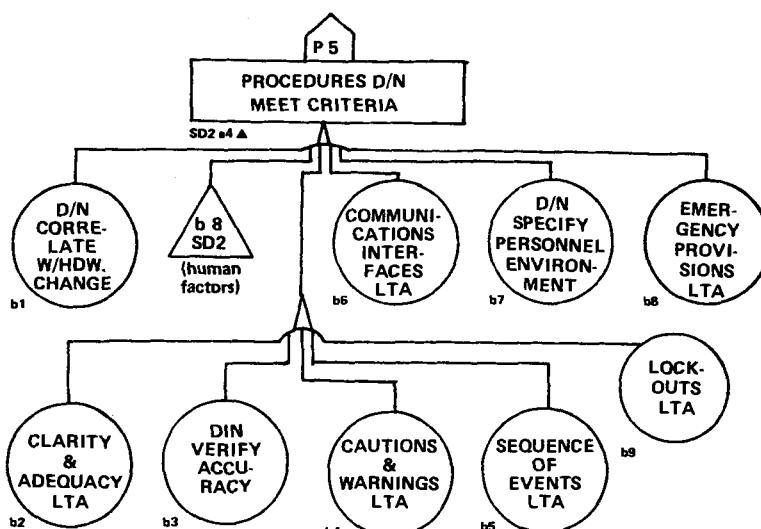
This page intentionally blank

32. PROCEDURES

Procedures criteria are shown in the MORT diagrams (Figure 32-1) as an aspect of the Hazard Analysis Process. Procedures recur in the diagrams as an aspect of performance - what were the procedures in repetitive and non-repetitive tasks (Figure 32-2) and were procedures followed (MORT, page 8)?

The logical format of procedures analysis in MORT seems clear in the two diagrams - the first (Figure 32-1) applies the concepts of procedures criteria, and the second (Figure 32-2) provides an action logic whereby (1) work assignment and special safety review are questioned, (2) the handling of repetitive and non-repetitive tasks is examined, (3) the role of employee suggestions, in addition to procedures criteria, is exposed for investigation and study.

Figure 32-1. Procedures Criteria

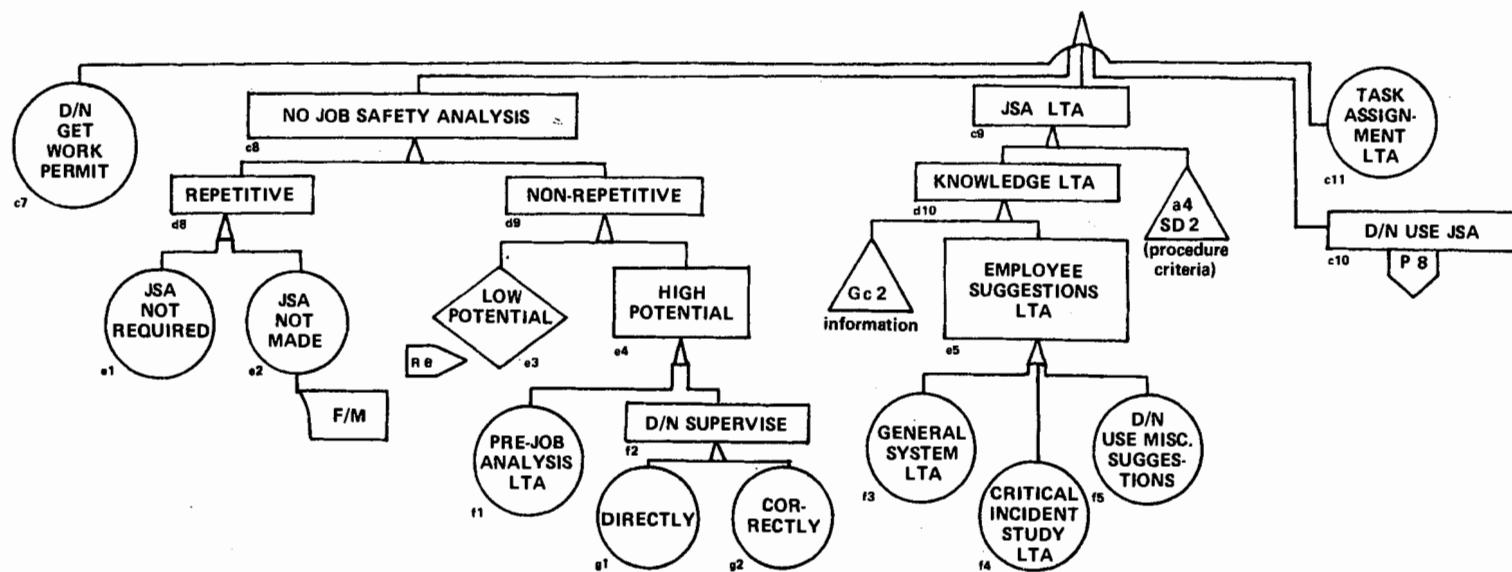


Procedures can well be scrutinized as to their sources - those which emanate from a management process (reviewed at the work level) and those which originate at the work level, such as Job Safety Analysis (reviewed by safety and management). This distinction is important in accident analysis to see where and why procedures may have failed, but poses no problems in concept. That is, a procedure from either source may be adequate to the need, or may be deficient.

The work control process as visualized assigns procedures or Job Safety Analysis a critical role. In many mass production business organizations we have seen a policy requiring written procedures for every task. But non-repetitive work, such as research or construction, finds universal coverage more difficult.

Standardized, repetitive tasks can be covered by written procedures.

Figure 32-2. Action Aspects of Procedures



So we can inquire into the frequency of repetition and the magnitude of energy.

Theoretically, non-repetitive tasks involving significant energy levels should be personally supervised as to procedure.

Procedures are the fifth step in the Safety Precedence Sequence--after design, safety devices, warning devices, and human factors. Procedures are a part of the iterative nature of the whole process in two ways:

1. Their preparation may provide feedback and recycling to design, devices, or HFE in SPS.
2. Their preparation involves the same conceptual, design-development, test, and operational phases. If writing a good procedure is difficult, the whole concept of the task may be wrong, and the project may recycle through HAP.

Procedures may vary from highly formalized and reviewed Safe Operating Procedures to Pre-Job Analysis. A Phase II statement of U. S. practice will be helpful:

The leading U. S. corporations develop a high degree of control over work practices by a three faceted program:

1. Every job should be subjected to safety analysis.
2. Every employee should receive instruction in performing each task in accordance with the written analysis.
3. The supervisor should not only see the man do the task safely, but have a planned observation program to continuously monitor performance.

For convenience we refer to this as JSA-JIT-SO, that is, Job Safety Analysis, Job Instruction Training, Safety Observation.

Despite the manifold tasks to be studied and controlled, some of the companies have, over time, attained a remarkably high degree of coverage and control.

Thus, General Motors is able to direct:

"Develop safety instructions for every job. Put these instructions in writing for every job in the plant. The supervisor should review the safety measures for each job before the employee starts to work and then follow up to make sure he understands."

U. S. Steel said:

"List all the occupations in the department, and the jobs performed by employees on those occupations. Then single out the jobs which represent the greatest injury potentials. These are to be analyzed first."

Importantly, U. S. Steel says that JSA-JIT-SO (with other features of their program) are applicable to all the diverse operations of the company. It is not a program for just high hazard operations or big operations.

The advantages of the JSA-JIT-SO plan are numerous, but certainly include:

1. The potential to get started, and build as you go.
2. The potential to measure performance in three ways:
 - a. By accidents - was the job covered by JSA? Or, where did the system fail?
 - b. By inspections - if an unsafe practice is observed, was it covered by JSA? Or where did the system fail?
 - c. By supervisory reports indicating degree of coverage with JSA.

It is axiomatic that complex systems such as organizations are operating in ways somewhat different than the directives, manuals, plans and procedures which were presumed to govern their operation. Some of these deviations may be very good, and may be compensation for limited or poor or impractical procedures.

There are two dangers in the "operating procedure" approach:

1. Accident causes may be seen primarily as deviations from the procedures, but correction may lie elsewhere!
2. The procedure may be seen as the "one best way" without much examination of alternatives!

Despite the emphasis on procedures in U. S. safety practice, and the tremendous number being written, few criteria are seemingly used to guide the preparation process. The criteria needed are of two types:

1. Management process of preparation.
2. Review of the procedures themselves.

These kinds of criteria make it abundantly clear why procedures cannot be informal, oral and unreviewed in other than the lowest energy situations. If there are poor criteria - procedures can be fatal!

Criteria for the Procedure Development Process. A good example of some parts of the procedure process is in Sandia's guidelines for underground tests. The context of the operation is well established, topics to be included are defined, and a format (including step-by-step) is established. Sandia also has a general format for procedures. However, these are hardly definitive as to methods of preparation.

Typical methods doctrine includes: "The four basic steps in making a job safety analysis are:

1. Select the job to be analyzed.
2. Break the job down into successive steps.
3. Identify the hazards and potential accidents.
4. Develop ways to eliminate the hazards and prevent the potential accidents." (NSC Manual or Supervisor Safety Manual.)

The U. S. Steel analysis form for identifying the hazards in each step or operation uses a three-part classification of hazards - Caught-Between, Strike-Against, and Struck-By - to prompt enumeration of all possibilities for injurious contact. The energy release concept could also be explored for analytic potential.

The Job Safety Analysis and the Safe Job Procedures are developed by the foreman working with a small group of his most skilled craftsmen, and their work is reviewed by a management committee.

Obviously JSA may reveal needs for guarding, displays, or signals, better equipment, or physical arrangements. And it is understood that, where applicable, physical revisions are preferred solutions. Or, the human task may be eliminated by assigning it to the machine - improved controls or equipment.

The iterative nature of procedure development was suggested, and an opportunity to exercise MORT analysis, was provided by the following incident:

NSC's Research Department was doing a study of occupational safety of urban police. High speed pursuit driving is a controversial source of serious accidents. When the MORT discussions moved to Job Safety Analysis requirements for repetitive tasks, especially those with high potential, a not uncommon confusion was evident: (1) Was the task repetitive? (2) Should any training be given? Or, (3) should high speed pursuit be discontinued?

After some discussion, it became clear that rational analysis would be

aided by following the sequential steps in analysis. These in order would be:

1. Conception and requirements: What criteria are to be used in the decision to pursue or not pursue? (E.g., seriousness of the apparent crime.) What alternatives are available? What are I/B/V/T criteria?
2. Equipment: What design, maintenance and inspection requirements should be established for equipment suitable for high speed pursuit?
3. Job Safety Analysis: What hazards and countermeasures can be described from data or police experience? What is the step-by-step procedure?
4. Training: What training (or prior selection), and what practice are needed to minimize hazards of pursuit?
5. Supervision and Review: What data should be accumulated as the basis for management of this activity, and possible subsequent modification of policy or practice?

This type of sequential analysis seems well calculated to maximize safety within operational requirements, and minimize confusion and controversy.

A key issue which might then be framed in the light of the above kinds of analysis might be:

Are the criteria to be used in high speed pursuit decisions the same, or different for: (a) A young officer with specialized training and well-maintained equipment? (b) An older officer without specialized training and with poorly maintained equipment?

Procedure preparation is inherently the same as the Hazard Analysis Process itself. In particular, the knowledge input must be clear. Known precedents (including previous mistakes in using similar procedures) are one basis for present procedures. Therefore, a procedure can be examined for adequacy of the knowledge input process.

There will often be expertise not available to the group doing a JSA, for example, the biomechanics of lifting. Consequently, a JSA effort should be supported by providing pertinent general literature.

The final step in HAP is independent review and this is also a criterion for the procedure process itself. (See Figure 28-3, Aerojet's Review System.)

Three questions could profitably be examined:

1. Should the documentation, especially for high energy procedures, be extended to provide management with clear cut statements of failure-modes, consequences, trade-offs represented by the procedures, and summaries of alternative countermeasures for higher protection which are not recommended on practical grounds?
2. What is the threshold at which procedures are required? Should the threshold be progressively lowered to cover a larger percentage of the work?
3. If the threshold is to be lowered, what practical short-cuts are available to develop procedures for lower energy operations?

The discussion of scaling mechanisms touched in passing on a scaling of procedures effort to fit magnitude of problem. Examination of procedures requirements and practice at two research sites suggested need for a more flexible hierarchy of procedures, coupled with an easier, more nearly self-generating method of working up from the operating level to fill in gaps left in, or at the end of, highly formal Safe Operating Procedures. Job Safety Analysis (as used in many industries) and also Pre-Job Analysis (step-by-step, but

extemporaneous, oral, unreviewed) would seem to complete a spectrum of needed, but flexible controls. In a different, lateral aspect, Safe Work Permits (welding, radiation control, etc.) seem to cover more acute aspects of a specific task at a particular time and place, but not an adequate substitute for JSA.

Difficult aspects of work control are the routine maintenance and craft jobs. These are said by the skilled craftsmen to be covered by the manuals of the trade. On the other hand, accidents in this work are numerous, so the coverage is patently inadequate. It would seem that a useful concept could be:

1. Manuals, etc., may be sufficient if they include step-by-step procedures and are in writing, available, and used. In other words, references can be specific, and not "custom."
2. Job Safety Analysis is needed for other repetitive tasks with more than low potential.
3. Pre-Job Analysis is needed (and is step-by-step) for every task, even those covered by 1. or 2., and is needed for the frequent breaks and modifications in routine which occur so frequently in maintenance and repair.

Pre-job briefing may also constitute the "operational readiness" review whereby the net effects of all changes, maintenance, etc., since the last operation are analyzed for completeness, new hazards, etc.

Thus, the needed, flexible hierarchy may be:

- | | |
|--|--|
| 1. <u>Standard Operating Procedures</u> - major documentation, and one or two independent reviews. | Special Situations covered by <u>Safe Work Permits</u> |
| 2. <u>Manuals</u> - with step-by-step procedures, and reviewed. | |
| 3. <u>Job Safety Analysis</u> (producing "safe job" procedures) originating at work level, and with or without review. | |
| 4. <u>Pre-Job Analysis</u> - at the work level, step-by-step. | |

In all of these, the logic of HAP-SPS-LC is unvaried, just the amount of study and review is varied. Given these or similar definitions, accident data can be collected as to coverage in the above ways, or "out of bounds."

Sandia has computerized its extensive system of 250 or more Safe Operating Procedures for ease of up-date control and review, subject matter retrieval, and cross-referencing.

Criteria for Review of Procedures. The literature search, field work, and accident analyses have accumulated criteria which should be valuable in preparing or reviewing procedures for oversight.

The best document to date is from NASA. Dr. Preston T. Farish's, "System Safety Criteria for use in Preparation or Review of Procedures." Its main body was used in MORT Trials at Aerojet. Farish's introduction says:

"Poorly written or unclear procedures are one of the major causes of accidents and incidents in space vehicle operation. Investigations of numerous incidents show that just such procedures were being used. In other cases, procedures did not exist at all.

"Inadequate procedures represent as great a threat to space vehicle safety as do faulty hardware and careless work. A well-prepared procedure leaves no doubt in the mind of the person following it. Nothing is left to imagination or guess. Values and units are spelled out, and

no step is omitted because it is 'obvious.' Instructions are clear and concise and the use of special test equipment is specified when required. A proper procedure is one that has been authenticated by a responsible individual and checked out against the hardware for which it is intended."

The MORT diagram (Figure 32-1) generally follows Farish's categories. However, he adds a set of general requirements, as does the list in Appendix F.

In three serious accidents, a total of 71, an average of 24, of Farish's criteria were applicable to the procedural deficiencies, and might have drawn attention to those defects and prevented or ameliorated consequences, if criteria were used in advance. Farish's criteria are properly redundant - that is, several criteria might have brought out a given causal factor.

Another useful set of criteria was prepared by Dr. R. J. Nertney (1967). Dr. Nertney's studies employing the "critical incident" technique have supported a conclusion that procedures developed from the top down as a system evolves will be lacking in coverage of human misinterpretation and misunderstanding, and may be somewhat divorced from job realities, unless a special effort is made to get employee feedback. Engineers find it difficult to understand why the procedures they write are sometimes misunderstood on the job, and engineers may have similar blind spots in reviewing - therefore, the criterion of on-job checking is important.

In the MORT Trials at Aerojet, Farish's criteria were reworked by a Procedures Review Board. The PRB list, with additional modifications, is provided as Appendix F.

Job Safety Analysis. The results of a job safety analysis can be evaluated against the above criteria. In the MORT Trials at Aerojet, the U. S. Steel manual chapter on the subject was reproduced and used. The function was also summarized in outline form as follows:

Goal: (1) Determine potential accident causes.
(2) Eliminate potential accident causes.

I. Determine jobs to be analyzed.

II. Establish priority in which jobs are to be analyzed.

- A. Frequency (of associated accidents)
- B. Severity (Accident potential)
- C. Supervisory judgment
- D. Regularity (High Exposure Rate)
- E. Job Changes (Hazards not clear)

Five steps to
decide proper
priority

III. Method

- A. Group discussion method
- B. Direct observation method

IV. Break down individual job into steps or elements

V. Determine the contact possibilities (environment)

- A. Can the workman be struck by anything while doing the job step?
NOTE: At this point - unless time prohibits - do not consider ways of preventing contact - only identify the contact possibilities.
- B. Can the workman strike against anything doing the job step? (It is important, not only to identify what the workman can strike against, but also how the contact could come about.)
- C. Can the workman be caught between any objects doing the job step? (e.g., look for "pinch" points.)
- D. Can the workman be caught on or in anything doing the job step? (e.g., clothing in machinery).
- E. Can the workman fall doing the job step?
- F. Miscellaneous accident possibilities.

VI. Eliminate or reduce contact possibilities.

- A. Establish a safe work procedure that will eliminate or reduce the potential contacts.
- B. Change the condition of the environment which contributes to the possibility of a contact (tools, equipment, machines, etc.).
- C. Wearing personal protective apparel.

VII. Develop safe procedure

VIII. Safe job procedure appraisal

- A. On-the-job review _____ Employee
- B. Conference review _____ Participation
- C. Management review

The present Aerojet approach to procedures has several supplementary elements, as follows:

1. The Detailed Operating Procedure is reviewed by a Board and meets criteria.
 - a. The DOP has been subjected to JSA, or at least reviewed with the work force.
 - b. JSA's are created for standard tasks (e.g., crane operations) and are plugged into DOP's.
 - c. Engineering review of radiological or toxic hazards is performed, limits are quantified, and corrective actions are specified in advance.
 - d. A "Safe Work Permit" is issued by safety personnel to cover field conditions and requirements.
2. Standard Aerojet policies and procedures provide a frame of reference and context. Thus, an integrated, comprehensive procedural system is created.

Collecting Accident Data on Procedures. Catlin (1969) provides an example of the key role of procedures in analyzing planning and operational failures.

Several sets of qualities can be visualized to describe procedures:

1. Source

- a. Higher level - from manuals, or from experts in complex processes.
- b. Supervision
 - (1) Instructions
 - (2) Personal supervision
 - (3) Employee Participation (both to pick up on-the-job experience and for motivational reasons).

2. Form

- a. Written
- b. Oral

3. Hazard Review

- a. Visible - thorough
- b. Visible - slight
- c. Not visible.

4. Feasibility (in terms of task frequency)

- a. Task repetitive (quantify as "daily, weekly, monthly, annually")
- b. Non-repetitive.

5. Need - energy level.

Thus, in an accident where a supervisor told an employee, "Hey Joe, close that valve." The employee closed the wrong valve, resulting in serious injury when a flange was opened, and shutting down a major process. We can classify the procedure as follows:

1. Source - Supervision - personal
2. Form - Oral
3. Hazard Review - not visible
4. Feasibility - task approximately monthly
5. Need - high energy.

An objective description of a "planning error (management)" is emerging. Results from numbers of accidents when so tabulated should give a useful assessment of the status of procedures and the major needs for the future.

Data on procedures may also be compiled using Rigby's "error tolerance limits" cited on page 52. "Custom and debate" are all too common and lead to sloppy, unsafe performance.

At Aerojet the use of Detailed Operating Procedures and Job Safety Analysis are being worked into a complementary and structural system suitable for clear and efficient guidance and good management. The similarities, as well as some few differences, are shown in Figure 32-3.

Figure 32-3. Similarities & Distinctions - Procedures & Job Safety Analysis

	<u>Procedures</u>	<u>JSA</u>
1. Originate at:	Higher levels	Working levels
2. Strengths:	High potentials, Technical difficulty, Control requirements, Inter-unit scope	Use of craft knowledge and experience
3. Criteria input:	Detailed, Searching	Simpler
4. Information input, acc/inc. reports	Formal search	Inquiry to safety
5. Draft	Show failure-modes, consequences, corrections for each step	Same scope, less formal
6. Specify "plug-ins":	1 Use JSA's ← 2 Back up data - e.g., engineering calculations 3 On-site work permit requirements	Standard tasks (e.g., crane operation) Components (e.g., lifting)
7. Reviews: Informal		Get work site experience
Formal	Board	Line & staff
8. Pre-job training	If needed	JIT routine
9. Pre-job briefing		both
10. Field change procedure	Formal	Supervisor
11. Monitoring		both
12. Post-use critique		both
13. Revisions	Formal procedure	Less formal, but in writing
14. Accident Analysis		
	a. Classify error by Rigby's tolerance limits (page 52). b. Describe deviations (plural) in terms of steps 1-13. c. If error was in selection or use of procedures or JSA, classify as follows: (1) Requirements LTA (a) Scaling Mechanism LTA (b) Other definitions of use LTA (2) Error by management or supervision. (3) Performance error.	

33. EMPLOYEE SELECTION AND TRAINING

The MORT logic for employee selection and training (Figure 34-1, a portion of Page 8 of the MORT diagrams) is a part of a general logic of successive elimination of perceptible accident factors in investigations or safety program reviews. In this context, the MORT logic presumes a competent Hazard Analysis Process, and excellent (or at least adequate) Supervision and Procedures. Employee selection and training, helpful as they are, are not postulated as effective ways of countering defects in the prior processes.

Training capacity to reflect accumulated wisdom and recent experience is, on the other hand, very often a "one best answer" to problems, and the MORT logic is not intended to in any way deprecate the values in training.

The MORT logic presents an objective test of selection and training - D/N See or Saw Correct Performance.

The idea of personnel as output of a system of selection, training, procedures and supervision is the basis for an "upstream audit" of processes, as can be inferred from the general safety system, and its monitoring subsystem.

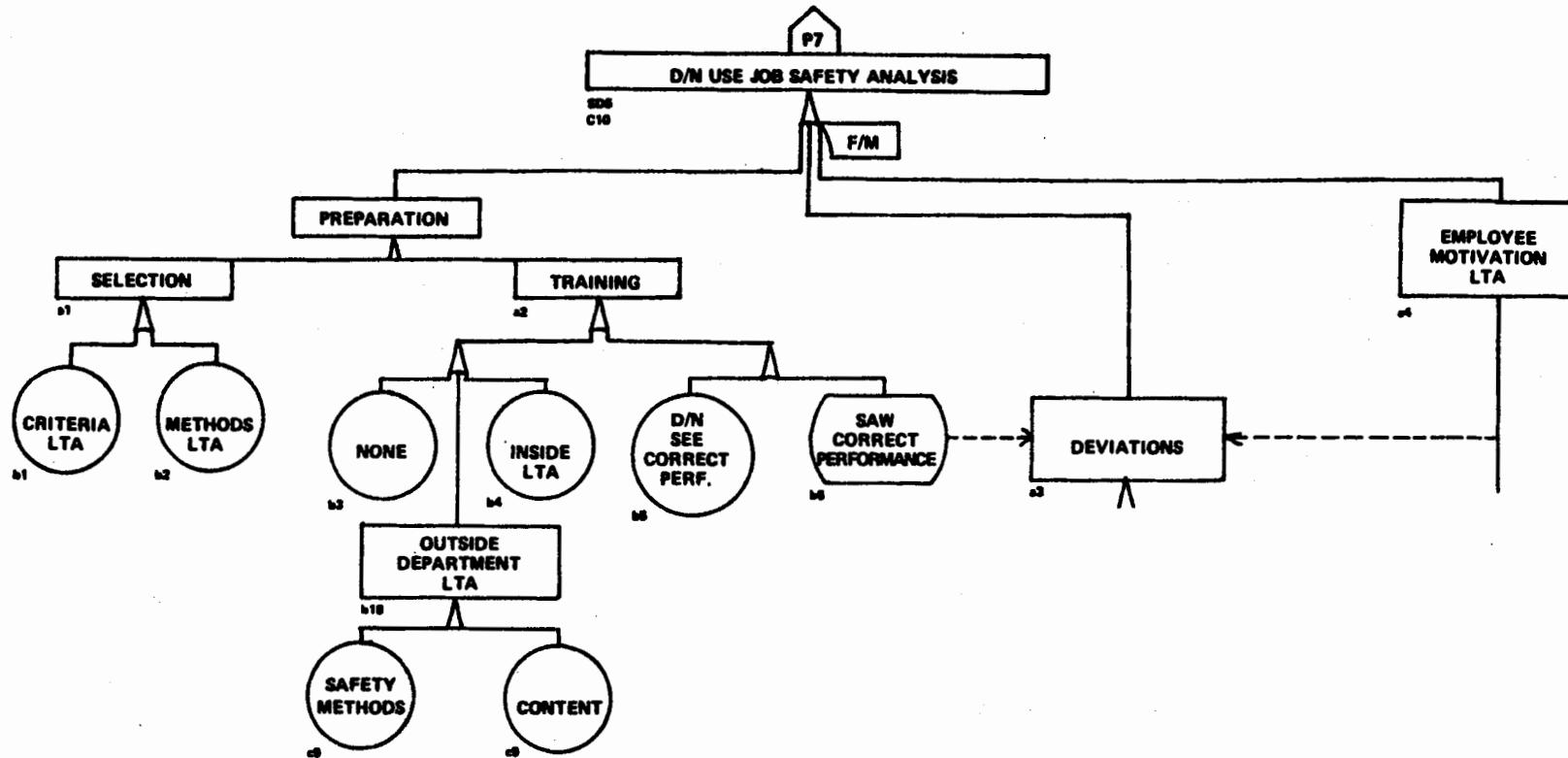
The first "walk-through" of the Aerojet personnel subsystem showed gaps which could be related to actual incidents. For example, an experienced crane operator said of training, "Who'll train me?" He later had a crane episode which suggested that the criteria for selection and training of reactor grade crane operators were "LTA." Upon examination the criteria were found to be, in fact, "much less than adequate," or "Poor."

The upstream audit process produced an outline of personnel subsystem requirements, as follows:

- | | |
|--------------------------|------------------------------|
| I. Selection | 2. New Reactor modifications |
| A. Criteria | 3. New Reactor experiments |
| B. Testing | 4. Special craft |
| II. Training | III. Test & Qualification |
| A. Basic | A. Basic |
| 1. Doctrine | 1. Initial |
| a. Initial | 2. Continuous |
| b. Continuous | 3. Periodic |
| c. Periodic | B. Special |
| 2. Conduct | 1. Craft qualification |
| a. Initial | 2. New programs |
| b. Continuous | 3. Physical exam |
| c. Periodic | IV. Current Status |
| B. Special | A. Medical |
| 1. Plant familiarization | B. Supervisor Observations |

The Test and Qualification for reactor personnel is one of the "gates" in the Aerojet Review System (Figure 28-3). The "current status" is assessed by supervisory, medical, or other observation.

Figure 34-1. Employee Selection and Training



Selection. In selection (SD5-al in the MORT diagram) the twin factors of criteria and methods are exposed for study.

There is a limited amount of information on safety-related physical capacities for specific kinds of risks; substantially more for the driving task than other tasks. Where performance can be critical, as for crane operators, and objective requirements can be established, selection of personnel can play a role in the human factors chain. Selection is widely practiced in motor vehicle fleet safety, but biographical data seem to have greater reliability than results of various types of psychological tests. In general, tests have not effectively discriminated those who will have accidents from those who will not.

Crawford (1965) recommends:

"The hiring procedure should be designed to-fit-the-man-to-the-job. Job requirements should be analyzed to identify job demands so an individual with desired characteristics be selected.

"Moreover, a review should be made of an individual's personal work history, which contains some of the best predictors of accidents: a previous record of accidents. If an individual has had several accidents, he may have other accidents. Accident predictors include: excessive or chronic absences, frequent gripes or complaints, low productivity, inefficient work performance."

Crawford's suggestion should not reverse earlier emphasis on first doing all possible to fit the jobs to the people typically available.

In any investigation, some questions on selection of personnel should be answered, for example:

Describe applicable personnel standards, and review procedures established (e.g., medical exam).

Did personnel meet the standards established for the work? When examined? When reexamined?

Training. MORT analysis presumes that training is auditable in terms of the steps on page 325 and for each of the relevant categories of personnel.

The MORT analysis uses the widely-accepted, simple yardstick of Job Instruction Training (JIT) to evaluate training:

1. Prepare the worker to receive the instruction.
2. Present the operation - perform and describe.
3. Try out his performance.
4. Follow-up.

(Added details are in the NSC manual and other publications. Interestingly, Juran (1964) cites JIT as a "management universal.")

Again we see not only the elements in upgrading a supervisor's ability to train, but also the anatomy which enables us to measure and to trace a breakdown in the system.

Smith (1967) provides criteria for judging the strengths and weaknesses in a six-phase training program developed by an NSC training committee. The phases are:

1. Identifying Training Needs
2. Formulating Training Objectives
3. Gathering Materials and Developing Course Outlines
4. Selecting Training Methods and Techniques
5. Conducting Training Programs
6. Evaluating Training Programs

Altman (1970) analyzes three key factors:

1. Monitoring and feedback
2. The role of reinforcement schedules in learning to have accidents
3. Transfer of training and safe behavior.

Reinforcement mechanisms inherent in the role of the person differ widely for four classes of roles:

1. The critical worker whose performance is always rewarded,
2. The series worker who receives feedback only on total performance of the series,
3. The parallel worker who may receive positive feedback even though he has erred,
4. The redundant worker whose feedback is unrelated to his performance (and so he performs poorly!)

Learning curves are favorable-unfavorable in terms of the 1-2-3-4 sequence above.

Transfer of training may be positive or negative depending on the similarity of stimuli and responses. No assumption of transfer could be relied upon without examination of the elements of two tasks and a decision whether positive or negative correlation with error is likely. Among techniques Altman urges is:

"Being assured that change does not fallaciously depend upon proficiencies which will not readily transfer or permit negative transfer to occur in critical operational situations."

Reinforcement of safe behavior based on Skinner's findings is discussed by Bird and Schlesinger (1970). The discussion ranges across three areas in this text:

1. Training - values in reinforcement,
2. Enforcement - some negative side effects,
3. Role of rewards - which extends into our topic of motivation.

Operations simulation is highly effective as a training device, and also contributes to a hazard analysis. Initially, realistic simulation seems expensive, but should be examined against the costs of emergency actions (good and bad). Evaluated in long-term results, simulation will

often show up as a low-cost approach. Simulation is easily scaled from class-room, intellectual problems through manual exercises to electronic and mechanical exercises which approach operational conditions. Given this range of simulation, a test question in an investigation could be: Did training include any simulation related to the event which occurred?

Programmed self-instruction is being increasingly used. Low cost and demonstrated learning potentials commend it. DuPont, as an example, has programmed instruction in general subjects, such as "Safety Principles" and "Planning for Safety," as prerequisites for a wide variety of specific hazard training topics.

Surry (1969) cites studies showing effectiveness of initial training in shortening a new employee's early period of accident susceptibility, but little or no long-term effect of initial training.

Retraining and Requalification? Accident reports often show a recommendation for retraining or requalification testing - but such reports seem to reflect a blind reliance on training or qualification, rather than a reasoned finding that such programs would in fact have prevented or alleviated the event. If the roots of the accident are in non-acceptance or weak motivation, training and tests may not correct the deficiencies. One explosives accident involved the person who gave explosive safety instruction - and he deviated from preachments and procedures in twelve ways! (Appendix A6.) Training is hardly an answer, nor is participation in safety programming. Adequate monitoring and supervisory follow-up seem closer to the mark.

On the other hand, if new materials or processes are involved, retraining and requalification may well be useful measures.

The adoption of system safety methods can be seen as a training challenge. The need for safety training for new employees is well recognized. For example, AEC's "Electrical Safety Guides for Research" says:

"A course in electrical safety should be provided for new laboratory employees, commensurate in coverage with each employee's work assignment."

Just what does this mean? A course in electrical safety, but not pressure vessels, lifting, fire, etc? Commensurate "with each employee's work assignment" - how is this to be done in a course regularly available?

Lawrence has a safety training course for new employees, but as with most such courses, the question can be asked as to whether it reaches new employees when they are really new and need it most, or whether it reaches them later, when a class is full, and need is lessened. Effectiveness is

not assessed.

A different kind of problem at Lawrence, namely, general non-attendance of graduate students, suggests some other questions about such training. Is it to be forced on these people, and with what results? Or, is the challenge to make the course so interesting and valuable that graduate students praise the course?

Perhaps the whole challenge to systematic safety can be expressed in the challenge to create a training experience which grad students see as an opportunity to learn about creative problem solving to attain an objective.

The challenge lies, then, in the contrast of Method and Content. Can employees of whatever type be taught how to analyze jobs and hazards, or must they be given lengthy "laundry lists" of hazards?

34. PERFORMANCE ERRORS

MORT logic for examining performance errors rests on prior processes of hazard analysis, management or supervisory detection of error provocative situations, and procedures. Also, the role of employee selection and training (for example, a supervisor's use of a JSA-JIT-SO routine) are considered to be a part of management and supervision. Thus, performance errors become a residual of systemic strengths or weaknesses.

Notwithstanding the major importance assigned to prior factors in the work situation, one trainer saw the end result of MORT as "blaming the operator for performance errors." The satisfactory answer seemed to lie in re-emphasizing that a typical MORT analysis shows 30 causal factors before considering employee performance errors.

The first task in analyzing performance errors is descriptive, that is, the errors could be tabulated as "unsafe acts," using the ANSI recommended method. However, this has been shown to be so highly subjective as to be of only marginal value, and a tabulation of errors in terms of Rigby's tolerance limits is likely to have more value in designing corrective measures. (See Chapter 4 on Errors.)

The kinds of questions raised by MORT analysis are not the types commonly asked on accident reports, not answered by mass data, and quite different from the usual "unsafe act" taxonomies. The clear implication is that there could be few "unsafe acts" in the sense of blameful employee failures unless or until the preventive steps (in priority order from front to back and left to right on the MORT charts) have been shown to be adequate.

In serious accidents analyzed with MORT, the numbers of systemic and procedural deficiencies were so great as to warrant an impression that "unsafe acts" (not correctable by HFE and good planning, supervision, training, etc.) are considerably fewer than implied by the safety literature. Further, if there be a responsibility connotation to "unsafe acts," the number of such acts is probably quite small - motivational programs and forces, positive and negative, being what they are.

The MORT analysis separates task and non-task errors, and analysis proceeds more easily if the latter are set aside for separate consideration. Fringe activities, such as going to lunch, recreational programs, etc., as well as horseplay, are separated from Task Performance whose control is a prime objective of the supervisory process and Job Safety Analysis.

Before moving into the analysis of Task Performance Errors, two other preliminary questions must be cleared away:

c7 D/N Get Work Permit. There are special situations commonly covered by work permits (sometimes as extensions of procedures otherwise prescribed). These include such subjects as:

1. Welding permits
2. Continuous test permits
3. Work orders
4. Other, or general permits (such as Aerojet's Safe Work Permit system).

The general Safe Work Permit system (including, at Aerojet, radiation limits and monitoring requirements) seems to have advantages over several separate systems.

A problem in any system is that the permit may give a false sense of security. For example, a permit for welding may have only been checked for fire, or a permit covering radiation may not have been checked for other hazards. Both the form design and signer's training should consider these forms of oversight.

In one accident a permit for hot work, which meant only that a tank space was free of explosive vapors, was construed as a general approval. The worker entered the space and was killed by an oxygen deficient atmosphere. Permit format should actively work against this type of error.

Continuous Test Permits. These appear desirable, but in practice they appear to be issued for such long periods as to make questionable their adequacy for conditions at the time of the accident.

Work Orders. These should be reviewed from three safety viewpoints:

1. Employees doing the work,
2. Employees exposed during work,
3. Persons using the facility after change.

Both the area supervisor and the maintenance supervisor should consider all three views. Accident reports suggest that dual approvals on all three points should be required. But, examination of field procedures in issuing work permits suggest that job 1. is done well, job 2. is done in part, and job 3. is seldom done, or partially done, e.g., for code violations.

c11 Task Assignment LTA. Was the task assignment one the supervisor should make? Was the task one an employee should assume within an approved project?

In a revised MORT format, these two aspects may be subjects that should be questioned earlier (e.g., c11 before c7, and both clearly review topics before application of the JSA-JIT-SO routine).

The subsequent MORT analysis (Pages 7 and 8 of the diagrams) stems directly

1. In the JSA-JIT-SO sequence. Therefore, the initial questions are directed to the existence of a Procedure or Job Safety Analysis which meets any given set of criteria.

c8 No Job Safety Analysis. This analysis proceeds from a determination of the repetitive character of the task. Objective information is needed, e.g., is this task done continuously, hourly, daily, weekly, monthly, etc?

d8 Repetitive. Either JSA was not required, or was not made. In the latter case there could be Failure to Monitor the coverage of the JSA program.

d9 Non-Repetitive requires a determination of low potential or high potential (a scaling mechanism).

e3 Low Potential becomes an Assumed Risk.

e4 High Potential. (Perhaps better described as "other than low potential). A Pre-Job Analysis (an extemporaneous, but step-by-step review comparable with JSA) should be made by the supervisor or employee. (The "positive tree" based on the Gold Powder explosion is an example of Pre-Job Analysis by a professional employee.) If the task is truly high potential, the supervisor should supervise directly and correctly. (Cases illustrate both needs.)

Perhaps one of the trickiest aspects of MORT Analysis is in the task performance area--that is, a high standard for JSA is postulated. What if the JSA criteria are not met? Does analysis terminate with no JSA or JSA-LTA? The answer is, "No!"

The analysis is continued with the analysis using whatever criteria are available--custom, or debatable, to use Rigby's terms.

Thus the distinctions in c8 No Job Safety Analysis may be to first see whether procedure criteria were met, and second, if not met, how well did subsequent definitions, even if oral, meet criteria.

For example, were such oral criteria fitting:

c9 that is, less than adequate; or were they more nearly c10?
c10 D/N use.

Without deprecating the values in holding procedures and JSA to high standards, the analysis of a particular event seems to proceed best by
(1) analyzing procedures against the highest criteria, and
(2) if procedures fail to meet these high criteria, continuing the analysis in terms of criteria then in effect.

For example, if criteria to be used by a supervisor were "forensic," i.e., debatable, analyze use of such criteria as were available to the man, but allow for the fact that criteria had not been well defined by management.

Going through the MORT process of elimination for roles of procedures

(or JSA), roles of selection and training, and the roles actually played by deviations from procedures, brings us finally to the roles played by normal variability.

a3 Deviations. In practice, Deviations have been analyzed even if the standards for job performance were vague--such limits as "custom" or "forensic" (per Rigby).

The chart shows contributions to Deviations from both Normal Variability and Changes. At present the proportionate contribution of the two factors is not known. Normal Variability is visualized as manageable in degree through Human Factors Review (and appropriate designs and plans) whereas Change is more the purview of Supervision (detection and counterchange) -- such characteristics as ill, fatigued, personal problems, or temporary handicaps.

Sources of changes and data collection are discussed in Appendix D.

b9 D/N Observe. There are a wide variety of corporate plans for safety observations. By definition, we are talking about safety observations by the first line supervisor (not inspections, audits, or sampling by observers). The plans can be seen in the following elements:

1. The common sense, hour-by-hour observation of a department to know what is happening.
2. The special follow-up to observe new employees, or new or changed tasks.
3. A required number of recorded safety observations per time period, e.g.,
 - a. Two per employee per month, or
 - b. Two employees per day.

Again we see the opportunities, not only for management guidance and direction of supervisors, but also the opportunities for analysis of system breakdowns and the measurement of performance.

If we hypothesize the highest degree of control of work by a JSA-JIT-SO plan, and actually set out to measure and document a departmental situation, we have to face a very real problem - the supervisor's time. An entry of N.D.T. (no damn time) should be a legitimate answer for a harassed supervisor, at least until management gives supervisors more aids and helps, or has developed new experience and standards as to spans of control and safety and other performance results to be gained from authorizing higher degrees of control (more time and budget).

One important point that is implicit in the JSA-JIT-SO system is that transfers to new jobs are "new employees" to that job. We still see accident reports which provide for total experience with the company, but not experience on the task. And transfers or changed jobs appear to be a more prolific source of errors than new employees.

c2 D/N Enforce. We come finally to the matter of rule observation and discipline. All companies with strong programs have some disciplinary system for repeated or major violations of rules. Obviously the JSA-JIT-SO plan eliminates much need for discipline by affirmative prior action. But, when discipline is weighed, the plan provides a background of clear rules, clear understanding, and a limited tolerance for variations.

Enforcement is, in theory, directed at the small minority who wilfully refuse to obey rules, or rebel at conformance. If a permissive attitude prevails regarding adherence to procedures, and rule-breaking is widespread, enforcement is probably not in order--neither fair nor effective. The general situation must be improved.

Bird and Schlesinger (1970) listed some side effects of punishment:

1. The employee may continue to behave the same way, but try harder to avoid being observed by the supervisor.
2. When the same behavior can lead to both reward and punishment, the employee will be in a state of conflict.
3. Conflict leads to frustration and aggression: the employee is likely to try to take out his frustration by reduced output, substandard quality, damage, waste, or fighting with other workers."

As a footnote he adds: "Of course, discipline may be necessary, but it is a last resort--never a solution to the motivational problem."

* * *

This section on supervision suggests such questions as:

1. Was the task assigned by the supervisor?
 - a. What instructions were given?
 - b. Was the task assignment one which the supervisor should make?
 - c. Was the task repetitive? How frequently?
 - d. If the task was non-repetitive, was the supervisor directly supervising? Do organization procedures require direct supervision of non-repetitive tasks involving potential injury?
 - e. If the task was not assigned by the supervisor,
 - (1) Was it an employee-designed task within the scope of an approved project?
 - (2) Was it a peripheral activity, not in conflict with rules (e.g., going to or from work on premises, authorized work breaks, etc.)?
 - (3) Or, was it an activity unrelated or prohibited?
2. Were the errors involved known to the supervisor?
 - a. What action had he taken?
 - b. Was correction delayed? How long? Why?
 - c. Had there been any employee reports or suggestions involving any of the errors? If so, what was the disposition?
3. When did the supervisor last see the man? Was he working according to procedure at that time?
 - a. When did the supervisor last see the person do this task correctly?
 - b. When did the supervisor last discuss safety with the person? What was discussed?

- c. When did the supervisor last make a safety observation (monitoring) on this man's work?
- 4. Describe training methods, aids, or procedures, which were specified.
- 5. Describe employee participation in hazard review and procedure development, if any.
 - a. Was this employee involved in job safety analysis?
- 6. Had emergency provisions been tested by simulation? How and when tested?

Some of the complexity of interactions of changes, training and motivation are revealed in the following incident:

A new employee was to repair a leaking flange in company with an experienced employee. The senior man went for some material. The new employee, motivated to show his eagerness (the eager beaver again) checked a gauge for pressure, saw zero pressure, forgot about the acid in a riser, and opened the flange.

35. EMPLOYEE MOTIVATION, PARTICIPATION & ACCEPTANCE

The title of the Chapter begins to expand considerations to the needed dimensions. Safety motivational programs, e.g., such common features as posters, contests, campaigns, interest-maintaining gimmicks, etc., are difficult to evaluate unless there is some stated context of motivational principle, including all-important opportunities to participate and to benefit from necessary feedback.

The organization of material in this area is difficult because of the lack of a framework of commonly accepted concepts.

MORT diagrams for analysis deal with a small, finite list of motivational programs, the emphasis being on ideas with some firmness in research support.

a4 Motivation. The analysis distinguishes directing the employee and motivation, and will examine interrelations.

Motivation is the last aspect of the Safety Precedence Sequence - partly because we know the least about it, and partly because the prior actions in SPS would seem to be a prerequisite for effective motivation.

The MORT analysis proceeds by first evaluating some specific aspects of motivation for which there is some factual or scientific information. These include, for example, schedule pressures, avoiding discomfort or effort, and the role of management concern, vigor and example.

b14 Job Interest Building. Herzberg (1968) says:

"The psychology of motivation is tremendously complex, and what has been unraveled with any degree of assurance is small indeed. But the dismal ratio of knowledge to speculation has not dampened the enthusiasm for new forms of 'snake oil' that are constantly coming on the market ... "

Herzberg then reports on experiments in job interest building and vertical loading. Reasons, research results, and principles are offered. However, the thrust is to improve general performance. A safety problem will be the degree of freedom permitted in high potential situations, a problem which was earlier seen in the suggestions of Jones and Rockwell that safety decisions be left in jobs.

More recently, Walton (1972) reports that job interest building and other single phase motivational approaches have not lived up to expectations. Nothing less drastic than comprehensive redesign of the workplace and work relations can get at the roots of worker alienation, in Walton's view. In reporting on one experimental plant, he says, "The safety record was one of the best in the company...", but cautions that new equipment and other variables were partially responsible.

b15 Group Norms Conflict and small group norms can effectively frustrate the goals of the larger organization. Two practical approaches are listed. (Also see Appendix G.)

c3 JSA Participation. This second reference to JSA is only intended to show that analysis, training or monitoring systems which provide opportunities for participation have double value because of the indirect benefits in participation itself.

c4 Innovation Diffusion. This research-based concept of developing desired behavior changes is discussed at length in Appendix

It seemed apparent at all three research sites that motivational programs were not formulated or judged and assessed from any clear-cut, articulated concepts. Consequently, for new methods or processes, obvious initial studies appear to be observations and tabulations based on the step-by-step progressions in innovation diffusion and acceptance.

The development of increased seat belt use would be a practical case for use of innovation diffusion techniques. While the start of an innovation diffusion program seems slow, that is, taking time for identification and personal work with key, influential innovators, it is often the short road to the goal. One-way messages won't work.

b16 Personal Conflict. Problems of interpersonal relations are also discussed in Appendix G. For the Deviant, the available answers seem to be, (1) treat, (2) transfer from a high potential situation, (3) terminate, or (4) tolerate--charge off to Assumed Risks.

b17 General Motivation Program LTA. Swain (1965) argues as follows:

"Aside from the ... difficulties and inconsistencies inherent in the slogan-and-sign approach to safety, have safety motivation campaigns been effective in modifying human behavior? What is the record?

"A search in the literature of industrial psychology has failed to show a single controlled experiment on the real effectiveness of safety motivation campaigns. A quotation from a USAF report may be revealing:

Over the past fifty years there have been innumerable campaigns of safety education, using all the varied media of advertising and propaganda. That the campaigns have in some measure been fruitful is suggested by the general diminution of industrial accidents over the years... Much of this reduction must, of course, be attributed to safety engineering, i.e., to reducing the hazards of the work situation. In fact, it is very difficult to isolate any part of the improvement in accident rates and say: 'This is due to our safety education program.' The possibility is not completely excluded that changes in the conditions of work together with changes in procedures for selecting and training

personnel may account for all the gain. Controlled studies of the effects of safety education procedures appear to be largely non-existent. Many articles state the value of the safety education program in a particular industry, but most of these are promotional articles offering little data on the relative effectiveness of a specific type of safety program."

At all three sites safety meetings seemed to be a "necessary evil." They are held, but their effectiveness is questioned. However evaluations are not carried out, nor are programs tested.

This study brought to light three anomalous cases, all involving people thought to be well-motivated:

<u>Meeting topic:</u>	<u>Accident Shortly After:</u>
1. Falls	Fatal fall from roof.
2. Hand tools	Permanent total disability from powder-powered tool.
3. An accident was discussed - partial amputation of finger moving heavy object.	Same kind of accident - same result.

These kinds of cases suggest the need for evaluating meetings. The meetings are alleged to be tiresome. If they are also ineffective, why not try something else - and measure?

In other accidents the motivation for general performance seemed exceptionally high--"eager beavers." Can these people be changed, e.g., taught hazard analysis, without slowing up their commendable drive?

Even in the proceedings of otherwise excellent Accident Review Boards, there are conclusions that people should:

THINK

BE ALERT

BE AWARE

The mechanisms to attain these states are not defined. Think - about what? How? Be Alert? - for what? What are the signals?

The role of supervisors can be examined against the guidelines suggested by Bird and Schlesinger (1970):

1. He will spend more time recognizing and rewarding safe performance, compared to time spent in disciplining employees for unsafe performance.
2. He will strengthen and enhance the importance of management-standards for safe performance.
3. He will focus attention on the importance of safe performance.
4. He will remind employees of the techniques of safe performance.

"5. He will be seen by the men who work for him as a colleague interested in their welfare--rather than as a disciplinarian (or 'nag')."

The role of participation in safety can be assessed in a program or in an accident by counting the specific opportunities. The form of participation seems less important than the substance. The critical incident technique has enough strength to suggest its universal value. On the other hand, most forms of cooperation, including some advocated by unions (e.g., labor-management joint committees) do not have records of proven value sufficient to prefer one form over another.

Obviously issues of equity, under-utilization or outright alienation in the plant will play a role in the background leading up to accidents, but assessing their influence in so-called safety studies may be impractical.

In Appendix G, Planek's Program Planning Model is presented for use in any program, but it is specifically aimed at motivational programs. The model requires hard work, but may be less painful than the disillusion of gimmicks and slogans. The model suggests examination of premises and information about a problem, direct and diffuse methods of reaching target groups, perceived relevance of message by audience, modes of presentation (e.g., humor vs. shock) and especially audience characteristics.

* * *

The spirit of an organization, or a safety program, cannot be ignored or underestimated. Lengthy periods without a disabling injury do not just happen. What is in doubt is whether propaganda did the trick.

"The intangible element of esprit de corps is one thing that separates healthy companies from candidates for the marble forest," says a veteran business analyst.

Lawrence's safety program is not systems or procedure oriented (with exceptions for certain areas). Yet Lawrence has a good record. Could it be that the high motivation for general performance, both in the safety group and the Lab as a whole, is a factor?

Behavioral Science Findings.

During the MORT Trials at Aerojet four documents were used in the design, introduction and implementation of specific safety program improvement projects:

1. Innovation Diffusion (Appendix H)
2. Appendix G (from the early edition of MORT) covered such topics as:
 - a. Participation and social forces
 - b. Supportive programs for the individual

- c. The individual in a sociotechnical context
 - d. The individual
 - e. Attitude
 - f. Changes in people
 - g. Motivation.
3. "Acceptance of Proceduralized Systems," (included as Appendix I), a summary paper produced because such acceptance can be seen as the Number One problem at Aerojet. The paper covered such topics as:
- a. Defined system goals,
 - b. Present Aerojet systems,
 - c. Personal variables in behavior,
 - d. Sociology and psychology of acceptance,
 - e. Deviant personalities,
 - f. A social science framework for acceptance,
 - g. Local factors,
 - h. Suggested Aerojet approaches.
4. "Improving Human Performance," Swain (1972), a new text already discussed as a "management method."

To the degree possible those working on various MORT projects endeavored to use the four documents as a frame of reference, and they seemed applicable and useful. However, two executive reviews of the materials showed broad agreement with the findings, but produced no consensus that they would be useful as a published organizational reference or guideline for management of the organization. The objections seemed to center on a "motherhood" tone of pious principles, and lack of clear-cut action plans.

The lack of action plans seems explainable by the view that principles of the type described are only a framework for handling serious current problems. They are not a program, but rather a philosophy. They can, however, be translated into a practice in day-to-day work.

Something of a stalemate in doctrine can probably be resolved only after further trials and study. In presenting this problem area to a seminar for AEC field safety directors in September, 1972, the material was handled about as follows:

1. You will spend a career trying to change human behavior.
2. Review appropriate materials and set down, at least in outline form, the group of findings, concepts and beliefs you will attempt to use.
3. Try out conscious applications of principle and measure effects.
4. Modify your practices based on experience.

No better advice seems possible at this time. Consequently a rather substantial body of reference material is presented in the three Appendices H, I and J.

Despite the problems, the role of people in MORT analysis and the safety program improvement projects at Aerojet has seemed to be clarified and steadily improved.

Role of People

As the logic of the MORT system has been made more nearly whole and tight, and as analytic and other technology has been assembled, the emerging system could impress one as a dehumanized or excessively technologic plan.

Fortunately, numbers of ways to help the people of the organization to do well at their jobs, participate in standards setting, and enhance job interest are also emerging. For example:

1. Improved concepts for management's responsibility and methods of meeting the challenges.
2. Improved supervisory concepts for both problem solving and handling people.
3. Improved services by and from one level of management to help subordinates.
4. Better methods for safety professionals, most particularly in management areas.
5. Greater attention to human factors, and reducing errors by improving the work situation.
6. Higher standards for designers and planners to help them fulfill their responsibilities, and the information and analytic services to back them up in their work.
7. Increased participation by the entire work force, as in RSO studies or Job Safety Analysis.

These mutually reinforcing approaches to helping the people control energy and changes are seeming to add up to a friendly, morale building, unifying approach to both safety and general performance goals. The techniques are kinder to the people in the system in that they recognize peoples' shortcomings, suitably offset or protect these, and then build on their strengths.

Running through this text is a seeming de-emphasis on personal, individual responsibility. This impression probably stems from the strong emphasis on helping people perform. The final reliance will, of course, be on individual managers, supervisors and employees. But it is to be hoped and expected that they will be given the help they need, and that personal responsibility will not be used to excuse man-traps left in the system, unwittingly and unnecessarily.

VIII. INFORMATION SYSTEMS

The model of a risk assessment system proposed in Chapter 21 (Figure 21-1) provides criteria for determining purposes, requirements and methods of constructing information systems. Details of hazard analysis were in Part VI.

In this Part we consider the working details of an information system which can implement the general risk reduction model, including hazard analysis and control of actual work.

The present, revised MORT concept of the elements of an information system is as follows:

INFORMATION SYSTEM

1. Technical Information
 - a. Knowledge
 - (1) Known Precedent
 - (a) Codes, Manuals, Recommendations
 - (b) Precedent
 - (c) Lists of Expertise
 - (d) Solution Research
 - (2) No Known Precedent
 - (a) Accident Investigation and Analysis
 - (b) Research
 - b. Communications
 - (1) Internal
 - (a) Network Defined
 - (b) Operations Adequate
 - (2) External
 - (a) Network Defined
 - (b) Operations Adequate
 2. Monitoring Systems
 - a. Management Routine Supervision
 - b. Search-out
 - c. Accident/Incident Systems
 - d. RSO Studies
 - e. Error Sampling Systems
 - f. Routine - HP, Inspection, etc.
 - g. Upstream Process Audit
 - h. General Health Monitoring
 3. Data Reduction
 - a. Priority Problem List
 - b. Summaries, Rates, Projections, Trend Analysis
 - c. Diagnostic Statistical Analysis
 - d. Depth Analysis of Special Problems
 4. "Fix" Controls (HRP Triggers)
 - a. One-on-one Fixes
 - b. "Priority Problem" Fixes
 - c. Planned Change Controls
 - d. Unplanned Change Fixes
 - e. New Information Use
 5. Independent Audit & Appraisal

MANAGEMENT ASSESSMENT
THE "WAR ROOM"

VIII

As organized in this text, perhaps the "revised list" should be revised! Chapter 36 - discusses some of the substance of technical information. Chapter 37 - Monitoring discusses principles and the specific system developed at Aerojet.

Chapter 38 - treats the major subject of accident investigation.

These two processes were developed before the concepts of information networks finally responded to analysis and the concepts in these three chapters become primary inputs into:

Chapter 39 - Internal information networks.

Chapter 40 - External information networks.

The internal network at Aerojet is a low cost, simple system, but is already producing more useful information than much more expensive, computerized systems used in many organizations.

The national information network has serious deficiencies.

Data reduction for management use, a most important need, took shape as two primary functions:

Chapter 41 - Measurement methods, some new and different concepts.

Chapter 42 - The "War Room" or safety control room with visible displays on measurement, error/accident reports, priority problem lists, upstream audit, and other problems leads into a brief, more definitive report to management.

Purposes and Requirements.

The primary objectives of measurement systems for the manager were stated:

1. Assess residual risk;
2. Take action, if risk is unacceptable.

Much of the occupational accident statistical material is of dubious or slight value for these two primary objectives. Standard injury rates are too often focussed on awards and comparisons, not germane to the objectives, and oversimplified and inadequate for any purposes. Group cause data compiled according to standard methods has little demonstrable decision value.

In consequence, it seems desirable to carefully separate types of data and their uses. Without clear definitions we may find ourselves back in the jungle of unrewarding arguments over standard rates which have confused and obscured measurement problems.

If past accidents were a stable, reliable measure of risk, the problem would be more simple. But accidents are statistically rare events. Therefore, the more severe the accident potentially, and the smaller the size or exposure of the unit, the less we can know from history about those potentials which concern us most. At the extreme, we need to know risk of "non-survivable" events.

While minor accident/incident reporting and error reporting have important uses, particularly in preventive work, such data must be used very carefully in predicting severe events (See, for example, Figures 3-1, 3-3, pages 38 and 42).

Therefore, we need data on major, individual risks by name (the "Priority Problem List") and on safety program, as well as properly analyzed accident data.

The requirements to satisfy the objectives are listed in a table below and flow diagram (Figure VIII-1) on the following page. As indicated in the chart (by underlining) and in the flow chart (by heavy boxes) the functions given detailed attention will be: Investigation, Group Cause Analysis, Incidence Analysis, Program Evaluation, and Control Evaluation.

Primary Data Requirements and Uses in Risk Reduction System

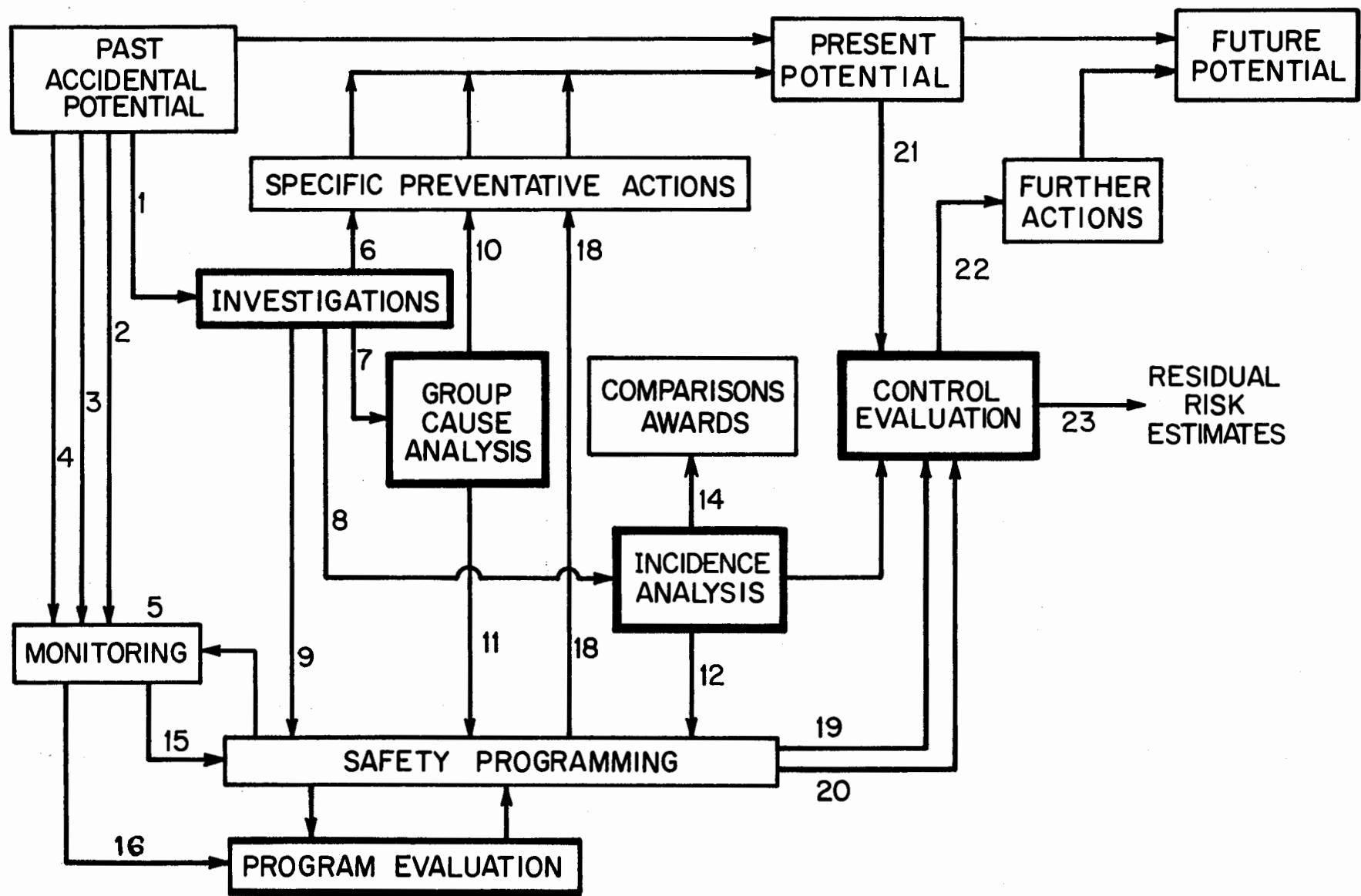
<u>Input</u>	<u>Operation</u>	<u>Data Type</u>	<u>Use</u>	<u>Output</u>
1. Accident/ Incident	Investigation	Basic (many systems) Supplemental In-Depth	Preventive Incidence Preventive Preventive	6, 7, 9 8 6, 7, 9 6, 9
2. Potential Hazard	Monitoring	Search Out	Preventive	15
3. Deviations		Systematic	Preventive Evaluative	15 16
4. Operational		Systematic Systematic	Rate bases Evaluative	13, 15-16 16
7.	Cause Analysis	Group	Preventive	10, 11
8.	Incidence Analysis	Group	Preventive Predictive Comparative	12 13 14
9, 11, 12, 16	Program Evaluation		Program Design	17
9, 11, 12, 15, 17	Safety Programming		Preventive Program Design Predictive	18 19 20
13, 19, 20	Control Evaluation		Preventive	22
21. Future Plans			Predictive	23

The following brief explanation is key to the chart and diagram:

1. Accident/Incident reports for the Investigative process are of three types. For prevention maximum numbers of reports are desired. For incidence, comparability is a criterion.
2. Potential Hazard - all possible reports are needed, from operational, safety or general monitoring and surveillance.
3. Deviations - changes, errors, and incidents, systematically monitored are needed for preventive and evaluative purposes.
4. Operational data are needed as rate bases.
5. Safety program should be systematically monitored, both for the safety supervisor's control of program, as well as for evaluation.

Figure VIII-1.

DATA FLOW - RISK REDUCTION SYSTEM



6. Investigation reports (as well as 7-10, Group Cause Analysis data) often result in direct line action to reduce hazards.
8. Reports for Incidence Analysis (coupled with 4. Operational data) produce rates and predictions used to (12) guide preventive efforts, (13) to predict risk, and (14) to make inter-unit comparisons, oftentimes for awards.
- 9., 11., 12., and 15. are primary inputs for safety programming, resulting in 18. specific preventive actions.
- 9., 11., 12., and 16. are used to evaluate safety programming.
17. Evaluations, with above program data, are used to develop improved program design.
19. Improved program designs, with estimated effects, are reported for control evaluation (which may include approvals).
20. "Priority Problem lists," effects of preventive actions (18), and additional countermeasure possibilities are put into control evaluation.
- 13., 19., and 20. are the basis for Control Evaluation and (22) further actions to reduce risk and (23) estimates of residual risk.

* * *

The concepts of measurement and control generally used attempt to follow those of Juran (1964). However, much remains to be done to precisely describe control elements before Juran's high standards would be attained. (See page 18.)

Planek's program planning model (Appendix G) is useful in developing the requirements for a planning process, for evaluation, and for prediction of results.

During this study, the author had the privilege of serving as "Chairman of Group III" at the National Safety Council's Symposium on Measurement of Industrial Safety Performance held in Chicago, September 15-17, 1970. The conclusions of the Group bear a strong resemblance to those of the author. Whether the group affected the chairman, or the chairman affected the group, and in what proportions, is indeterminate. But the group's report is so highly germane to the purpose of this study, excerpts are reproduced as Appendix K.

This page intentionally blank

36. TECHNICAL INFORMATION

An information or literature search has been stated to be a key element in a Hazard Analysis Process. The pieces of information to be handled by internal and external communications networks may range from research or a single precedent of accident or failure in an advanced technological process to the vast bulk of codes, standards and recommendations, which are really action consensus based on many "known precedents."

From common observation the bookshelf libraries of safety professionals are highly variable and somewhat spotty collections and dependent on the memory and personality of the man.

One test question used in this study was based on "Electrical Safety Guide for Research," an item in AEC's Manual Chapter listing recommended standards. Among both AEC and contractor safety personnel there were many individuals unfamiliar with the pamphlet, others who recalled but did not use the pamphlet, and only one laboratory where it was in common use. Not unexpectedly, in one serious property damage accident, the pamphlet was found to have been unknown to the designers and safety personnel involved. The pamphlet would have provided guidance and assistance.

Safety personnel commonly rely on their background of experience, and make a literature search only when baffled by a problem. Thus assurance that all relevant material, including new information, is applied is lacking.

From the MORT Trials at Aerojet the content to be handled, and minimal access methods by a low cost internal information network, appear to be divisible into three broad groups, with detailed definition of items to be included in each group as "a specific task for the local professionals.

- I. Major Sources- this would be a limited list including such items as OSHA regulations, NSC's Manual and Data Sheets, ASSE's bibliography, and perhaps cumulative indices to National Safety News and the Journal of ASSE. For this group, the information search protocol requires consulting the individual index of each publication. The Department of Labor has produced such an alphabetized index for OSHA.
- II. Other Published Sources- this would include pertinent lists of standards, reports, books, journal reports, etc. These would have at least minimal key word coding of titles, and would be inserted in a combined index using the key word plan described in Chapter 39.
- III. Technical Expertise- a list of topical experts (primarily local), e.g., cranes, chemicals, industrial hygiene or fire, provides a useful access to specialized literature as well as consultation. The same

key word system can interfile the names of experts with the material in Group II.

Existing technical information can be comprehended and managed by such a method.

Research as a means of providing needed technical information is a positive, articulated channel in aerospace and nuclear energy fields, but is not often used in general occupational safety.

Research should be seen as a way of answering the many, many questions in occupational safety. Yet business and industry have been singularly derelict in support; however, this may be in part because proposals have not been related to adequate concepts of practical system operations. Since research has an important place in system safety approaches, it would seem appropriate to measure performance on this facet of programming. The sequence of Research-Demonstration-Test-Evaluation-Application should be planned for. Support for more basic research is, however, also a need.

A review of developmental problems in safety research (Planek, 1969) suggests that factors include:

1. "... failure to view the accident phenomenon comprehensively as it relates to other sciences"
2. "Very often, the inability to find suitable 'measures' related to the accident situation rests on the inadequacies stemming from the state of the art in other behavioral and engineering disciplines rather than on a deficiency in safety research."
3. "Without two-way communication between 'program' people and researchers, the 'action' people do not obtain the advantage of research thinking and research findings, and researchers do not obtain the advantage of direct knowledge of 'action' people in regard to the setting in which accidents happen and in which research is needed."

A statement of research needs in occupational safety made in 1963 (Rockwell) remains largely unfulfilled in 1972.

The much heralded information explosion (technical information doubling every five years) again presents the recurrent safety question of emphasis on Method vs. Content. Although most accidents do not involve new technology, the information system must fulfill the needs of the organization. In considering technical information it is obvious that it is the Content that saves lives. Yet, if the safety professional does not have Method of processing, retrieving, and searching for relevant information, he'll either drown in content, or be unaware of relevant content, or both.

The information science people talk in terms of establishing information networks as a realistic way of coping with the unending flood and continuum of information. The construction of internal and external networks of information is thus a necessity to make sense or system.

37. SAFETY MONITORING SYSTEMS

Shortly before the trial of the MORT system began at Aerojet, an incident at one of the reactors led to an AEC recommendation that "audit and surveillance" be increased and improved. Thus major interest and study was and is focussed on the monitoring aspect of safety programming.

A wide variety of monitoring plans had been used, or were in use by Aerojet. Thus a very fertile field for comparison, analysis and planning was presented. Aerojet and predecessor organizations (Phillips Petroleum Company and Idaho Nuclear Company) had pioneered in many forms of monitoring, and could show persuasive evidence of values in certain plans and controls. Unfortunately, some of the better plans, as the result of a succession of organizational changes, had lapsed.

The Aerojet goal, as would be expected for materials testing reactors, is the very highest degree of safety and control. However, materials testing reactors present the problems which stem from a constant succession of changes, modifications, and experiment insertions - a much more difficult situation than that presented by relatively stable and unchanging power reactors. Control requires planning, engineering and development, and proceduralized operation of the highest order of excellence. The monitoring systems should be of an equally high order of effectiveness.

The Need for Monitoring.

It is axiomatic that complex systems depart from plans and procedures in some degree. Therefore, information systems are needed to detect deviations, initiate corrections, determine deviation rates and trends, and in general assure that goals are attained.

The Nature of Monitoring.

MORT presents monitoring as a final step in an ideal hazard reduction program. The principal elements of monitoring were listed as follows:

- A. Supervision, inspection, sampling, measurement, and appraisal.
- B. To detect Changes, Errors, Incidents, Accidents (we could add Deviations in general).
- C. This providing Hazard Analysis Triggers to reactivate the whole reduction cycle.

This definition clearly indicates that fundamental, searching analysis should follow detection of deviations. This definition should not obscure the need for fast action fixes to immediately restore the system to operational balance.

AEC's Standard for Quality Assurance (1969) provides that the scope of quality assurance includes the "means of control and verification whereby .. safe, reliable, economical operation will be achieved." The nature of the verification is elaborated: "Quality achievement shall be verified by individuals and organizations not directly responsible for performing the work but who are responsible for checking, inspecting, auditing, or otherwise verifying that the work has been performed satisfactorily."

In its report on the J-10 incident (previously alluded to) an AEC Investigating Committee defined two aspects of monitoring as follows:

1. Surveillance: "An overview or observation of an operation which may include tour of a facility, review of logs, instrument calibration, etc."
2. Audit: "A detailed, in-depth review of any operation as it is being performed by comparison of the operation with the approved procedure to determine the degree of procedural compliance."

Several aspects of monitoring which have emerged during the current study at Aerojet should be briefly enumerated (and will be discussed in more detail later):

1. The so-called "critical incident" technique taps the information store of operational personnel, and produces reports of large numbers of valuable, predictive events which are difficult to detect and relatively scarce in the usual audit, inspection, and surveillance programs.
2. The raw data from monitoring systems requires analysis and interpretation for managerial use. If voluminous reports of specific observations are handled on a one-at-a-time, crisis basis, operational continuity may be impaired, and fundamental, more permanent solutions are unlikely.
3. Those systems with built-in feedback to lower levels of supervision appear to stimulate the kind of immediate administrative action which can build higher degrees of control.
4. The monitoring system should follow information through to the determination of immediate, interim, and long-term action. However, long-term action may require substantial study and this may occur only as evidence builds up to show a chronic problem's importance.
5. The monitoring system should also follow the "upstream" processes by which hardware, procedures, and personnel are developed and delivered to the work site. The improvement of upstream processes may be more important than the correction of a specific work site error.

Thus, the concept of monitoring which is being constructed has the following elements:

- A. Detection of changes, errors, incidents, accidents and other deviations from system plans;
- B. By an optimum mix of observation plans of the following kinds:
 - 1. Normal, good supervision,
 - 2. Accident/Incident reporting systems,
 - 3. Audit, surveillance, checking, and inspection,
 - 4. Work sampling,
 - 5. Operational experience of personnel (prompted to report fully and accurately by appropriate study plans);
- C. Work site observation and upstream process observations;
- D. Internal operational, as well as independent, external sources of observations;
- E. With data analyzed and interpreted to provide:
 - 1. The feedback bases for rapid action at appropriate levels of supervision,
 - 2. Longer-term assessment of rates and trends to identify priority problems;
- F. Measurement of the fixes attained by the system.

This concept of monitoring is intended to have the broadest useful scope, rather than the narrow scope of individual, specific observational plans or methods.

Development Work.

The purpose of developmental work at Aerojet was suggested to be: Develop monitoring systems adequate to assess the degree to which the operating systems conform to prescribed requirements and procedures, provide a basis for assessing deficiencies in present control programs, and provide one element for residual risk assessment.

In a proposed safety project description the following observations were made: There is little literature on monitoring systems. Therefore, Aerojet has both the need, and the great opportunity, to develop a documented system of monitoring and surveillance. Such documentation can not only provide Aerojet with a better basis for its monitoring systems, but also make a major contribution to safety engineering principles.

Juran (1964), in the second half of his book, discusses control systems, and was considered to have furnished definitions and a frame of reference for the study.

Basic to control are standards of performance, and these are seen as having

two major dimensions:

1. A safety program schematic and/or description which adequately describes the safety and work systems to be monitored.
2. Error and deviation definitions which adequately describe the error standards or limits encountered in practice.

The inputs required for the design of a monitoring system(s) include:

1. Schematics and descriptions of operations and safety programs to be monitored.
 - a. Government and other standards.
 - b. What programs (as described) should do,
 - c. What programs could do - against higher standards (e.g., MORT).
2. Error and deficiency definitions as established by (a) precise criteria, (b) examples, (c) custom, habit or practice, or (d) debatable. Unfortunately, these are in ascending order of frequency and descending order of value.
3. Methods of sensing - for example, accident/incident reports, eyeballing work, qualification tests, critical incident studies, paper audit, process audit.
4. Direction of attention - for example, "hot spots," as well as time, place and other controls. Intuitive as well as defined controls seem useful.
5. Assessment of apparent strengths and weakness of various methods.
6. Manpower and other budgets.

Unless elements 1. and 2. above are stated in adequate detail, observations will be vague and debatable, and the efficiency of observation schemes will be low. Deviations will be more difficult to detect and will, in many cases, represent the subjective opinion of the observer. Results can hardly be reproducible measurements.

Although Aerojet is highly proceduralized, incidents and accidents reflect gaps in the procedural system. For example, in the J-10 incident the detailed procedure for the work of removing an in-pile tube reflected an assumption that routine task components such as welding or use of a crane would be performed in accordance with a set of predetermined safe practices. But the practices had not been reduced to writing for incorporation by reference. Job safety analysis, if performed, had not been recorded.

Similarly, requirements for pre-job briefing of crews were not clearly defined, nor was responsibility for stopping work when difficulty was encountered clear and fixed. Thus "forensic" standards were used in the incident analysis. Such standards are inefficient in the basic safety program and

particularly in the monitoring of the program.

Inspection for compliance with codes, standards, manuals and written procedures can be highly objective. But there is considerable subjectivity as well as variable technical competence in other observations of so-called "unsafe acts and unsafe conditions."

An anomaly in monitoring is that the better the definition of error, the more the possibility of error detection and outwardly high error rates.

A useful guide to the scope of monitoring is found in the AEC Quality Assurance Standard: "Operation, maintenance, and modification efforts include quality assurance through systematic planning of work; application of work instructions or operating procedures for controlling operation, maintenance, and modification; preparation of records and reports of operation experience; and performance of scheduled, periodic inspection and testing."

Early in the developmental work it seemed clear that possible gaps in the program would have to be defined if monitoring was to provide a basis for a tight system of control. Thus, monitoring could yield two types of observations: (1) deviations from the system as promulgated, and (2) deviations of the promulgated system from a higher order system.

Ordinarily it would be expected that a safety system would be first improved, and results then monitored. In this case, it became necessary to at least postulate certain safety program improvements for assessment if monitoring was to make a maximum contribution to a high degree of control.

The error literature contributes, not only the notion of values in precise definitions of error, but also the need to collect "error opportunity" data to make possible the calculation of error rates, or conversely, reliability. Few past monitoring schemes had collected rate base data. Yet, initial inquiries into availability of such data showed it was often readily available - for example, total warning tags checked as compared with tags in error, total tests required as compared with tests not made or not recorded. Thus, a valuable criterion for evaluating any monitoring scheme emerged.

Not all monitoring schemes can routinely collect error/opportunity data. However, wherever practical, an initial report of error should be followed up to get a rate assessment, preferably in terms common to earlier observations.

A basic concern in developing monitoring systems is the accessibility of information:

- a. Many actions or conditions can be detected by observation at the scene by supervisors or auditors.
- b. Certain actions "leave tracks" which can be detected in records, conditions or subsequent actions.

c. Some actions are known only to the persons who did them.

Only a few monitoring systems obtain the third class of data.

The program position and function of monitoring (and independent review, as well) should be as downstream assurances that the safety process is operating as intended. The primary reliance is on upstream processes of hazard analysis, hardware-procedure-personnel development, and work supervision. A desirable strategy would be to optimize upstream processes. The allocation of effort to downstream review and monitoring should be minimized as possible and practicable in order to allocate maximum resources to upstream preventive work.

Evaluation of Specific Monitoring Schemes.

The work of evaluation of various plans was performed in large part by R. J. Nertney, Ph.D., Nuclear and Operational Safety Division, Aerojet. Dr. Nertney was able to draw on his extensive experience in supervising or conducting earlier trials of many monitoring plans. Aerojet thus provided unique and valuable experience, as well as professional competence, for the in-depth assessment of a wide variety of monitoring plans.

The method employed was to list some 23 descriptors and criteria of monitoring plans, and then set down a judgment of strength or weakness of a plan for each of the criteria. Also, if a program was design sensitive, that is, could easily be swung from strong to weak dependent on program design, such a judgment was set down.

Later, the detailed criteria were combined into a single evaluation for each of four broader criteria: (1) low cost, (2) reliability, (3) perceptivity, and (4) action propensity. A fifth broad criterion was then added, namely, capability for upstream process audit (as contrasted with work site audit).

As finally utilized the broad groups and detailed criteria were:

I. Low Cost

1. Direct, additional expense
2. Negative impact of sampling mechanism on normal, organizational activities.
3. Negative impact on other work from diversion of effort to monitoring.

II. Reliability

4. Objectivity
5. Ability to validate raw findings
6. Ability to set up monitoring and control systems
7. Ability to classify, scale, and generalize conclusions
8. Ability to maintain observational effectiveness - that is, reliability in attention and seeing.

III. Perceptivity

9. Relevance to operational safety problems.

10. Ability to reveal different safety-related information than that already known to line management and supervision (qualitative).
11. Tendency of auditors to direct effort into "proving" preestablished conclusions.
12. Scope--ability to monitor a wide variety of organization work.

IV. Process Capability--ability to audit upstream processes which produce hardware, procedures, and personnel.

V. Action Propensity

14. Ability to set up corrective feedback loops (mechanical)
15. Tendency for line organization to set up corrective feedback loops without stimulation.
16. Ability to convert findings to specific operational response (based on quantity and quality of data).
17. General acceptance by line organization.
18. Tendency for line organization to rationalize findings.
19. Visibility.

Results of the Evaluation are shown in Figure 37-1 on the next page.

The 28 monitoring mechanisms evaluated according to the above criteria are generally reported as follows: (a) Brief description, (b) Evaluation, (c) Recommendation, (d) Subsequent Action.

I. The Operating Organization.

1. Management routine supervision - the normal surveillance, trouble-shooting, change and problem detection, with aggressive and vigorous search-out as a characteristic to be desired and cultivated.

Evaluation: The marginal additional cost for safety functions is low. Reliability and perceptivity are poor, and if this evaluation seems surprising, the detailed criteria given above should be reviewed. Process audit capability is good. Action Potential very high.

Recommendation: Continue to emphasize authority, control and prompt action, and sensitivity to the role of changes.

At Aerojet certain incidents have in degree sensitized personnel to change, but this is a costly route. One reactor has a system of daily reporting of "anything of possible significance" not provided for in logs. The logs record a variety of changes. The problem is in selecting significant items from the mass of continuous changes.

2. Management audit time budgets internal to the operating unit - time requirements for the audit function outside the normal scope of responsibility, or allocated to back shifts or other functions not normally receiving necessary attention. Also, the same, from higher levels of the organization.

Evaluation: A relatively costly program which it is suggested be redirected from the work site to process audit for which it probably has unique capability.

3. Error sampling.

- a. In-house staff sample errors. The operating manager's staff systematically sample operating errors using checklists or definitions. Aerojet's predecessor organization utilized such a plan with Shewhart control charts fed back to supervisors. There is need to standardize the denomina-

Figure 37-1. Results of Evaluation

Numbers from 0 to 1 = "Poor" to 4 = "Good or Strong" were used.

	Low Cost	Relia-bility	Percep-tivity	Process Capability	Action Propensity
I. The Operating Organization					
1. Management routine supervision	4	0	1	4	4
2.a.Audit time - internal	2	0	1	4	4
b.Audit time - higher	1	1	2	4	3
3.a.In-House error sample	2	4	3	0	4
b.Project engineers	3	2	3	0	1
c.Supervisor checklist	2	4	3	0	4
4.a.Redundant - training	1	0	2	0	0
b.Redundant - operations	1	1	2	0	1
II. Safety					
1.a.Field engineer	1	3	4	2	2
b.Health Physics	1	3	3	0	2
2.a.Surveillance - work	1	2	3	3	1
b.Surveillance - paper	2	3	2	4	1
c.Surveillance - review	2	3	2	4	1
3.a.Hq - review	3	1	2	4	2
b.Hq - audit time	2	3	2	4	2
4.a.RSO - C.I. Studies	2	3	4	2	4
b.Special studies	1	4	3	4	4
5. Reporting Systems					
a.Accident/Incident	3	4	3	2	4
b.RDT Incidents	3	4	3	2	4
c. Control Charts	4	4	3	0	4
III. Other					
1. Technical support	3	3	3	0	2
2. Conventional audit	2	3	3	4	2
3. Quality Assurance	3	4	3	4	3
4. Miscellaneous	3	0	3	0	1
5. Outside - technology	2	2	2	0	3
Outside - method	2	2	2	4	2
IV. AEC					
1. Review	3	2	2	2	1
2. Audit time	2	2	2	2	1

tor, which is an hour of structured observation by the same or comparable persons employing a relatively simple (14 class) definition of kinds of errors to be observed.

Evaluation: The apparent results were spectacular - in a response time of 5-6 months it appeared that normal administrative controls reduced operating errors to relatively stable levels at the lower limit of previously wide fluctuations. Thus a substantially lower average rate was produced. (Figure 37-2.)

Recommendation: reinstate.

Action: This is the only recommended work site monitoring plan not yet implemented.

Figure 37-2.

OPERATOR ERRORS vs TIME

Data Sampling

Data Sampling and Feedback

Vigorous
Management
Attention

- 359 -

Errors Detected

300

200

100

0

First Year

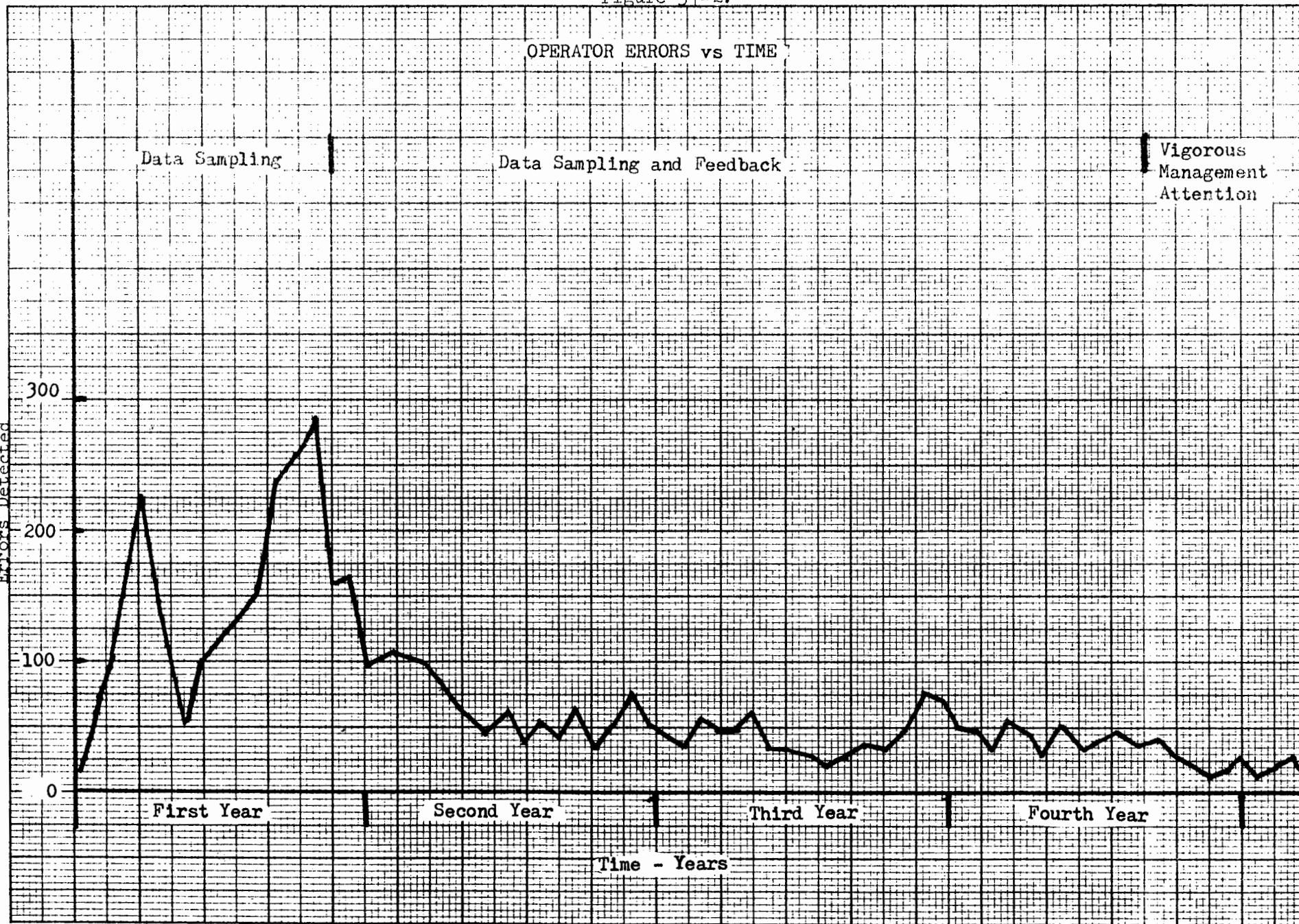
Second Year

Third Year

Fourth Year

Time - Years

Error Sampling



- b. Project engineers evaluate operating shifts. This type of study proved useful in detecting inter-shift differences (or lack thereof) in two plants. (Nertney, 1965.) Repeat occasionally.
- c. Supervisor checklist for reactor operators. The checklist was developed by American Institutes for Research (1968) based on a "critical incident" study of reactor operations. The list provides task-specific definitions of good and bad practice. (For those not familiar with nuclear reactors, it is probably well to say that the errors do not permit a major nuclear reaction, since the reactor "scrams" itself automatically for any kind of instrument anomaly. However, the errors do relate to performance, experiment handling, and more routine accident/incident types involving personnel.) (Other supervisor safety observation plans, such as U. S. Steel's plan shown in Figure 30-1, were not evaluated at this time, although one or more will be suggested for other than reactor operations.)

Recommended, and carried out, May, 1972.

- 4. Redundant employee audits - two examples of providing a redundant, extra employee with only audit functions were evaluated:

- a. Training representative audits procedural compliance,
- b. Operations employee audits for a single type of fault.

These expensive forms of audit have a limited usefulness because human factors studies have shown their unreliability. In the J-10 incident the training representative failed to function in time of need.

The evaluations suggest the effort be discontinued, or redirected into other more effective programs.

II. Safety Division.

- 1.a. Field safety engineer - inspection and search out. Routine inspection reports (largely housekeeping) are valuable, but may not detect major hazards. The independent search-out of hazards is vital, but is highly dependent on personal characteristics and was difficult to scale and measure.

There was no doubt that the work of the field safety professional was highly valued, so scaling or measurement was abandoned for the time being. Later, a schematic and audit plan was developed. See Part IX and Exhibit 16.

- b. Health physics field monitoring - a necessary, valuable, and routine program in reactor operations. The merits and values of fixed monitors versus personal monitoring for radiation were not examined. Obviously a mix of the two types is needed. A computerized radiation badge record system is maintained.

- 2. Surveillance Branch - a unique organizational unit for independent monitoring of both operations and the safety program itself. It includes:

- a. Work audits and spot checks for procedural compliance,
- b. Paper audits - e.g., review of work documents, such as procedures, for compliance with sign off and other requirements, and
- c. Review failures - detection and analysis of failures in utilizing Aerojet's highly developed independent review processes.

Evaluation: a basic question has proven to be the cost of specialized safety observations as compared with general observation plans which include safety. Thus, responsibility for field audit of procedural compliance has now been concentrated in the Quality Assurance program. Paper audits are relatively inexpensive, but produce the least significant information. The recommendation was made that major portions of time be shifted to audit of

"upstream processes" and such interdepartmental processes as shipment of radioactive materials. This has been done, and a list of 39 such special audits prepared and rank-ordered by a scaling mechanism. The work proceeds well with schematics, steps and criteria for each such study.

3. Safety Division headquarters

- a. Annual Reviews - field reviews of overall program used as an input to work of Review Boards. (The annual and special Boards are described on page 238.)

These programs (at whatever level conducted) seem weak. They are highly affected by the reviewer. They often concentrate on one program aspect in order to attain depth (which implies that comprehensive review will take five or ten years).

Restructuring in two respects is suggested: (1) adopt a comprehensive framework for review, and (2) adopt a plan for internal ongoing program measurement so that a comprehensive annual review is possible.

- b. Audit Time Budget - field review and audit of safety division functions.

Audit of Safety Division functions has value, but produces little input for a manager's overall risk assessment. Results should be translated into operational inputs to management.

Also, a later recommendation was made that this time budget be systematically directed to high energy units and locations, and utilize the more intensive audit plan developed for field engineers. (Part IX.)

4. Special studies.

- a. Reported Significant Observations (a substitute term for the traditional title - Critical Incident studies, since the events are neither "critical" nor "incidents" as those terms are used in nuclear operations). Such studies, whether by interview or questionnaire have proven capacity to generate a greater quantity of relevant reports than other monitoring techniques, so much so as to suggest their presence is an indispensable criterion of an excellent safety program.

RSO-CI and other special studies have excellent capabilities for direction at primary problems. Although Aerojet's predecessor organization pioneered in the RSO-CI studies, a present review of their organizational impact suggests several weaknesses to be corrected. The raw material was distributed, rather than classified and assessed in forms suited for managerial action. The reports were not indexed and otherwise made accessible to designers and planners. The principle reservoir of information on potential troubles appears to be in the heads of the people doing the work and their immediate supervisors and associates. A limitation is, of course, their lack of knowledge of underlying factors. The so-called "critical incident" technique has produced more information on the seemingly minor errors or deficiencies than other forms of monitoring. And we now have persuasive case histories to show the preexisting errors and deficiencies do, ultimately, occur sequentially and create major incidents.

Several major, recent incidents have been shown to have occurred by sequential linkage of lesser events reported two or three years earlier in RSO-CI studies. Thus, two major points are underscored:

- (1) The RSO-CI studies do provide the necessary reports for the safety process.
- (2) The relevance of so-called minor deviations in causing major incidents supports appropriate management attention to the minor events

as they are currently reported.

Further discussion of incident recall is in Appendix D and a sample of Aerojet's forms are provided in Exhibit 13.

One RSO study has already been completed, and others are scheduled. Three fix cycles are set-up:

- (1) Quick pulls of clusters of reports showing high likelihood of cumulating into major sequences are furnished to Branch managers.
 - (2) All reports in an indexed binder are furnished to line management and upstream processes, such as engineering or training.
 - (3) Project engineers are required to use the key word index and produce an information display and analysis.
- b. Other studies - special questionnaires and analyses to detect problems and causes. These task-oriented studies are also an indispensable supplement to on-going, continuous monitoring systems.

5. Reporting Systems.

- a. Accident/Incident reports of the basic AEC reporting system.
- b. RDT Incidents - the auxiliary reporting system operated under RDT standards.
- c. Control Charts - Shewhart control charts were formerly used to provide supervisors with assessed feedback, with experience similar to that for error charts.

Reporting systems are the most fundamental and valuable of independent monitoring programs. However, they require verification of completeness of reporting. Also, the records of follow-up action - immediate, interim and long-term - should be complete and actively reviewed, as is the case with the RDT system.

Reporting systems can be brought to full utility only if a flexible, supplemental reporting system is inaugurated. An example of such a report, one of a series used for short periods to get sample data, is shown in Figure 37-3. Further, the usefulness of reporting systems (as with RSO-CI reports) will depend on their accessibility and retrieval for future engineering, development and planning.

The basic accident/incident reporting systems of AEC are briefly listed on page 198. Also, a computerized process is operated, including first aid cases, by AEC-Idaho.

It is essential that fix cycles be established for accident/incident reports in the manner required for AEC-RDT incident reporting: (1) Immediate action, (2) interim action, and (3) long-term action.

Aerojet has placed the control charts in operation. An early example is shown in Figure 37-4. The current charts are being printed out from a standard computer program. They don't look pretty, but are cheap and quick.

The calculations used to derive control limits are standard:

1. A Poisson distribution of accident rates is assumed.

2. Upper control limit = $I_e + 1.64\sqrt{I_e}$

- a. $I_e = R \times \text{man hours in period}$ (expected injuries at rate R of previous two years)
- b. The limit gives a 95% confidence limit, that is, there is only one chance in 20 that an observed rate above the limit could occur due to chance.

The interpretation of the charts can cause trouble, that is, the rate is

Figure 37-3

Supplemental Accident/Incident Report

Proceduralization

1. Was task under a Detailed Operating Procedure? _____ Yes _____ No.
2. Was task under a Safe Work Permit? _____ Yes _____ No.
3. Did either cover the specific safety aspects of the task? _____ Yes _____ No.
4. Was there any other written safety procedure covering the task? _____ Yes _____ No.

If yes, specify. _____

5. Was the task repetitive? _____ Yes _____ No. About how frequently? _____

6. Describe the hazard review given the task prior to the accident. (Who?
When? What was decided?) _____

7. When did the supervisor last see the person do the task correctly? _____

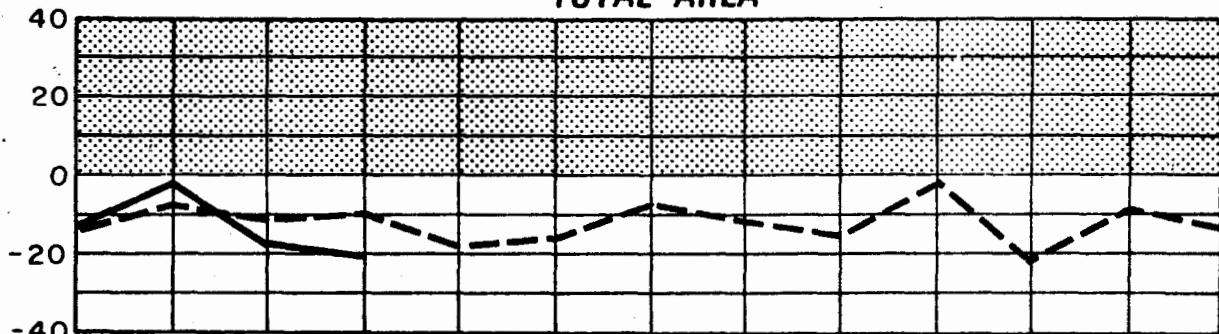
8. When were the physical elements (area, tools, etc.) last inspected? _____

Figure 37-4

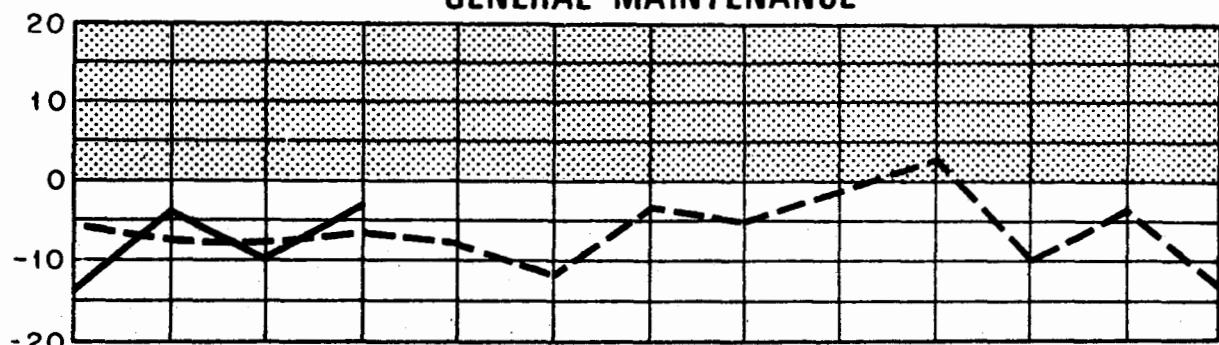
CFA OCCUPATIONAL INJURY CONTROL CHART

Previous ----- Current —————

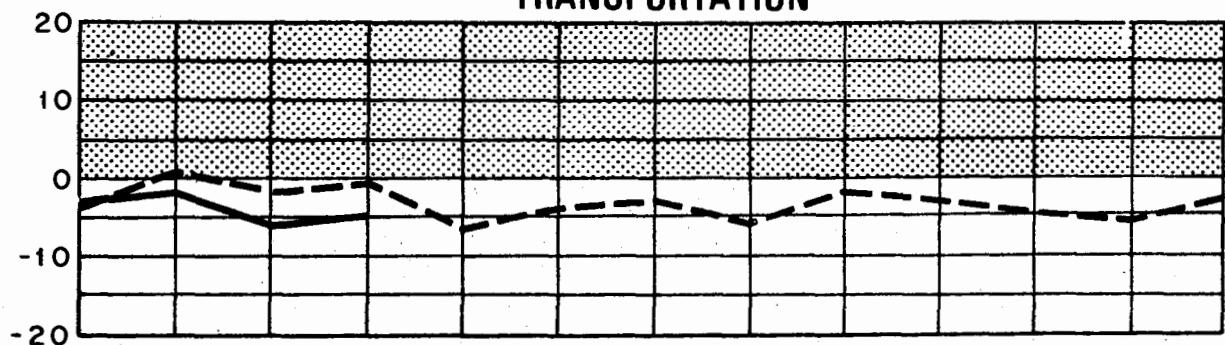
TOTAL AREA



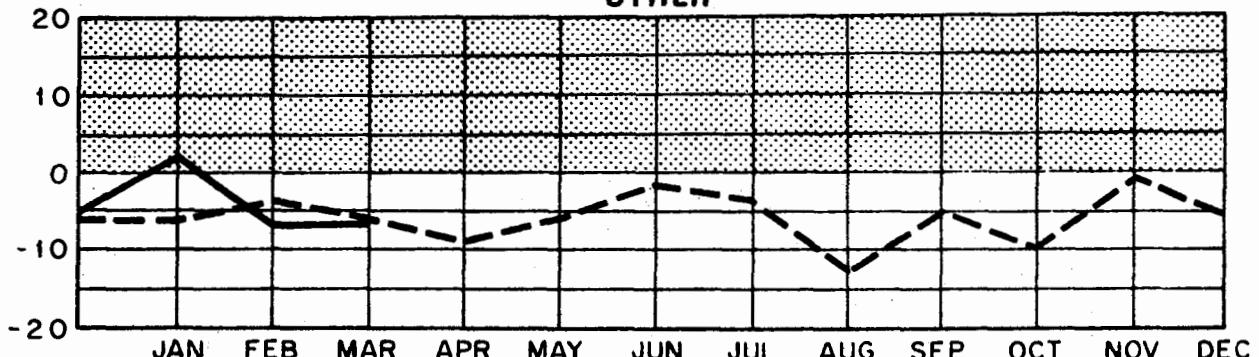
GENERAL MAINTENANCE



TRANSPORTATION



OTHER



Points above zero indicates injuries above normal

not "out of control." There is likely an assignable cause for the variation, but this could be added emphasis on reporting, or a new, pretty nurse! The charts could be called Change Control Charts.

One other reporting system, "High Potential Incidents" not meeting any other criteria, was not analyzed. (Comment on HIPO reporting will be found on page 189.) At no site has a HIPO plan been found to produce more than a few valuable reports, and Aerojet has such a plan, as should others. However, the critical incident technique produces vastly more useful information.

III. Other.

1. Technical Support - monitoring functions. Operations supervisors can be sensitized to report aberrations and deviations for technical analysis, and this has been and is being emphasized. In such instances technical assistance is requested. However, there are past incidents to suggest that field monitoring and inquiry by technical personnel will likely produce earlier and more comprehensive detection of operating problems.
2. Conventional auditors - the managerial staffs who regularly audit field compliance can include some aspects of safety. Where pertinent records are available, large numbers of observations can be made at low cost. However, the forms of deviations of greatest significance may not be detected.
3. Quality Assurance - this major program, largely hardware and procedure oriented was evaluated to only a superficial degree, partly because it is apparently very well organized and operated. When the overall monitoring schemes were developed (and the current effort is more concerned with human error control) it was suggested that three potentially valuable steps be taken:
 - (1) The present Quality Assurance programs be placed in perspective on the safety program schematics,
 - (2) QA data be integrated into the managerial risk assessment plan,
 - (3) Dependent partly on results in (1) and (2) above, a safety audit and evaluation of QA similar to this effort be considered.

To avoid duplication of effort, the principal independent surveillance role was assigned to R & QA. Valuable reports are being produced to show the procedure audited, number of steps, compliance (with nature of non-compliance, variations, and revisions adequacy. A periodic report showed the following kinds of data:

Procedures audited	25
Total steps	1,497
Steps audited	1,390
Compliance variations (99.6% compliance)	6, or 0.4%
Revisions needed	19, or 1.4%.

Such data can become a reliable basis for trend analysis.

Confirming an early hope, the reliability and low error rates produced by this plan produced a recommendation that the surveillance effort could be lightened and yet maintain control, thus saving money as well as benefiting employee attitude and acceptance.

4. Miscellaneous "Look and Run" - the variety of people who make casual, collateral observations.

5. Outside experts
 - a. Technological
 - b. Methods or process of analysis or program review.

IV. AEC Surveillance

1. Periodic review and appraisal.
2. Audit time budgets.

(Aerojet did not participate in analysis or evaluation of AEC programs.)

Comments above on annual review procedures seem relevant to AEC programs, but require first implementation by Aerojet. The criteria employed to evaluate Aerojet monitoring should be considered for use by AEC as a possible means of enhancing the values of its monitoring work. The values in independent observations seem clear. However, as possible and practical, AEC should extend itself, for example, in classifying and scaling significance of observations, collecting rate base data, or giving attention to upstream audit potentials.

Preliminary plans have been developed with AEC-DOS to perform its next audit and review of Idaho operations by a system appraisal, because Aerojet will have most or all of the basic data needed.

Inspections. A variety of these programs ranging through departmental or divisional checks, field safety engineer monthly inspections, and R & QA audits of cranes, slings and such equipment. The topic has already been discussed in Chapter 31.

In the monitoring study, two recommendations were made regarding Aerojet's many inspection programs:

- (1) A detailed listing of inspectional responsibilities so that effectiveness can be systematically audited and measured (QA may have this in part)..
- (2) Fuller use of point-of-operation maintenance and inspection logs to facilitate field monitoring.

Summary of Monitor Plans.

In order to provide a framework for summary or analysis of overall plans for monitoring, the general work process schematic (Figure 29-1) was used.

This distinguishes primarily:

1. Work Site plans,
2. Upstream plans.

The Work Site plan for error reports was summarized and is shown on the next page.

From the study, it was argued that improved control could be achieved by a well-designed effort, at less cost, and with less work site impact. The suggestions for error monitoring at the work site reduced levels of effort, but are still extensive. Several ineffective systems were dropped. The audit time budgets could be transferred to upstream work. Theoretically, it had been

Summary of Work Site Plans for Error Reports

<u>Methods</u>	<u>Internal</u>	<u>Independent</u>	<u>Who?</u>
1. Management routine supervision	x		
2. In-house staff sample w/ control charts.	x		
3. Injury control charts		x	NOS
4. Check-list used by supervisors	x		
5. NOS field engineers*		x	NOS
6. HP monitoring*		x	NOS
7. Procedural surveillance		x	QA
8. Spot checks*		x	NOS
9. File audits	?	x	
10. RSO studies	**	x	NOS
11. Technical support		x	
12. Miscellaneous	x	x	

*subject to NOS headquarters audit.

**internal input; external analysis.

possible to have 16 people observing an operator, if all monitors arrived at once - the actual record was seven!

With all plans, except number 2., implemented, the prediction seems correct, fewer monitors and the factor of participation in RSO studies have had favorable morale effects.

Audit of Upstream Processes.

Upstream audit emerged as a vital and underemphasized aspect of monitoring. However, it is probably best understood in terms of some of the specific schematics of Aerojet's reactor operations.

In the organizations studied to date, there is a notable absence of work flow or safety program schematics and descriptions. Consequently, it is unnecessarily difficult to examine the adequacy of monitoring programs and the deviation or error definitions which monitoring requires. In accident investigations it is difficult to trace the upstream processes which should have prevented the accident.

Even though the diagrams which have been developed for Aerojet are specific to that organization, and are based on its procedures and organizational elements and responsibilities, it should be generally useful to examine Aerojet schematics as instructional examples of values, problems detected, and methods of analysis.

A basic safety-related work schematic was developed and subschematics were developed for elements of the process.

The basic Work Flow schematic (Figure 29-1, already discussed) can be examined from the top down, or one can begin at the work site and proceed upstream to examine the process by which ingredients of work were delivered to the work site. The latter approach has seemed to be of greater value in producing potential audit points likely to be significant.

Within the time available in the study, only preliminary "walk through" analysis of upstream processes was possible. But even a crude analysis revealed a number of kinds of deficiencies:

1. Gaps in responsibility (particularly at interfaces).
2. Sequential operations in which each believes the other performs a necessary task (the usual interface slippage).
3. Incomplete analyses.
4. Vague or nonexistent criteria for judging adequacy of an operation.
5. Specific hazard reduction operations of a higher order (MORT) which are largely unfulfilled (e.g., literature search and human factors engineering).

The impression was clear that Aerojet's fine, extensive effort at proceduralization results in lengthy documentation which needs simple schematics and detailed audit to reveal the kinds of deficiencies suggested above.

A few details of the subschematics, in their original incomplete form, are furnished in Exhibit 14 simply to illustrate the value of even a simple, exploratory effort. Incomplete as they are, they show many possible audit points. They led to the following specific recommendations:

1. List the processes requiring audit:
 - a. Major-ongoing processes, such as
 - (1) Engineering modifications,
 - (2) Projects
 - (3) Configuration and Document Control
 - (4) Hardware - construction, installation, test, etc.
 - (5) Personnel Systems
 - (6) Procedure Systems
 - (7) Review agencies.
 - b. Safety functions.
 - (1) Anti-C Clothing
 - (2) Health Physics Instruments.

c. Inter-department functions

- (1) Shipment of radioactive materials
- (2) Critical facilities
- (3) Preventive maintenance

(Later a list of 39 such topics was developed.)

2. Develop schematics, steps and criteria.

The acceptance of the monitoring study was followed by major work to develop the needed schematics, steps and criteria (pages 193-5). A wall chart on the program showed the need:

MANY BLOCK-FUNCTION WORK SCHEMATICS.

STEPS TO FULFILL EACH FUNCTION

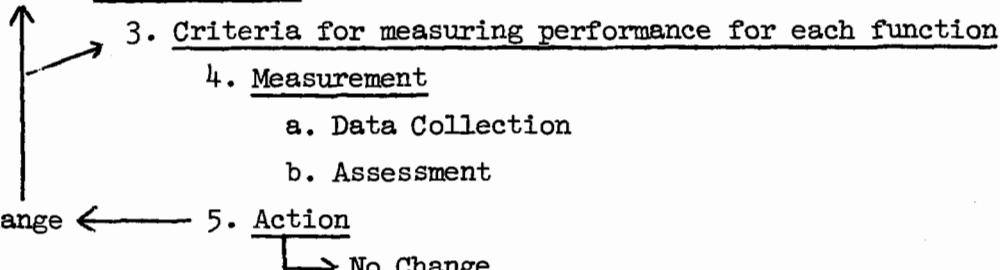
CRITERIA TO KNOW WHEN THE JOB'S WELL DONE

As rapidly as these are completed, major portions of time are being assigned to audit and correction.

The analysis of upstream processes can be seen as proceeding through five major phases:

1. Broad Function

2. Who Does What?



It is possible to use MORT charts to chart audit points and plans in operation, and further needs. Also, the Nertney Wheel, Figure 24-6, is a useful schematic to design audit points and methods.

A step-by-step plan for design of a safety monitoring function, also prepared by Dr. Nertney, will be found in Exhibit 15.

MORT diagrams touch on dozens of monitoring systems. However, the list is far from complete.

It is useful to make a separate list of monitoring systems in an accident, using these kinds of questions:

Describe the monitoring (work sampling) procedures used to measure the safety level of this work area.

- a. When was the area last monitored?
- b. What were the findings? Was the level of safety improving or retrogressing?

As a general study, a set of diagrams can be used to note all the monitoring systems present in an organization. Filling the gaps revealed is a major aspect of program improvement.

Aerojet's highly developed Independent Review System includes within its Nuclear and Operational Safety Division a small unit, Operations Surveillance Branch, with the primary objective of observing, reviewing, evaluating, and reporting field compliance with established safety rules and standards.

In addition, from its experience, the Branch reports on apparent needs for additional controls, improved training, and other possible improvements. It reviews operating incidents and near misses. The Branch also, at management's request, audits non-safety aspects of performance. Through a formal reporting system for failures in the review process, as well as by observation, the "black hat" also audit the safety operations internally. The Branch follows up to see that recommendations are carried out and needed studies are performed. All this is in addition to the normal surveillance and search out of field safety engineers, industrial hygienists, and health physicists.

Monitoring can be seen as of two types:

1. General - in conjunction with normal activities,
2. Specialized - time or personnel allotted specifically to the monitoring function.

Sources of observations in both categories can be seen as:

1. Field Observations,
2. Creation of, or review of, "paper" information systems, e.g., work orders, or departmental reports of JSA coverage, or general operating reports.

At one site, preventive maintenance was computerized, but no one routinely monitored overall attainment.

The four-way classification can, in turn, be divided into "potential trouble" orientation and "work sampling" orientation.

Correctly the bulk of a monitoring force should go to the spots (time, place, process) estimated to have the highest accident potential. The safety engineer's studies and intuitive sensing combine to help him ferret out causes before the accidents occur. However, he may develop his comfortable habits of observation. Therefore, a non-directed control is needed.

Some portion of time, however small, should be assigned to reproducible, randomized observations. The long term value of making comparisons, and of having the randomized system send observers to "out-of-the-way," and normal, supposedly non-hazardous operations is believed to be substantial.

The work sampling schemes can be of a wide variety of types - critical incident studies, observation tours, etc. Photographic methods are being studied.

All of this is in addition to the normal feedback given to people to help them do a better job.

Need for rapid feedback (monitoring) to correct errors is axiomatic--and increasingly recognized at the operator level of man-machine systems. But the principle is not fully implemented at the managerial level of occupational systems.

Feedback devices should be built into systems. Just as maintainability and preventive maintenance plans are facets of the development process, so plans for monitoring performance for conformance with plans are an essential for management.

The need for monitoring systems arises from the principles of control and "management by exception." The skilled manager concentrates his attention on the deviations from plan or standard. To do this, adequate monitoring systems must be in place and operating to give signals when deviations occur.

General Program Audits. Audits of the safety program of a plant or of a typical or a high rate department of a plant, are a common feature of large company and government programs. One company reports two to four man-weeks as a normal requirement for a biennial audit. (Windsor, 1969.) Most audits use corporate headquarters personnel, but some also use operating personnel from similar plants (Wilson, 1969). Naturally, either type of personnel would bring to the audit a thorough knowledge of organization practices and expectations.

However, both a steel company and the accelerator groups at Lawrence report that audits really get tough when operating executives from comparable installations made the appraisals!

AEC has a comprehensive safety staff appraisal system. Greater use of advanced technology groups from representative locations might be valuable.

Neither AEC nor its contractors now have data systems which provide the raw material to "monitor, audit, compare" nor does any other organization. The design of such systems should be a major program improvement objective.

The concepts discussed in this text suggest an altered or additional approach to audit of an organization or plant:

1. Adequacy of safety system design as compared with stated criteria.
2. Results of system operations:
 - a. Data
 - b. Fixes
3. When was the monitoring system itself audited by the organization or plant? (Findings and action?)

4. How does the organization or plant know the system is not failing?
5. Field spot checks to verify above.

Auditing experiences on large-high-energy machines suggests, however, that system considerations, e.g., the need for strict change control, will not be seen by managers as major needs unless incident data from a group of similar machines is available to provide illustrations.

Accident investigation is, of course, one obvious way to check the safety program. The following questions are indicative:

1. Was the safety department's technical information adequate in this case? Describe how relevant information had been transmitted and disseminated. Who? When?
2. When did the safety department last inspect this area? What results?
3. Describe work sampling techniques applicable to this area by safety department.
4. Is the safety program description and data up to date? What features should have prevented this accident? Why didn't they work? Had their effectiveness been tested or verified?
5. When was the safety budget last altered? Direction and percentage? What is growth in totalable safety expenditures in the last five years? How does safety budget compare with the growth of organization?

Safety program audits could easily be discussed in Part IX, Safety Program Review, but it seems better to deal with this aspect while monitoring concepts are fresh in our minds.

Data Reduction and Analysis.

Early in the study it became very apparent that data reduction, and analysis and interpretation were neglected functions. Managers were deluged with raw data. If each report was to generate an individual fix, the top manager would have no time to manage. There are situations where action is based on a single report (serious cases or to set an example), but the kinds of fundamental fixes needed are more likely to result from numbers of cases, careful diagnosis and study, and a plan which enhances system operation, rather than producing continuous perturbations of the system by rapidly changing emphases.

Past data were largely unclassified for diagnostic purposes, and lacked adequate trend and rate measures.

Two positive examples of assessment can be cited:

1. The error reported was 7 missed readings of a pressure gauge. The base was 24 required readings (3 per day for 8 days). Therefore, the error rate was 32%, or reliability could be stated as .68, a sharp contrast to the several 9's reliability of many reactor components.

2. Two checks of Warning Tags at ROD showed:

	<u>Number checked</u>	<u>Number Deficient</u>	<u>Error Rate</u>
8-11-70	108	34	31%
3-19-71	231	38	16%

A significant drop in error rate is shown.

Further, the 1971 data showed locations as follows:

at ATR	1%
at ETR	27%
other	33%

The RDT Standard for Quality Assurance sets an impossibly high standard for common deviations, that is, "preclude repetition." However, the standard goes on to say, "Quality trends shall be analyzed to furnish a basis for improvement in work performance," and this is an eminently sound guideline.

An analytic function is needed in the Safety Division (so that its products are processed for management use) and in the operation manager's office to digest and interpret internal as well as external data.

A related need is the kind of information center which could make relevant past error data available to planners in usable form.

Health Monitoring.

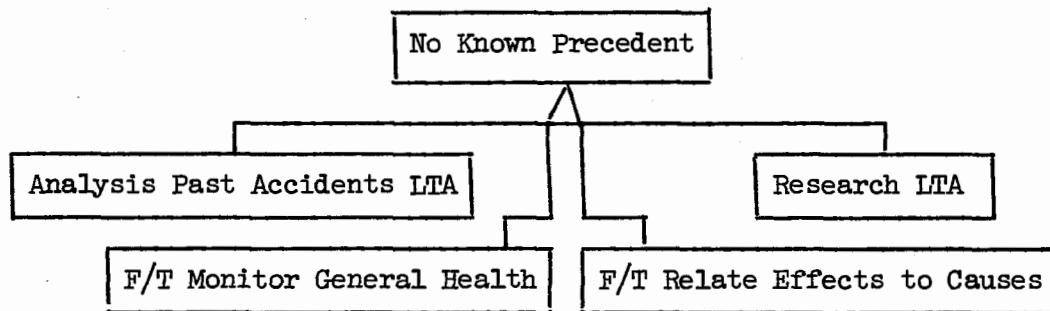
The need for surveillance of general health of employees in order to detect possibly job-related developments was discussed in Congressional Committees during passage of the Occupational Health and Safety Act. The need for such monitoring was also voiced by a group of British safety directors during a seminar on MORT techniques.

Potential general health problems are not readily related to the types of trauma-producing events diagrammed in the MORT analyses. However, since the need for surveillance of health seems clear, an analysis can be arbitrarily inserted at an appropriate point in MORT.

First, let it be said that certain types of health problems are already covered:

1. Exposure to radiation and toxic substances is already susceptible to MORT analysis.
2. General environmental conditions (noise, heat, cold, or any others) which have been shown to be related to injury or disease can be handled as "Environment LTA" in the MORT analysis.

Therefore, general health results of an unsuspected nature can be treated as an information problem in which there is "no known precedent."



38. ACCIDENT INVESTIGATION

In this chapter we shall deal with the investigation, analysis and reporting of the single event, or occasionally, a group of related events. (Cause analysis in a statistical sense is treated under information systems.)

The purpose of investigation is to guide and stimulate preventive actions by the line and staff organization. The emphasis should be on discovering all cause-effect relationships from which practical corrective remedial action can be derived.

The intent is not to place blame--all people err--but to determine how responsibilities may be clarified and supported and errors reduced. Pride, sensitivity and protective actions are nevertheless inhibiting forces. An analytic format which requires objective review of appropriate topics has proven valuable in counteracting such forces.

Collateral purposes of investigation may be for law enforcement or for evaluating legal liabilities. However, investigation solely for such purposes is seldom adequate for preventive purposes.

Also, investigation can be looked upon as answering public and professional curiosity in a "need to know" sense.

Although safety literature is replete with references to the value and importance of accident investigation and analysis, there is an alarming and startling lack of text material on methodology. One text placed great emphasis on "getting the important facts," and then discussed tabulations with an introductory phrase, "Now that you have the important facts." The ANSI Method, Z 16.2 (1962) is so weak in causal concepts as to provide little of practical value, and much that may be misleading, even bad guidance in investigation. Even a focus on mass data at a time when the "state of the art" is so ill-defined may lead to a false conclusion that valid and useful data (i.e., adequate to design countermeasures) have been collected.

The analytic format of MORT, or at least the style of analysis, provides one point of departure. To the extent MORT concepts permeate the preventive program, understanding will permit at least modified MORT approaches to investigation of less serious events.

AEC reports of in-depth, board investigations provide a standard of excellence. The extensions of analysis of these events by MORT has been possible only because the initial investigations were very good.

Other examples of detailed analysis will be found in National Transportation Safety Board Reports (see particularly the Waterloo, Nebraska school bus accident report and "A Systematic Approach to Pipeline Safety" for Tree types of analysis).

The NTSB has several attributes which should be understood:

1. Independence. The man who makes the regulations or manages the facilities should not investigate what may be "his" accident (i.e., his error).
2. Good procedures.
3. Competent, trained staff.

A Board representative said:

"A prime attribute of the Board is its typifying the check and balance system needed to review reports, determine causes, make recommendations, etc. with an absence or minimum of bias (except perhaps towards safety). Should investigation results fundamentally funnel up to one man, the outcome might well be weighted in one direction--actually favorable or unfavorable to his office. Some people have been observed to be too critical of themselves as well as not critical enough."

The Board's reports provide excellent examples of investigative and analytic techniques, but these are, quite understandably, obscured in the specific content of the event the Board is analyzing; thus principle or method of analysis are not always apparent. The Board has been urged to develop principles and methods for wider application in transportation fields and for training, and has these intentions, but budget inadequacies have largely stifled progress in this respect. The legislative history of the Board and its predecessor show strong Congressional recognition of the essentiality of independence.

Air accident investigations are the only available examples of mass procedures keyed to adequate concepts. However, even these have weaknesses stemming in part from legal requirements (e.g., find probable cause), and have major, positive (but largely unstated) premises--that is, intensive and exhaustive system safety analysis prior to accidents and research as needed after accidents--which could mislead the casual observer as to the nature of investigation and analysis requirements for topics other than air, particularly the role of a high ideal of system safety might not be visible.

Disaster reports available from other fields of activity are highly variable. Even those which are generally good (such as NFPA) have a tendency to become silent as they approach the borders of managerial responsibility--planning errors, mostly omissions, and decision criteria and mechanisms.

Various accident reporting forms provide, in effect, analytical frameworks. However, these are, in general, so simplistic as to give no great guidance to analysis of serious events. In general, forms may be barely adequate in the "What Happened" phase if the narrative is well done, but less than adequate for other phases such as "Why It Happened" and successive causal layers.

The possible exception is the Department of the Interior reporting system (Pope, 1970) which provides for examination of successive layers of causation in terms of actions needed by higher supervision, management, personnel, finance, and other support services. This form begins to examine the "Why" aspect. If it is possible for a single, simple form to collect adequate facts, the Interior form is unquestionably a step in the right analytic direction. However, it is unlikely that the successive endorsements as to causal factors will be searching unless an analytic method is prescribed, and systems analysis is likely to be weak or absent.

The NSC and Federal occupational accident forms are intended to provoke analysis, but in fact tend to produce barely adequate information on what happened, and simplistic, inadequate information on why the system failed. For example, although the role of management and supervision are said to be primary, a reading of thousands of such reports shows only rare analysis of supervisory errors or actions, and complete silence on management system deficiencies or errors.

There is need for manuals for investigating occupational accidents. Bradley (1967) discussed the deficiency in the Air Force (but used traffic accidents to develop a draft approach).

Braunstein and Coleman (1967) said:

"Accident investigation may be considered a member of a large class of problem-solving tasks which require extensive experience for the development of expertise. A characteristic of this class of tasks is a marked difficulty in conveying the fruits of such expertise to the novice and thus avoiding the need for a duplication of this experience. In addition to the practical problem of training new 'experts,' the inability of persons to describe the manner in which they perform such tasks makes it difficult to develop a general understanding of this type of behavior and to augment the human performer with artificial intelligence devices."

On many occasions, when pressed for description of accident investigation technique, very competent safety engineers have ended by saying, "I guess you just follow your nose."

Causal Factors.

This discussion is predicated on the presence of a number of causal factors, rather than the finding of "probable cause" (singular) which is the stated objective of several Federal safety laws and tends to be an obstacle to proper analysis (Johnson, 1967).

A good investigation of an accident/incident in a complex system will commonly reveal on the order of 25 specific errors and omissions and 15 systemic failures--a truly shocking situation. If adequate medical or psycho-

logical expertise were used, the numbers would be even larger.

But after the initial shock, pain, anger, frustration and humiliation occasioned by such findings have abated somewhat, it is helpful and useful to remember:

1. Well-run systems foster precise identification of more errors because definitions and tolerances are stated.
2. Complex systems (including working people themselves) have many error opportunities, and even low error rates produce many deviations.
3. The large number of causal factors revealed are correction opportunities--fixing any one will usually interrupt the sequence and prevent the accident.
4. Fixing systemic failures will prevent many future errors and accidents.

Investigation, Analysis and Expertise.

The process of investigation can be seen as a mutually supporting triangle of competencies:

Investigation--definition, description, detection--fact collection.

Analysis--fact interpretation and arrangement based on accident concepts, essentially safety analysis. But, most important, what kinds of facts to seek.

Expertise--the technology involved in the event--what facts may be, energy and operating patterns, and technical action possible or feasible.

All three of these competencies are present in an individual, but usually the higher levels of each competence are found in different people. Only the combination of the competencies can create a disciplined investigation--the greater the joint competencies, the greater the discipline.

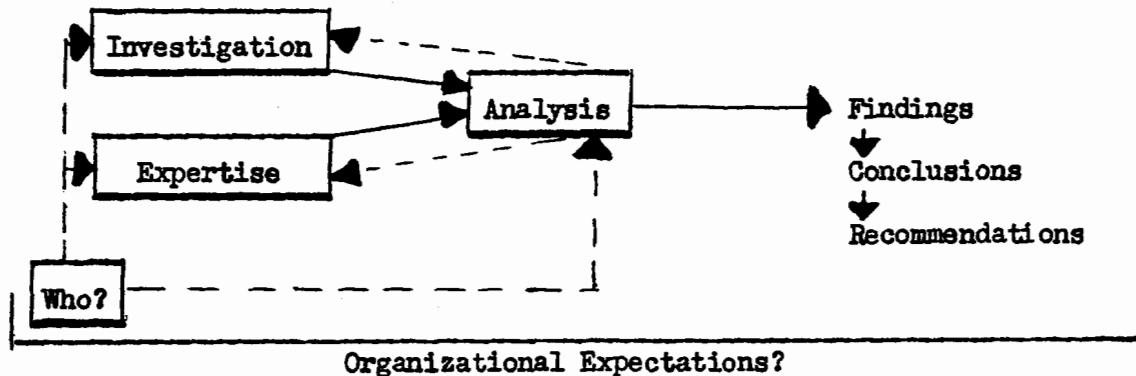
In a time sequence, investigation will precede analysis; but the process is iterative. Analysis requirements, if known to the investigator, will help him in knowing which facts may be relevant and needed, so analysis will be discussed first. Analysis is a form of "independent review" of the investigator.

The three facets are depicted (Figure 38-1) along with the variables in who investigates or analyzes, his competence and independence, and the factor of organizational expectations. AEC, for example, has high standards as to the quality of investigation it expects, and this prompts thoroughness, searching inquiry, depth analysis, and verification of hypotheses where possible. A manual for investigations would further enhance the process.

Costs of Investigation.

The costs of high quality investigations can be considerable, particularly if multi-disciplinary teams or boards are used, or if research is

Figure 38-1. Investigation-Analyses-Report Process



needed to find cause, but the efforts seem warranted for serious events, especially when systemic failures are revealed.

The costs of using well-designed analytic techniques are not great, and in part offset any lack of multi-discipline resources.

The time required for analytic review of accidents by MORT (or by the Kepner-Tregoe process) gives inexperienced people concern. In one serious case, MORT analysis took $1\frac{1}{2}$ hours preliminary, 1 hour discussion and review, and $1\frac{1}{2}$ hours meticulous, a total of 4 hours. The Kepner-Tregoe process for the two grizzly bear accidents took about five hours. In less severe accidents a quick MORT analysis was completed in 20 minutes per case for six cases. These costs are small compared with other investments in the investigation.

MORT analysis costs less than a mass data program, and only a few MORT cases are needed to clarify substantial program improvement needs, data not available from mass tabulations.

Scaling of investigative effort is a requirement, and will generally be on "seriousness," but this in turn has several considerations other than severity (damages to people and property), such as mission impact, public or other sensitivity, public involvement, and who is involved, or novelty (new problem) or recurrence (old problem needs thorough "look-see").

Discussion of investigation will be premised on serious events, with full understanding that minor events use less effort, and full data needs will be met by sampling with short, supplementary reports, critical incident studies, etc.

Examination of the values from good AEC investigations or MORT analyses suggests that more useful information, particularly systemic needs, will be obtained from a few good investigations than from large numbers of marginal or superficial investigations. Thus the cost question is more nearly a question of the manner of distributing available resources. Certainly some in-depth investigations should be conducted in any organization of more than

moderate size.

What Should be Investigated?

Every accident or incident should be investigated. In practice, this means every injury, fire and motor vehicle accident, no matter how slight, property damage above \$50, and any "high potential" incident.

A typical injury-scaling mechanism is:

Type	Investigated by:	Reviewed by:
First aid and medical	Supervisor	Safety Middle management
Disabling	Supervision & Safety	Middle management Plant management
More serious	Middle management, Safety, and/or a Board	Plant management Top management

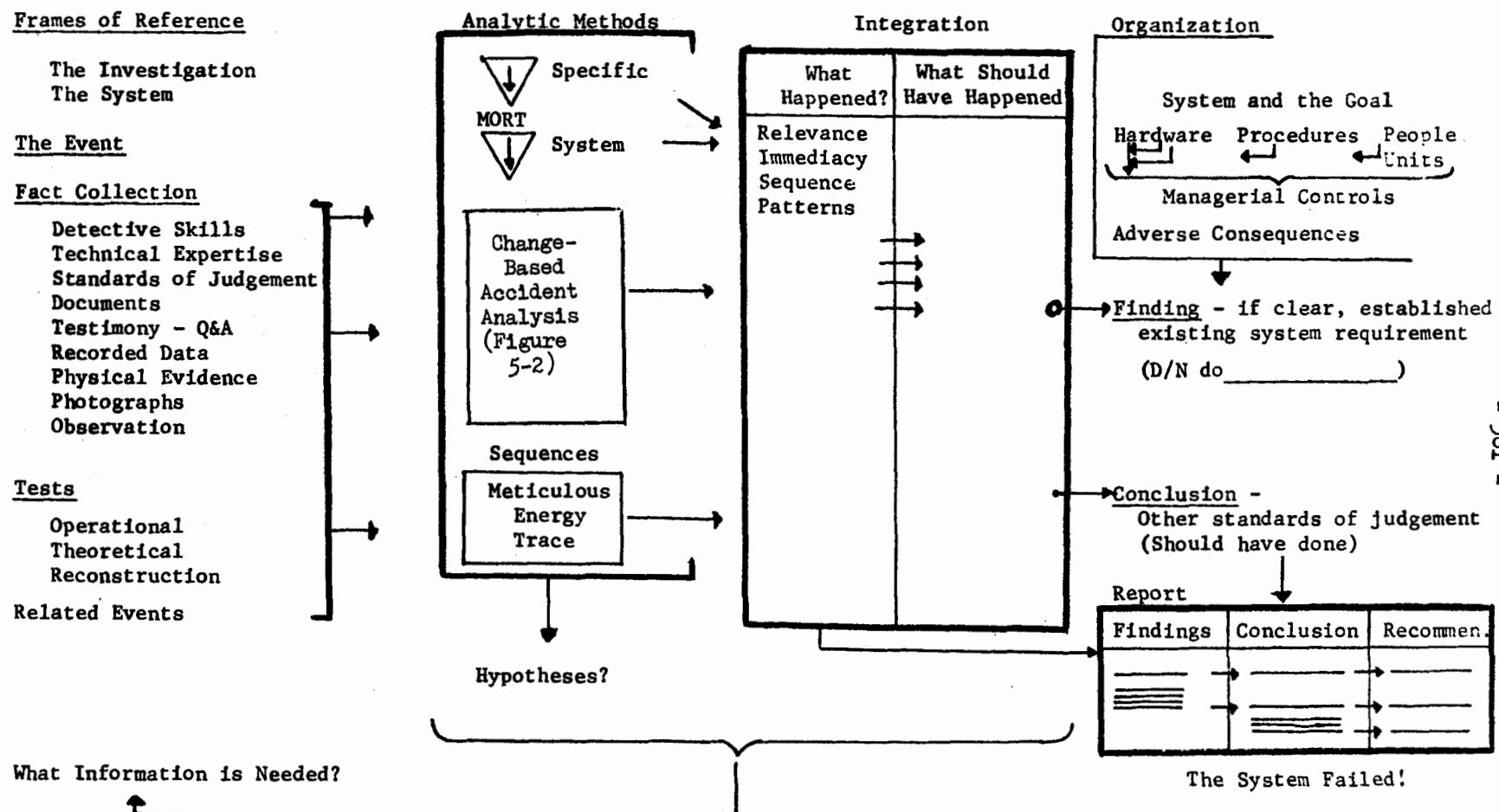
For incidents, dependent on the potential, the same scaling takes place. Some extremely valuable results have come from full-scale board investigations of incidents in which there was no damage or injury.

The Analysis Process.

In order to provide help to an AEC Board whose members had great expertise in the technology involved, but little experience (as is normal) in accident analysis, a schematic (Figure 38-2) was developed to provide an explicit logic and technique for reducing a large volume of material to a concise and precise report in the AEC format: Findings, Conclusions, Recommendations.

1. The frame of reference for the investigation and the system which failed should be established (manuals, directives, authority, organization, etc.).
2. The event is briefly described in a preliminary way.
3. Then sources of facts are depicted in a general way.
4. The facts from various sources are constantly being organized by at least three analytic methods:
 - a. MORT (shown inverted to place final events near bottoms of sequences),
 - b. Change-Based Accident Analysis Worksheet (Figure 5-2),
 - c. Sequences--most especially the meticulous energy trace.
5. Note particularly that the analytic methods in turn generate hypotheses and thus provide ideas as to what information is needed--an iterative process.

Figure 38-2. Accident Analysis Schematic



6. The analytic methods then provide raw material for integration into sequences and patterns as to What Happened? and What Should Have Happened?
7. The conversion of the above two sequences to findings and conclusions is handled in the following manner:
 - a. What Happened = Findings
 - b. What Should Have Happened:
 - (1) Can be a Finding if there was a clear, established existing system requirement, in which case a typical format would be D/N do _____. (At Aerojet a failure to obtain the required independent review would be an example.)
 - (2) All else is Conclusion--that is, standards of judgment as to what should have happened are not "clear, established existing system requirements."

A difficult situation is posed by accidents in which causal sequences are obscure. If a board of investigators is scientifically oriented, and evidence supports a fact "beyond a reasonable doubt," the board members should probably have the latitude to submit a "finding." On the other hand, if doubt exists, or if a finding is more nearly a group conclusion, such should probably be reported as a conclusion. In any event, the articulation, use and reporting of guidelines will contribute to searching analysis and avoid any real confusion as to standards of judgment used in preparing a report.

8. Organization of the material can be developed from the schematic in the upper right corner of Figure 38-2, and will typically consist of:
 - a. A statement of the system (or subsystem) and its goal.
 - b. One or more sequences showing the development of the hardware involved.
 - c. The sequence by which procedures were developed and applied.
 - d. The sequences involving people--operators and supervisors--and organizational units.
 - e. The managerial controls--those applicable, the sequences of loss of control, and the improvements needed. This would include failures of monitoring processes to detect evolving changes, errors, or hazards.
 - f. Finally, the adverse consequence--injury, damage, performance degradation, and program impact.
9. Report. The findings must support the conclusions, and the conclusions support the recommendations. This may be a 1-1-1 relationship, or >1-1-1 basis, or general conclusions may stem from prior conclusions,

and in turn support one or more recommendations. It seems desirable to assure this tracking on a single large worksheet (even though AEC's final report format provides that Findings are in Volume I and Conclusions and Recommendations in Volume II).

10. Note the schematic shows a general conclusion--The System Failed!

The immediate purpose is to allay the concern of investigators that their results will be used to place blame or as a basis for discipline. The note also helps top management's awareness that it was their system, not people, who failed (in most cases).

MORT Analysis.

Although MORT has shown itself to be a powerful analytic tool in the hands of a few analysts, it has not "caught on like wildfire." This has raised questions as to how it can be introduced and assimilated, and how training could be conducted. If not widely usable, MORT would not be of great practical significance.

The MORT diagrams, while intended to guide rigorous final analysis, are quite usable as "scratch pads" for notes of relevant factors. In turn, they suggest many questions to be asked. Naturally, the more one knows about the analysis, the better the questions.

One technique which has been used in several cases is described in "Getting Started" on page 23. In one serious and complex accident, a bright, young fire prevention engineer used this technique. At the end of three working days, he had the following results (over and above other Board and regular tasks):

44	likely problems
38	"don't knows"
<hr/>	
82	total

The number is large because of redundancy in lines of inquiry and redundancy in specific and system faults. The number of problems will likely reduce to on the order of 25 specific and 15 systemic faults, a typical "par" for a good MORT analysis. The engineer also had a good grasp of the information needed to resolve questions, and already had collected much of it. This work was performed after only 30 minutes briefing, and a short, later meeting to supply definitions not clear in the text.

Paul Hernandez, the head of the Mechanical Engineering Department at Lawrence, expressed the view that the MORT diagrams would have greatly reduced the cost of the national board which investigated the Cambridge bubble chamber explosion and fire by guiding the board's work and reducing confusion over analytic processes.

At present the two wall charts developed for use at Aerojet are excellent "analytic scratch pads" for use during an analysis. Analysts initially seem to suffer from paralysis of the wrist, so we urge them to start marking up a sheet.

The question of whether or not to draw a special MORT Tree to portray an accident (as in MORT Appendix A), or to simply attach a marked up copy as an exhibit for the review agency, or do both, is judgmental. The value in drawing a special tree is an explicit portrayal of relevant causal factors. The value in the marked up general tree is that the review agency can review a visible record of the analytic process, including the factors found satisfactory or deemed not applicable.

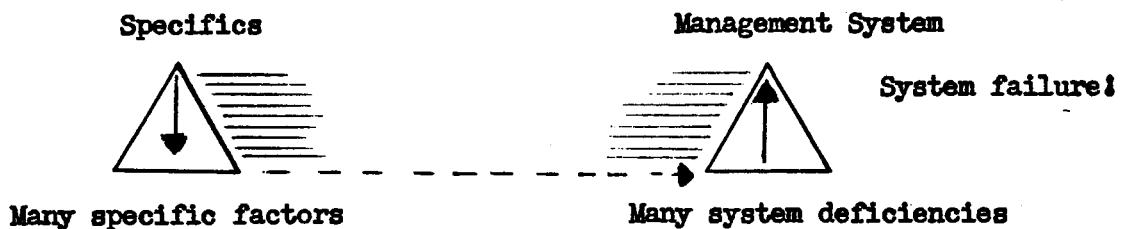
One major effect of the MORT analysis, widely noted at Aerojet, is to open the management system to authorized, even required, analysis. Prior to MORT, the analytic process stopped short, as it presently does most places.

In investigations, it is quite common to find errors or faults which are serious, and should be recorded and corrected, but were not part of the causal sequences. For example, a procedure may have been adequate, although it did not have the prescribed review. For these, a special symbol is shown in the tree:



It has been said that the quality of a fault tree hazard analysis can be judged by the number of layers in the tree. The same can be said of MORT analyses of accidents. An experienced NASA investigator described the analytic process as "peeling off layers as in an onion." If this metaphor is used for the MORT tree the process would look like this:

Figure 38-3. MORT Causal Layer Schematic



MORT analysis also destroys the false logic whereby the apparent absence of system or hardware deficiencies in a superficial investigation so often leads to a conclusion of human failure. If the system has not been properly analyzed according to high standards, who can say anything truthful about the relative roles of system failures and personnel errors?

Sequences.

The MORT analyses in Appendix A (1 to 6) show that meticulous tracing of energy transfers and changes is very often useful, even necessary. At Aerojet, a number of accidents/incidents were of this character. The sequences usually do not emerge in sequential order. This suggests that the sequential notes may have to be redrafted in extended or corrected order during the investigation.

Two special virtues of the meticulous energy trace are:

1. Facilitate questioning and testing of hypotheses,
2. Facilitate use of the MORT barrier analysis to examine possible interruptions. Barrier analysis has produced tested methods of interrupting energy transfer as well in innovative and effective ways.

Although the listing of sequences is first an analytic tool, there may often be substantial value in putting a time-sequenced event diagram in the final report. In NTSB's Systematic Approach to Pipeline Safety (1972) such a chart of "events and causal factors" was used to show how system analysis could have identified hazards prior to the accident. Thirty-seven events and factors are concisely displayed.

Change-Based Analysis.

This methodology was discussed in the chapter, "Role of Change in Accidents," and a worksheet (Figure 5-2) was suggested.

Initially it was thought the change-based analysis need be used only when cause is obscure. But, in the early stages of investigation, who knows whether cause is obscure? Further, it is quite easy to rule up a 17"x23" sheet of paper and keep interim, cryptic note of facts in a potentially revealing pattern, and as a guide to what information to seek. In one analysis of two related accidents the technique revealed several potential factors which had not been checked out because the analytic worksheet had not been maintained as a current, working tool during the investigation.

Finally, in another accident, the change-based format proved to be a very concise method of displaying the causal factors and created a useful exhibit (Figure 5-1). The best advice is to use worksheet (Figure 5-2) on every serious accident.

Investigation Process.

This can be examined in terms of Who should investigate, and How.

Who involves questions of investigative skill and training, and degree of competence in the technological process involved.

It seems axiomatic that since line management is responsible, its basic right, as well as duty, to investigate cannot be abrogated. However, an

essential element in line investigative responsibility is a more searching review and endorsement at each level of higher supervision, on up as far as seriousness warrants carrying the case. This can go on to "What Else?" is seen as necessary by higher supervision.

The question outside line responsibility then becomes one of involving additional expertise (from safety or process people) and developing independent review by safety or others. In practice these two ingredients begin to be added at a low threshold--that is, the safety engineer usually screens first aid and other minor accident reports for HIPO's and begins to assist and review supervisory investigations.

As events progress toward the more serious, the AEC requirement for Boards of Investigation represents a present "best practice." The question of independence deserves further consideration. As events become more serious, representation from a field operations staff may be added, and if even more serious, from headquarters staff. But are these representatives independent, or are they part of the directing process? There is no simple, practical resolution of such a question. However, consideration (within budget) could be given to using more substantial representation from the physical, managerial and analytic technologies not involved in the process; in major events, the use of independent scientists and investigators should be considered. The problems of independent review were also discussed in terms of the MORT Hazard Analysis Process.

In one serious AEC accident, the Board included the supervisor of the man involved, the contractor's safety engineer, and the field office safety engineer. The field office engineer, himself, raised the question of "incest." Such a situation should probably be improved by added, more independent representation. However, another safeguard is to instruct the Board to, at least, use the MORT format. This precludes the avoidance of questions simply because they are sensitive or difficult. This again is the Method vs Content redundant safeguard on a process.

The Air Force has Board Members' manuals and guides which seems a valuable practice.

The great educational values of Board service suggest that Boards be used as frequently as budget and circumstances permit. Board members frequently express a recognition and determination to do things differently when they return to their jobs.

The use of interdisciplinary teams has usually been limited to research. However, the Air Force (Scott Air Force Base, 1967) developed in-house teams

drawing on competencies available to a large installation. Such a procedure should be examined for practicality at AEC sites, especially for serious accidents.

An obstacle to good analysis (or investigation) is the tendency to see violations of procedures, standards or laws as "cause." Such violations may be part cause, but the standard may be wrong or inadequate and other factors may be more important and actually more "causal." A standard is just that, a standard of judgment, but there will be other, perhaps more important, standards of judgment.

The persons who investigate or review need objectivity and open minds. They should not just verify a given hypothesis or theory, and should avoid premature conclusions. The trick is to get these attitudes!

How to investigate follows out the skills involved:

1. Advance plans
2. Detective work
3. Technical work
4. Analytic work.

Advance plans should be in state of readiness for catastrophic events. The act of planning will also establish scaled down requirements for lesser events. Rescue and prevention of additional trouble are first order requirements. All necessary support and communication facilities should be quickly available. The management of the process should be clearly established and exercised.

Detective skills include preservation of evidence, physically and by photography, and by logs, sketches, and maps. The search-out of clues and witnesses. Go-Look-Listen-Ask. Sensitivity to change is helpful. "Don't be surprised."

Analytic talents include using concepts of sequences, layers, analytic formats, as well as scope--man, machine, environment, management, and prevention--engineering, education and enforcement.

The technical team skills may be more difficult to acquire (particularly medical or psychological skills). Aircraft investigations use specialists in subsystems--power, structure, controls, human factors, etc., and are working within a highly defined system. However this could not be seen as different from other accident investigations, only more advanced--better!

The meticulous tracing of energy flow and control is a facet of aircraft investigation to be emulated.

A note on motor vehicle cause analysis was made in an earlier section, that is, classification of defensive driving practices by a review board.

Material on commercial vehicle accident investigation is available (NSC Manual, 1970). Northwestern University Traffic Institute has published extensive material on police and research investigation methods.

Accident investigation reports can be audited for internal consistency, that is, do any assignments of cause follow from the facts as stated. Also, if reports are poor, did higher supervision not recognize deficiencies, or not return reports for further work? Did higher supervision participate in investigation in any way? Other major audits of investigations are for analytic method--and assumptions verified, evidence.

Plans and Operational Readiness.

It is essential that plans for investigating serious accidents be in a state of operational readiness. There is little time to study investigative and analytic techniques when a serious accident occurs. This suggests that plans and procedures be carefully designed, and that practice on lesser events is needed to develop skills. In a large organization, a cadre of trained, experienced investigators should be available to assist field staff and local staff.

The investigation manual (whether a formal, special document or a less formal, loose leaf assemblage of pertinent directives, plans, procedures and checklists) should be immediately available. Duties of briefing Board or staff members on methodology, for example technical experts, should be assigned. Guidelines for the assemblage of appropriate competencies should be provided the group's appointing authority.

Channels of authority and communications should be established. If public accidents or public officials are involved, these should be specified with actions to be taken.

Each safety professional should have a well equipped kit of investigative tools at his desk (or in his car) (and one additional kit in his personal car if circumstances make it possible that he should respond quickly at a site other than his office). The kit includes such items as tape, flashlight, danger, warning and marking tags, stakes and sample bottles, camera (if no photographer is a part of the team), distinctive tape to mark off the investigative area, measuring devices appropriate to his specialty, sketch pad and clip board, forms for witness statements, various supplemental reports and checklists.

This type of investigative equipment is not related to the ameliorative services--fire, rescue, emergency medical service--although under some cir-

cumstances the respondent has some duties in these areas. If appropriate, for example, his car may be equipped with fire extinguisher and/or first aid kit.

General Checklist for Investigations.

A generalized checklist was developed by Thune (1969) and included the following items (much abbreviated):

1. Remember--accidents are multi-factoral.
2. Go-clean up destroys evidence.
 - take photos
 - make notes of conditions
 - gather pieces, record locations, rubbings, scratches, piles of dirt may tell what was moving, which way, points of impact, and order in coming to rest.
3. Listen--for clues to sequence,
 - causes.
4. Study--the evidence,
 - ask Why?
 - seek proximate and distal factors.
5. Encourage--people who knew the process to volunteer ideas.
6. Confer--with experts.

He concludes with write up of report, and follow up.

A more detailed checklist can be developed from one of the Air Force Manuals (Air Force Military Airlift Command, 1966). With some adaptation to occupational systems and much deletion of aircraft detail, the list is provided as Appendix J. Appropriate detail should be inserted by any using organization (for example, a specific chemical plant would have very detailed checklists on its particular chemical possibilities). However, carrying out the intent of this checklist, despite some remaining aircraft flavor, would unquestionably produce an excellent investigation.

This page intentionally blank

39. THE ORGANIZATION'S INFORMATION SYSTEM

The MORT information system (page 343) and data flow model (Figure VIII-1) describe three kinds of inputs:

1. Technical Information,
2. Monitoring reports (those flow, use and fix cycles described will not be repeated in the system below),
3. Accident Investigations.

Considerable study has been given to data purposes and uses at research sites and elsewhere. In particular, uses of EDP coded information from routine accident reports in a variety of organizations was found to have few uses and those of marginal value, not warranting substantial investment without depth study and carefully planned usages. Consequently the primary focus points which developed were:

1. Simple key word coding of accident/incident reports and other documents, indices being easily merged by computer.
2. Action cycles to get data application.
3. Data reduction and analysis for functional purposes.
4. Management assessment of data.

Many key pieces of a comprehensive information system were placed in operation on at least a pilot basis, and at low cost. The system showed great promise of fulfilling criteria of relevance, timeliness, economy, accuracy, and flexibility.

Concepts.

At the conceptual stage, conclusions from earlier work were set down as follows:

The MORT diagram suggests that the information available to a decision-maker at the time of risk-acceptance is a critical aspect of a risk reduction system. Therefore, accidents/incidents should be analyzed as to the availability of known precedents and recommendations, and the reasons for non-communication and/or non-use.

It seems clear that conventional accident data files, as now constituted, provide very little information of decision value.

It seems equally clear that national and local data files are not utilizing available computer techniques to transmit available information to the point of need.

Although the first element in design of an improved information system is primarily conceptual, and can be exercised on a hand-tabulation level, the focus should be on national-local development of a computerized information system. There are important deficiencies in the national information system.

The broad project here conceived requires execution of a variety of local and national subprojects.

The safety professional must establish internal and external information networks adequate to his needs, and should test and exercise the networks systematically.

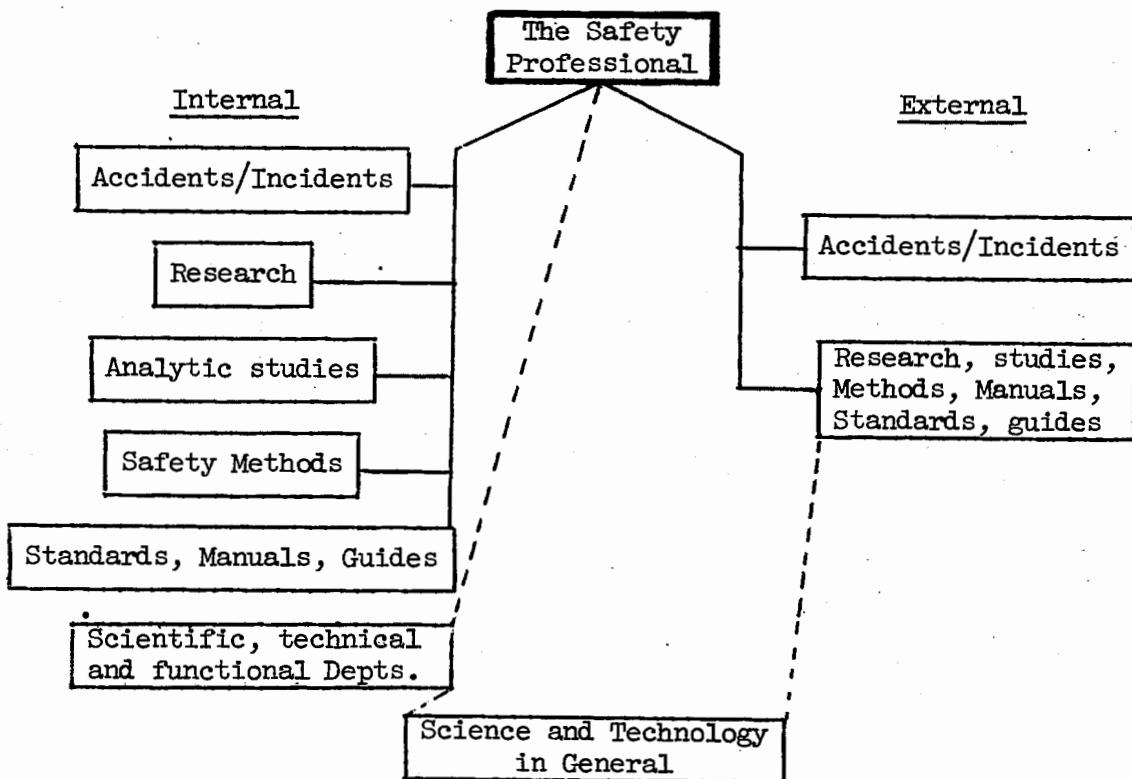
The network can be conceived in terms of kinds of information needed and internal and external sources.

Figure 39-1 indicates the obvious, direct responsibility for managing major internal sources:

1. The organization's accident-incident files.
2. The organization's direct research on significant questions.
3. Analytic studies of major problems.
4. The organization's methods and program
 - a. Standard operating plans
 - b. Committee, inspection and other inputs.
5. Standards, manuals, etc., used as internal guides.

The organization's scientific, technical and functional staff are seen as intermediate processors of the vast amount of literature relevant to the organization's work. The degree of formalization of these roles needed in the network can be determined by (a) the criticality of the problems, and (b) deliberately exercising the network on current problems, or retrospectively for accidents which occur.

Figure 39-1



The external sources needed include (1) rapid, effective channel(s) for information or known precedents in other organizations, and (2) general sources for safety research and technical information.

Conceptual Aspects of an Ideal Accident/Information System (Figure 39-2) has a central focus on operational responses. The genesis of this focus was the observed, widespread collection of data of dubious value, indicating the need to refocus on preventive value.

The second focus was on diagnostic leads for search out or follow up and response - an important use, but one which also contains the premise that statistical tables are seldom more than diagnostic, and that a requirement of easy retrieval of original reports is an essential sequel to diagnosis, if operational response is to be expected.

In the upper left section of Figure 39-2, the essentials of information on department, area or geography, function, activity, occupation, source (or agency of injury), and accident type are suggested to be individually useful, but more importantly, are useful insofar as they produce, in combination, "task specific" descriptions of error concentrations.

Identity of persons involved is also potentially relatable to personnel data already stored in computers from other files, but such inter-relationships are almost never explored or used in present EDP systems.

Proceeding counter-clockwise in the diagram, the matter of rates - that is, consequences and denominators - to get frequency and severity rates (incidence and impact) is identified.

Nature of injuries and part of body injured are objective data and valuable as diagnostic aids.

"Subjective Data" include particularly the ANSI code classifications of Hazardous Conditions and Unsafe Acts and such data have not been shown to be bases for operational responses. In the absence of MORT analysis, or its equivalent, many of the data on causes are most certainly WRONG, and dangerously misleading. (First discussed on page 56.)

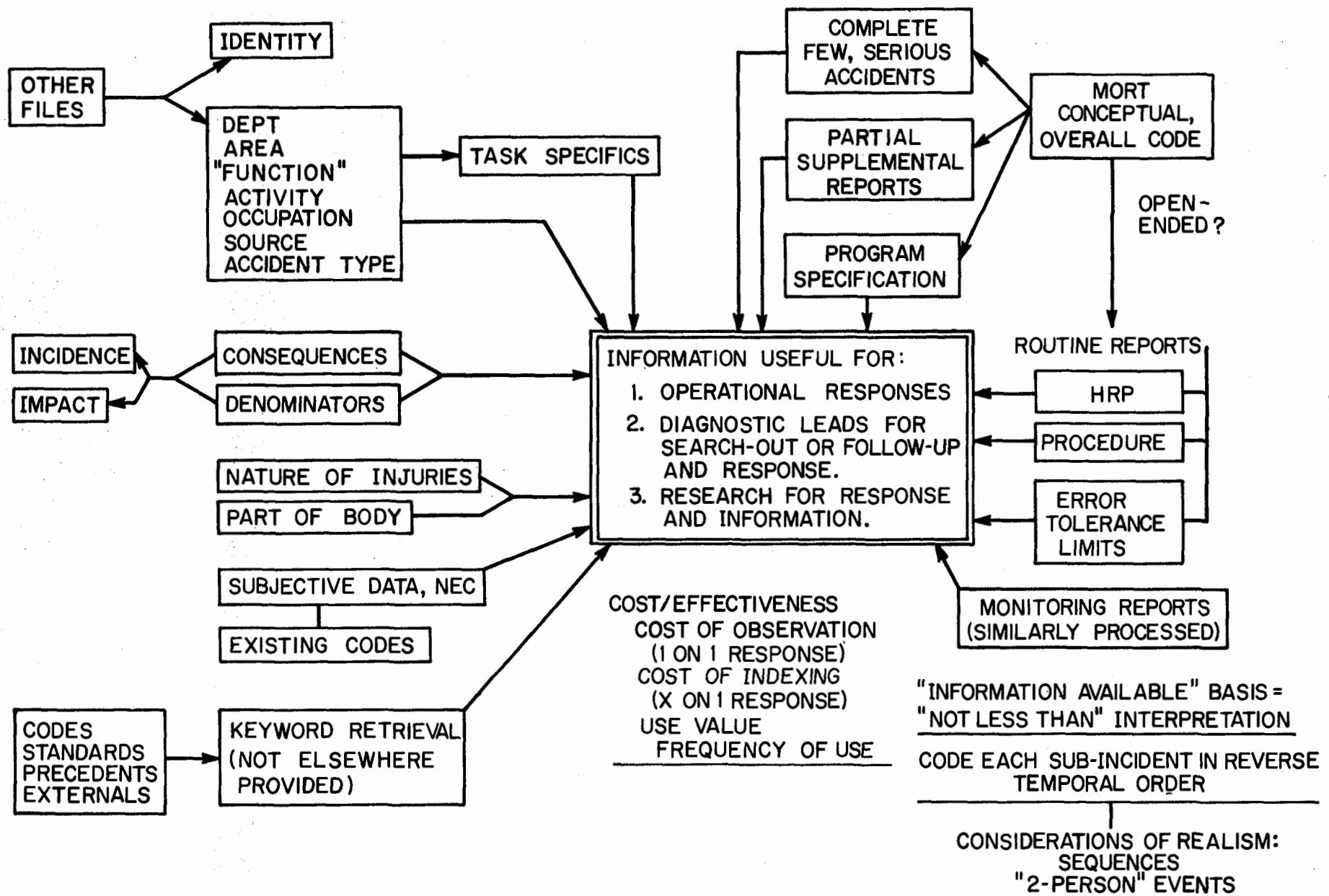
"Keyword Retrieval," that is, retrieval by subject matter, is shown as a need for codes, standards, etc., as well as accidents/incidents and error data. Later this was stated to be the primary, first requirement, since EDP-coded data of the ANSI type have little value, and practical, useful studies almost always return to original reports for "task specific" language and classifications.

Moving to the upper right quadrant, the MORT concept of analysis is shown as a primary aspect with four classes of outputs:

1. MORT analyses of a few serious accidents/incidents,
2. Supplemental reports on short-term samples of accidents which collect data on segments of MORT,
3. Program specification and measurement - in sufficient detail as to relate accidents to a program deficiency.
4. Routine reports - not a likely source of MORT type data - but worthy of experiment as sources of data on the quality of the Hazard Analysis

CONCEPTUAL ASPECTS OF AN IDEAL ACCIDENT/ INCIDENT INFORMATION SYSTEM

Figure 39-2.



Process (e.g., "not perceptible," "extemporaneous," or "oral" rather than documented), the presence and quality of procedures, and in the same vein, the error tolerance limits (Rigby).

Monitoring Reports are shown conceptually as being processed in the same way as accident/incident reports, and this introduces a major innovation, a major difference from present systems.

A variety of conceptual aspects are shown at the bottom of the schematic:

1. "Information available" basis. A major defect in some kinds of data (e.g., Hazardous Conditions or Performance Errors) is lack of sufficient investigation and/or analysis to render the data full and complete. Therefore, some potentially valuable data can be collected on an "as available" and "at least" basis - e.g., human factors review, proceduralization, etc.
2. Complexity of the accident is a real analytic and preventive problem. The possibility of EDP-coding of serious events as a series of incidents is here suggested for exploration.

Cost/Benefit aspects are then suggested. First, the cost of an observation can be assessed against the immediate preventive action, "one on one" response value. Costs of indexing, coding, and retrieval can, however, be assessed only against longer-term operational responses. If long-term responses are nil or do not use data and report retrieval, expenditures for coding and retrieval are wasted. Conversely, if data are not retrievable, long-term, effective responses (except for very serious accidents) are less practical.

A Basic System.

Key aspects of the basic system are expressed in Figure 39-3, which began to translate the foregoing considerations into operational terms.

A variety of Inputs was shown. A phase of Processing, Distribution, and Application in Fast Action Cycles is diagrammed.

In practice the Fast Action Cycles should be at least two:

1. Immediate oral transmission to the supervisor.
2. Rapid, written analysis to four addresses: Line manager, plus his technical staff, safety headquarters, and field.

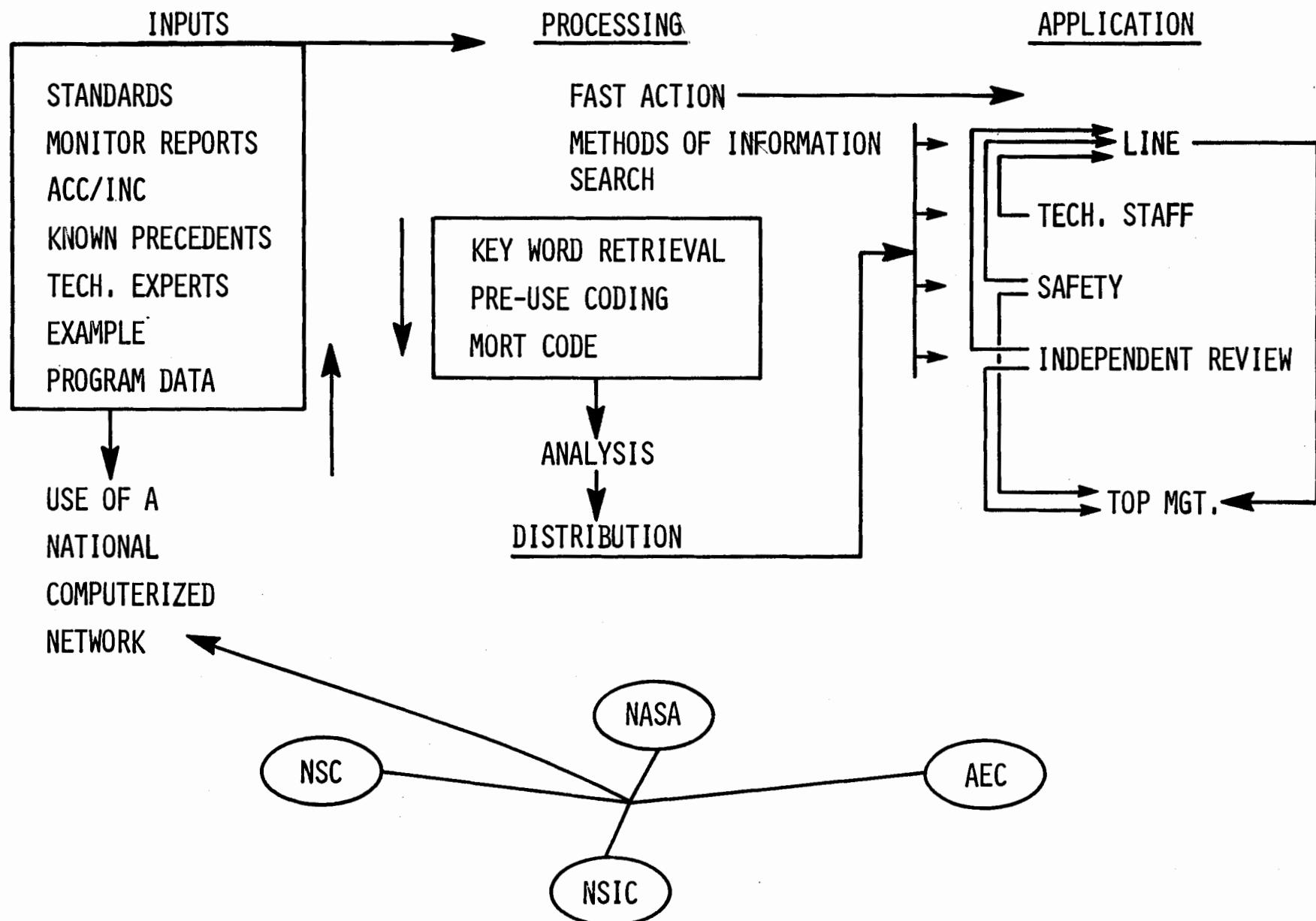
The second phase, Retrieval by Keyword List, is shown as the next major consideration, ranking ahead of purely statistical tabulations. Examples of specific information retrieval needs at Aerojet are easy to supply:

1. Cranes handling casks
2. Personnel working adjacent to canals
3. Removing in-pile tubes
4. Removing flux wires
5. Casks improperly labeled
6. Electrical lock outs (for complex systems)

These kinds of tasks and problems are not accurately or well identified in

Figure 39-3.

SAFETY INFORMATION SYSTEM



statistical types of categories. Also, retrieval of original reports is almost always needed for efficient and effective analysis.

Pre-use coding for statistical analysis is shown as a third requirement and is discussed below in some detail.

The Figure postulates an analytic process prior to distribution of data. Two reasons can be inferred from present experience at several locations:

1. Analysis is necessary if misinterpretation is to be minimized. In the same vein, interpretation and predictive values can be enhanced by competent analysis.
2. Raw data, undigested, is unlikely to be used by busy designers and managers, judging from past experience.

Distribution is shown as resulting from two processes:

1. User requests in terms of their projects and problems.
2. Automatic distributions originating in the information unit.

Application reflects the primary role of line management, but shows safeguards in the independent NOS and Review processes. Thus top management has redundant assurances of adequate application of information.

Uses of Operational Data.

Figure 39-4 cross-tabulates the principal Aerojet information inputs (accident/incident systems and monitoring systems) against the major kinds of uses of information. The inputs are defined in some detail in Chapter 37.

The principle kinds of uses are:

1. Summary Data - aggregates and rates, and trends thereof, plus presentations of such data as Shewhart control charts, and projective models (extreme value, matrices, and perhaps reliability models).
2. Statistical Diagnostic Data - circumstantial (rather than causal) to identify clusters of accidents or errors warranting further study and analysis. The most useful tables are likely to be two to four variable cross-classifications, e.g., by Occupation, Part of Body, Type of Accident, and Nature of Injury as a diagnostic aid.
3. One-on-one Preventive Action (immediate and subsequent) is shown as a use of every input. This use is so important as to warrant visible display in the table as a universal requirement and a planned, audit-able use.
4. Mass Data for Design or Intensive Study. Substantial data to be called out when a process or design is being developed or changed, and data for intensive study of problems identified by cases or diagnostic data are believed to be the second most important kind of use. These have

Figure 39-4.
Information Types and Uses

InPuts	Kinds of Uses				
	Summary Data, Projection & Control	One-on-one Statistical Diagnostic Data	Mass Data Preventive for Design (Imm&Sub)	Safety or Intensive Action	System Study Status
A. Accident/Incident Data					
1. Injury	x	x	x	x	x
a. OSHA	x				
b. Z16.2	x	x			
c. First aid	x	x			
2. Property Damage	x	(few)			
3. Fire		(few)	x		x
4. Radiation Exposure	x	(few)	x		x
5. Vehicle	x	x	x		x
6. HIPO			x		x
7. Other AEC defined			x		x
8. RDT Incidents	x	x	x		x
9. Supplemental		some	x		x
10. MORT (serious)			x	x	x
11. Other			x	x	x
B. Monitoring					
<u>Work Site</u>					
1. Management			x		x
2. In-house sample	x	possible	x	possible	x
3. Supervisor observ.	x	?	x	?	x
4. NOS field engr.			x	possible	x
5. H.P.monitors			x	possible	possible
6. Radiation badges	x		x		
7. Procedural surveil.	x	x	x	x	x
8. Spot checks			x	possible	x
9. File audits			x	possible	x
10. RSO Incidents			x	x	x
11. Technical Support			x		
<u>Upstream</u>					
12. Management			x		x
13. QA			x		x
14. NOS			x		x
<u>General</u>					
16. Higher Management			x		x
17. Q A	x	x	x	x	x
18. NOS			x		x
19. Management Control			x		x
20. Annual Review			x		x
21. AEC			x		x
22. Other and misc.			x		x

almost invariably used original, detailed reports, rather than summarized data.

5. Safety System Status. The safety system, as defined in MORT or corporate schematics, must be audited and measured. Such data will be a summation of information fragments, rather than comprehensive for all events.

Some inputs can give temporary or continuous data on segments of MORT - e.g., supplemental reports on proceduralization or hazard review, or inhouse staff samples of error rates. MORT, for a few serious accidents, may be complete. The larger number of inputs do, however, provide observations or evaluations of particular aspects or elements of MORT. The diverse character and coverage of inputs should not be permitted to obscure the need for a continuous and up-to-day assessment of the safety system status.

Figure 39-4 was prepared as a simplified analysis of inputs and kinds of uses. It will be immediately apparent that some inputs supply information for two kinds of uses, some for three uses, and some for four. No single source supplies data for all uses (Quality Assurance seems to be an exception, but is probably a substantial list of separable inputs, no one of which fills all needs).

The patterns which emerge in the Figure are interesting, and appear to provide insights for the organization and operation of the information system:

1. Control data sources total 12.

Shewhart control charts are to be prepared for organizational units. These should be based on total injuries, but as OSHA data accumulate, their value can be assessed. In order to accumulate data by organization (Division and Branch) present EDP coding must be adequate.

2. Only 5 sources seemed to present important mass statistical possibilities.

(EDP coding is discussed below.)

3. Every source is used in one-on-one action.

Review of all injury reports by the safety engineer and supervisor is required. However, such action is not usually reviewed up to the level of Division Manager, and such routing is suggested. Further, some record of "fixes" is required for summarization in the Division office. Similarly, the routing and action on each other kind of input should be carefully reviewed for adequacy.

4. Mass data study (which may be for only a few relevant cases) came from 13 sources, and possibly 5 others, supporting need for key-word retrieval.

5. Safety system status by 20 data sources, underscoring need for system schematics and other assessment methods.

Key Word Coding.

Several key-word coding systems of national centers were reviewed, but provided no simple plan for use by a smaller, local system. Several experiments in coding sample batches of reports of various types, and results helped provide simple coding protocols.

The system design which evolved was as follows:

1. Every report must be reviewed by a cognizant professional - but he cannot underline key words as he reviews, inconsistency and cost being primary obstacles.
2. Key-word coding must be done in the information unit, at first by a professional, later by a supervised, trained clerk.
3. User needs are likely to center on an activity, one or more sources, who is involved, and where.
4. Code only terms for which retrieval is likely for special study. (Add to vocabulary as deficiencies appear.)
5. Establish protocols for information search on selected topics, for example:
 - a. "Fire" or "Housekeeping" should utilize safety engineer's periodic reports, not coded in detail.
 - b. For a topic, e.g., "reactor top work," construct a list of sources likely to be involved.
6. Among "sensitive" categories (in addition to three examples listed above) the category of "reactor instruments" is to be coded by specific major systems (list them) and a sub-item, maintenance and repair.
7. Indexing must be done by a person (or a group) operating from a defined, consistent base .
8. Later, terms in the evolving vocabulary can be cross-indexed to the ANSI detailed source code (231 items) to produce a cross-reference to information items in EDP injury codes which might have been missed in key-word coding.

The system was initially applied to an RSO study (critical incidents). Coding time was not burdensome for an experienced analyst, because he was thoroughly reviewing reports for clusters or potential sequences. Data to be punched into cards was only: key word, major plant, location in plant, and an identifying report number. The computer print-out revealed clusters, and was immediately put to use in project design. A similar report, preexisting, for RDT incidents was also used. Thus two valuable data sources were put to increased use at low costs.

The potential for an incremental system whereby each data source is considered separately as a possible addition was analyzed for mobile and overhead

cranes. Twenty four sources were identified none of which could be overlooked in a comprehensive review of these accident sources.

The National Product Safety Commission had a procedure for routine daily indexing of incoming material which should be examined for interim applicability. This was a temporary study commission, yet a computerized system was operated with only a key punch in the commission and access to a GSA computer. Daily indexing of a minimal character was accomplished at lower cost than the customary typed cards, logs and endless document routing. A weekly print-out keeps everyone informed and should stimulate field office reports of relevant projects.

The excellent experience of the NCPS with a "dump print" index of its reports and communications strongly suggests that the safety system be expanded, increment by increment, continuously testing values in each increment.

The possible increments for addition to the system include:

1. Codes, standards, regulations and technical literature (as discussed in Chapter 36),
2. Internal policies and procedures (already indexed for one Division),
3. All accident-injury reports (supplementing EDP Codes),
4. Error and Hazard reports from whatever source,
5. Detailed Operating Procedures and Job Safety Analysis,
6. The source of the report, assignment for study (organization and person) and the location of problem need be coded in addition to the key word and document number.
7. Methods literature using MORT terms.

Group Cause Analysis and EDP Coding.

The flow chart for the risk reduction system postulates that Investigation reports are, or should be, adequate, and that they are being fully exploited for preventive changes as individual reports, particularly those showing high potential.

Our present concern is the cause analysis of groups of reports for prevention purposes. The results of such analyses will have their decision value as a primary criterion of worth. They should lead to specific preventive action, provide program guidance or point to the need for further studies. If one accident provokes some action, proper analysis of groups of reports should provoke greater action.

Cause analysis is, however, interlocked with questions of EDP coding. The small, special studies usually employ categories and methods appropriate to the problems under study. In any event, studies must be evaluated individually.

Cause analysis by EDP methods, usually standardized and simplistic, spits The small, special studies usually employ tailor-made categories and methods appropriate to the problems under study. (Catlin, Patterson and Phillips)

out numbers of impressive size. With standards (such as ANSI) and large numbers, what could be more plausible? And less useful? Unlikely as it may seem the quality of the data is often in inverse ratio to its quantity.

For some reasons we shall shortly show, we must distinguish two phases of use:

1. Preliminary Diagnosis - notions of where trouble, past, present and future, may lie; in other words, clues. From this phase (which includes much presently published data on causes) no published statements should issue - no statements implying, "Because , so"
2. Final Diagnosis - using special studies and tabulations, rate bases, on-the-spot surveys, task specific analysis, etc.

Given the distinction of these two phases it is possible to salvage much useful information from present EDP systems.

We can distinguish four major characteristics of various types of present data:

1. Objective - data on name, department, length of service, occupation, part of body injured and nature of injury. Also type of accident and source of injury are in considerable degree objective and useful.
2. Subjective - unsafe conditions, agencies producing them, and unsafe acts.
3. "Messed up" - using the injury as the unit event, and collecting data on the injured person rather than the error-committing persons or departments.
4. Misleading - using a single-cause concept, or a single condition plus single act concept.

Data on the first, "objective," category should be compiled by all organizations as statistical, diagnostic data. The ANSI method (Z16.2) is an excellent method, although some industries seem to have found that alterations increase usefulness for them.

The second class of data, "subjective," sometimes called cause codes, have all the last three faults listed above. Therefore a moratorium on further publication outside the using organization is strongly urged. Enough harm has been done, and will take years to correct.

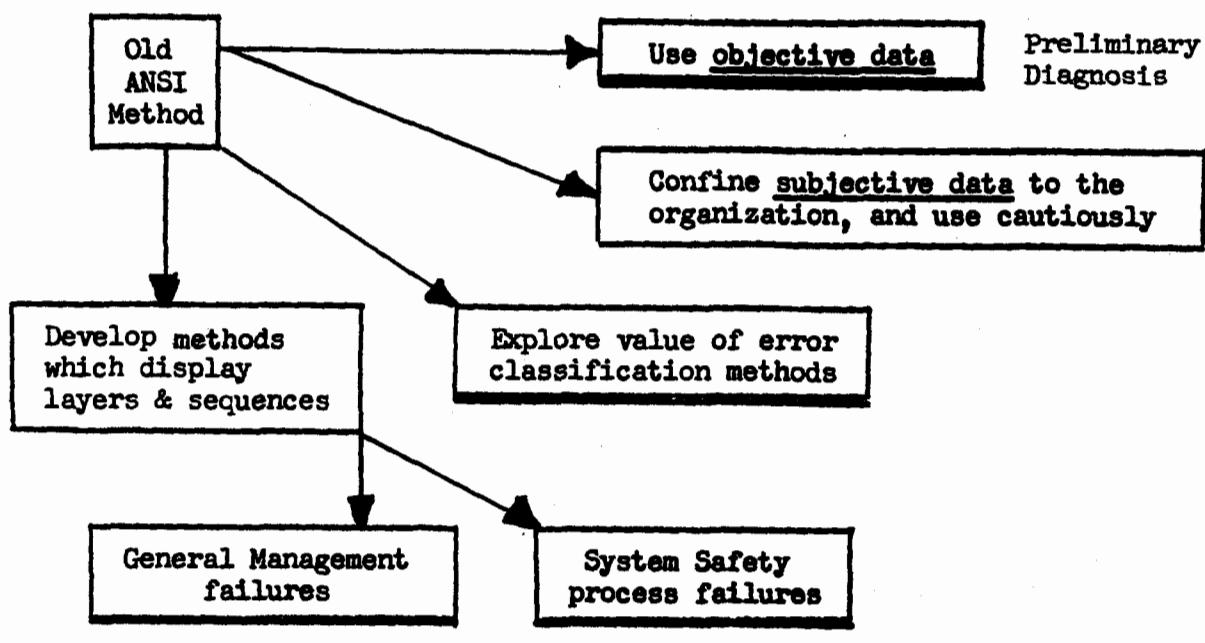
The development trends which can be visualized, and should be encouraged, are shown in Figure 39-5 on the next page.

Some general suggestions on routinely tabulating data by subproblems, rather than "all accidents" can then be given.

Also, problems in conducting studies for final diagnosis can be explored.

The use of computers can be valuable within the necessary qualification

Figure 39-5.



as to type of information computerized. Modern quick-access facilities can produce considerable data useful to field personnel - practical service to the field is a test of any computer set up. Valuable studies can be made by relating accident incidence data to other data stored in a large computer, especially personnel data.

All three research sites involved in the study have computerized accident data systems which follow, more or less, the ANSI method. Sandia's system could probably be called "best" of the three - occupation coding is excellent, activity coding is attempted, and research data (e.g., environmental weather data) are added to codes. A quick-access method is utilized. However, cross-tabulations useful in headquarters and field are only starting to be used. With a few slight reservations the Sandia system is as good as all but a few and far superior to most systems.

Fundamentally, the systems at any of the three sites produce little information of decision value, and the machine capacity at two of the sites is almost unused.

These problems stem from conceptual deficiencies at the national level, rather than from local deficiencies.

Examples of (1) the need to supplement coded cause data with additional observations, measurements, and experience, and (2) the type of study needed for low severity-high frequency topics are found in National Safety News, September 1972, for slips and falls.

Greenberg (1972) provides examples of useful diagnostic tables with simple computer routines to assess significance of minor/major injury ratios.

* * *

Present Objective Codings. The ANSI method is typical of some aspects of these data. The suggested cause-related codes include: Nature of Injury, Part of Body, Source of Injury - object, substance, exposure, or bodily motion which produced injury, and Accident Type - event which directly resulted in injury. (This latter classification may be improvable through use of energy concepts and hazard classification (Stein and Cochrane, 1967)). Source, as defined, is useful (but "Agency" requires a showing of unsafe condition which is subjective).

To these four objective ANSI codes are typically added, locally defined identification data such as name, department, occupation, length of service, area, etc. Such codes as occupation must be locally defined to be compatible with local records.

Activity (task) codes are sometimes used, and are useful if they are task-specific to the organization.

Severity, days lost, and cost data (with limited scope) are useful in evaluation and diagnosis.

Present Subjective Coding. Presumably earlier discussions in this paper have adequately explained deficiencies believed to exist in ANSI-type cause data. (See particularly page 56 and Chapters on Change, Sequences, and MORT Analysis.)

The incorrect information and fallacious concepts are perpetuated all around us.* Thus, the plea to Stop Now in propagandizing nonsense.

In fairness to the ANSI method, its preamble alludes to "general patterns of injury" and "guides to areas, conditions, and circumstances to which accident prevention efforts may be most profitably directed," which imply preliminary diagnosis. Further, among its purposes is ability to handle "mass data and take into account the wide variations in completeness and accuracy." But the sins committed in the name of the method remain - how can valid data be obtained from incomplete and inaccurate reports by using a conceptually weak and misleading method? Yet tables reporting compilations of xx,000 reports by an official agency have a surface plausibility, and are widely quoted by those with little understanding of the problem (or from inertia).

Among the best, if not the best, of the adaptations of the ANSI method, is the method used by Bethlehem Steel Company, especially as it is based on

* For a current example, see National Safety News, January 1971, p. 10.

a JSA-JIT-SO concept (see Appendix L).

The classifications are as follows:

<u>Category</u>	<u>Items</u>	<u>Code Capacity</u>
1. Man Cause	17	2
2. Man cause background	15	3
3. Environmental cause	17	2
4. Environmental cause background	17	3
5. Actions to prevent recurrence	<u>21</u>	<u>3</u>
Totals in <u>5</u> Dimensions	87	13

This is an admirable effort to reflect multifactorial concepts. Coupled with the use of intra-organization definitions and system, and a coding of JSA number and step, the method is proving most useful.

For comparison, the ANSI method would yield:

<u>Category</u>	<u>Items</u>	<u>Code Capacity</u>
1. Hazardous condition	47	1
2. Unsafe Act	<u>52</u>	<u>1</u>
Totals in <u>2</u> Dimensions	99	2

The number of dimensions used provides a check on internal consistency and validity, a point stressed by Bethlehem.

If any organization were to seek a method for use tomorrow, the Bethlehem code (or that of the U. S. Department of Interior) might be a good point of departure. And certainly no one should discard present coding until a better alternate is found. (Bethlehem forms and codes are in Appendix L.)

Originally it was hoped that a useful, valid cause coding applicable to all (or almost all) accidents could be developed from such sources as: (1) MORT, (2) Bethlehem Steel Company codes, (3) Sandia and Lawrence codes, and (4) ANSI methods. The attempts have, thus far, been unsuccessful. In numerous trials, coding clarity and definitions broke down due to lack of a stated Hazard Analysis Process in the original reports. Despite the fact that discrete, mutually exclusive categories may not be needed for preliminary analysis, so many compromises were made as to vitiate meaning and use.

Therefore, the primary needs seem to be development along lines indicated early in this section before anything like a uniform practice could be considered. It may be useful to have data on the characteristics of six major systems compiled during the study. See Figure 39-6.

Error Classification. Those who have studied errors find that the meaningful data usually involve numerous task-specific descriptions of acts.

The broad classes and types of errors described in the literature are seen

Figure 39-6.

Characteristics of EDP Codes

	NSC OSHA	ID	Sandia	ANSI	AT&T	Beth.St.
<u>Employee</u>						
Name	x+#	x	Number			
Soc. Sec. #	x		x		x	x
Age	x	x	Birthday		x	
Sex	x	x	x		x	
Occupation	16	x (?)	x			Pos.Title
Occupation Class			x		x	
Service - Total					x	x
- Occupation					x	Pos.Title
- Job					0	
Employer	x	x			x	
Area	Premises 3	x	x		x	x
Nature of Location	10				x	
Department	name		Org. #		3	3
<u>Accident/Incident</u>						
Class	OSHA 8	x	x		x	x
Medical Disposition		x				
Extent	OSHA 3					
Days Out	OSHA	0	x		Dates	x
Time Charges						
Costs			x			
	Term, Transf.					
Date	x	x	x		x	x
Day of Week		x				
Time	x	x				x
Time elapsed		x				
<u>Objective Data</u>						
Nature of Injury	12	ANSI 26	2x27	26	25	19
Part of Body	11	9	2x40	9-50	16	9
Source (Agency*)	Aoc 18	ANSI 49	2x44	49-231		3 digit
	Inj 18		+25 Veh			
Accident Type	15	ANSI 15	2x21	15-61	36	12
Activity	Task 11		2x36		43	JSA#(4 digit)**
	Activity 14		+16 Veh			& Step# 2 digit
Hours on Duty			x			
Weather and Solar			x			
<u>Subjective Data</u>						
Hazardous Condition				10-49	27	2x17
Unsafe Act			}	2x32	17-54	+3x17
					36	2x17
						+3x15
						3x21
<u>Preventive Action</u>						

*ANSI codes source, and "Agency" if a hazardous condition is reported for the source.

Others sometimes use term "agency" for source.

NB. Sandia and AT&T also provide additional motor vehicle codes.

**Assign # if no JSA and if one needed.

primarily as taxonomies for use in task-specific studies.

Despite these words of warning, several attempts were made during this study to use error classification, either alone or in combination with the concepts of unsafe act. The efforts thus far produced some interesting ideas, but nothing useful for "export." For example, the error matrix as adapted from Rook was applied to management errors - the results were provocative but mostly speculative. Error classifications, as well as unsafe act classification, founder on present ignorance of the underlying work situation. If a situation hasn't had good hazard analysis, the data seem either inaccurate or meaningless.

However, the effort to produce useful error classification methods seems worth pursuing. If a useable method can be found, it offers the hope of reporting safety conditions, from all kinds of reports, in common terms useful in other management problem areas.

A positive example of task-specific error lists useful in accident/incident reporting is the Reactor Operator Performance Checklist developed by American Institutes of Research (1968). Based on this type of concept, other task-specific studies of reactors have been made (Nertney, 1965).

As early as 1943, Grieve reported that ANSI cause code titles were useful only if each category was broken down into task-specific categories for a specific source of accident. At the same time such language eliminates much of the subjective judgment from which ANSI data suffer.

Swain (1970) has defined error rate data needs in terms which, in large part, preclude mass, standardized data systems. Rather he seeks uniform methods of reporting task-specific studies. For error studies his report suggests:

1. "A procedure for establishing a non-computerized, manual entry, interim human performance data bank,"
2. "Error rate as the basic criterion variable," and
3. "Questions whether the gains realized from automatic high speed data retrieval would be worth the added complexity .." and other associated problems.

Examining Causal Layers. This objective would presume to inquire into the management systems which produce accidents and errors. R. J. Nertney, human factors specialist at Aerojet, has the belief that minor error and accident data, while having marginal value as predictors of serious events, do have value in detecting the kinds of system deficiencies which can produce major events, and has shown case histories of minor events which cumulate into sequences.

Management System Failures. The U. S. Department of Interior's accident record system is predicated on successive review of accident reports to determine failures and problems by functional responsibility: supervision, higher supervision, personnel, supply and logistics, engineering, finance, and legal.

(Pope and Cresswell, 1965.) The Department has numerous illustrations of the value of its system. However, it is believed that this is only a first step in designing a system to approach system safety objectives, and that, without depth review, reports of human error and condition defects will tend to be subjective. It is noteworthy and commendable that the Interior forms attempt to identify a variety of management problems.

System Safety Failures. This paper is replete with illustrations of the kinds of data believed necessary. However, for any broad, standardized system, the information needs would center around a few key concepts:

1. Risk Assessment System,
2. Hazard Analysis Process, and a subclass, Life Cycle,
3. Safety Precedence Sequence.

This approach would lead, for example, to attempts to get objective data on the "Triggers" and "Information" available before and after an accident.

Since the system approaches to be used as measurement standards are generally under-developed, it has seemed that initial analysis might be focused on Procedures - a central point in the Hazard Analysis Process, and an aspect for which standardized and practical classifications are attainable. The text suggests how the quantity and quality of Procedures might be assessed. (Also, Catlin, 1969, provides a useful example.) If Procedures are a useful base point, analysis can then proceed in two directions:

1. Backward in the process to attempt to measure the elements of Hazard Analysis.
2. Forward in the process to attempt to measure supervisory coverage by the JSA-JIT-SO concept.

In this approach, the first step would be a transfer code or statement of equivalence between MORT concepts and the organization's operating safety program. The data are then tabulated by the organization's criteria.

An illustration could be found in Aerojet's Independent Review Program. In this case Aerojet exceeds MORT standards. Aerojet could easily tabulate at what phase accident situations slipped through its Independent Review process.

Routine studies. At one site a field safety engineer was preparing, by hand tally of first aid reports in his facility, a cross-classification of Occupation, Part of Body, and Nature of Injury. Such data were stored, unused, in the computer.

A drive to help and service people with presently usable data is warranted.

Many cross-tabulations of function-related and cause-related data can be found by exploratory studies. (Probably nothing of value will be found in one-variable tabulations. And voluminous print-outs without summaries are wasteful of time.)

Other Major Categories. Motor vehicle and fire accidents are other examples of types deserving special study. Their presence in other functional tables may provide more confusion than light. That is, cause-oriented data could set aside motor vehicle accidents for separate study.

Computers. "Garbage in, Garbage out" is a common phrase. But much data in computers is not garbage. A quick-access method, and a service-to-people, decision-oriented, imaginative analyst can develop considerable useful data.

Accident data are not being correlated with other data in the computer. Therefore, much potentially useful data is going unused. Two types of illustrations are in order:

1. Accident and occupation exposure data can be used to produce rates by occupation by simply using two separate computer tabulations.
2. Accidents and such data as transfers to new jobs can be tabulated in research-type programs to diagnose high accident rate situations. This may require special programs, probably on a one-time basis. Then accident type and circumstance data can be obtained by quick-access methods.

* * *

The NSC Symposium's Group III report (Appendix K) has short sections on Diagnosis and Decision-Making Potential, plus other useful suggestions.

* * *

The organization's information system does, of course, need an adequate national system (Chapter 40), good measurement techniques (Chapter 41) and management assessment methods (Chapter 42).

This page intentionally blank

40. NATIONAL INFORMATION SYSTEMS

The basic purposes and functions of a national system do not seem to differ from those of a local system, except in a few respects:

1. Fast action cycles are less important, but still necessary - for example, a flash bulletin on an emerging problem,
2. Information for operational decisions and application are still purposes,
3. Application at a local level is still primary, and this raises the question of speed, accuracy and relevance to local users,
4. Collation, translation, analysis and "state of the art" summaries should emerge from national centers (rather than long, long bibliographies),
5. Assessment for various types of national leadership or management is a function.

There are seemingly deficiencies in these services at all of the national information centers, in part because the centers are underused.

Information Networks. Scientific information is so broad and interrelated that the idea of networks of computerized systems has evolved.

The Highway Research Board of the National Academy of Sciences, and the National Safety Council have a two-element system now. Several contractors to the National Highway Safety Bureau have recommended expansion to three or more elements of concentration with full exchange.

The NSC, Highway Research Board, and selected universities are primary nodes in the traffic system.

NSC has the function of screening (1) behavioral, social, mathematical, engineering, and biomedical sciences; (2) academic, professional, industrial and government sources; (3) bulletins, proceedings, journals, books, and technical reports; (4) completed and in-progress research projects; for safety information, which also yields occupational information.

Thus it is not difficult to envisage a computerized occupational safety information network (Figure 40-1). Under such a concept, each center assumes primary responsibility for coverage of its area and utilizes other centers in their special areas. Functions most ready and relevant for network trials are:

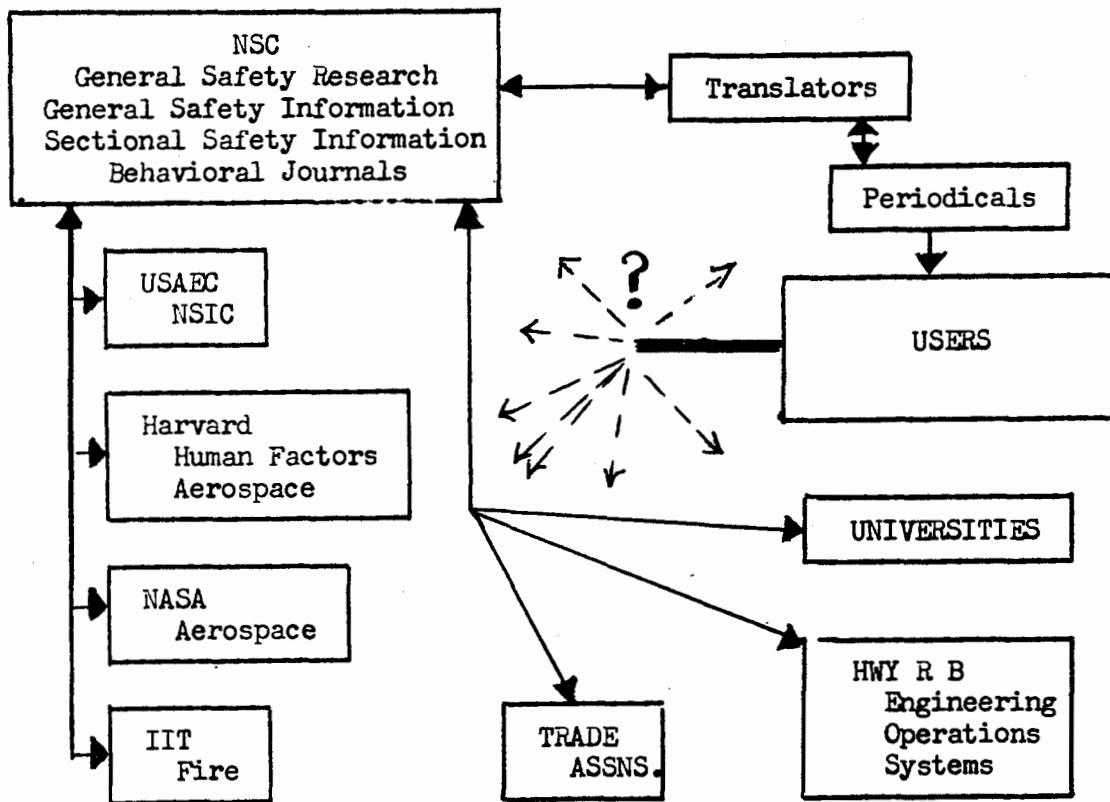
1. General occupational safety - NSC
2. Nuclear safety - NSIC
3. Aerospace - NASA

Initially, these three major centers should be organized into an efficient network giving fast and complete service in useful forms.

Other centers or nodes to be added are not hard to envisage:

4. Human factors and aerospace - Harvard

Figure 40-1.
A Possible Computerized Information Net



5. Fire - Illinois Institute of Technology

6. Aerospace and other - military centers, for example.

A major, chronic weakness is in the translation of findings into usable form. In a multi-layer organization, the headquarters has an intermediate service relationship to its branches. In general, the broad spectrum of scientific and technical information relevant to safety requires "state of the art" translation into usable form, and this is a function of both internal scientists who know the organization's problems and/or external agencies familiar with safety. State of the art papers have the important collateral function of reducing subsequent needs for reference to unwieldy, large numbers of references.

A growing number of pleas for better service and reports of progress are being published, for example:

1. Nuclear Safety, a journal.
2. Miller - The Safety Information Challenge. (1966)
3. System Safety - Progress Report on National Technical Information Center.
4. Montgomery - System Safety Information Exchange.
5. Pinkel - Data Requirements Analysis in Support of System Safety (1971)
6. McIntyre, et al - A Technique for the Acquisition, Storage and Retrieval

of System Safety Information (Air Force, 1970)

7. American Nuclear Society - Information Center on Nuclear Standards.

Both AEC and NASA have reported additional studies of information systems underway.

Measurement of effectiveness of existing networks, internal and external, should be determined by both study and conscious exercises. Initial trials of remote terminals linked with major information centers seem to be in order.

In the near future, on-line access to remote information banks will become routine. Experiments to develop safety-related experience are desirable. An experiment between an AEC site, NSC, and NSIC could provide useful, guidelines. (NSC does not now have on-line capacity, but should have it.)

In the interim, telephone or teletype could be used for regular dialogue.) Such an arrangement between NSIC and NSC should be explored. (NUCLEAR SAFETY, Vol. 7, contained some opinion on training procedures filtered to different audiences, safety organizations and other items which should be of general application.)

In MORT Trials at Aerojet, several trials of national centers produced mixed results - good and poor. Telephone exchanges were necessary to clarify needs. Undigested volumes of information were received. Despite these problems, much good information was produced.

Local organizations sorely need improved national services.

Thus, if an accident investigation brings to light accident information in the national network which would have been relevant to the accident, the fact and the causes of non-communication should be recorded.

This page intentionally blank

41. MEASUREMENT TECHNIQUES

Measurement techniques, specifically, Incidence Analysis brings us to the thicket in the jungle where the opponents and proponents of standard injury frequency rates and severity rates lurk. To avoid being jumped by the tigers, we shall approach very, very cautiously! However, after considerable hacking around in the jungle, it really doesn't seem that we can get where we must go from there. New roads are more promising.

Proceeding carefully, it seems wise to begin with where we want to go, and work backward.

In the opening section we stated purposes of measurement, one of which was to help managers assess residual risk. Incidence Analysis was shown to have three functions. Using the flow chart numbers (Figure VIII-1) they are:

12. Preventive - supply helpful information for program design and program evaluation.
13. Predictive - provide statistical information useful in assessing risk.
14. Comparative - provide information for inter-unit rankings or awards.

Preventive, the first of these, is rather easily disposed of for the moment. It consists of providing rates plural, generally moving toward the Error/Opportunity type of comparison, e.g., accident rates of personnel transferred to new jobs.

One of the facets of human factors review which specialists have emphasized is the identification of "error opportunities." In traditional safety effort, a new employee has been seen as an accident prone situation, or in the language of human factors, an "error opportunity."

In non-safety operating records, there should be at least a modest number of rate-base data, for example, new employees, transfers, changes in occupation or status (e.g., supervision), work orders in production or maintenance, etc.

As rapidly as such rate-base data are located and defined, the tabulation of comparable accident data should be instituted to derive rate numerators.

Pending explorations of easily obtained rates, it does not appear worthwhile to consider special, new rate-base data. But, if the first trials are encouraging, it may be worthwhile to consider other, and perhaps new rate-bases, e.g., new models of vehicles, machines, or other equipment. In such cases it would, of course, be necessary to collect data on former equipment as control data.

These rates or other indices are an aspect of Program Evaluation.

Comparison, the third of the purposes, is or should be of minor significance. Rankings are useful for only gross comparisons. (NSC Symposium Appen-

dix M. Also see Journal of Safety Research for symposium papers.) Awards are nice, but even good plans such as those of NSC and AEC do not qualify as relevant to risk of the major specific disasters and accident problems of an organization. Too often, award ceremonies are clouded by shortly subsequent disasters, and the award may have done a disservice.

The Predictive value of statistical data is our primary present concern. (Name-of-the-hazard, priority problem information comes from another source (flow items 19 and 20)).

During this study, and prior thereto, a wide variety of approaches and proposals for making standard and non-standard frequency and severity rates more meaningful to management have been examined, and some new approaches tried. But, for reasons which will be developed, the standard frequency and severity rates seem largely useless in predicting risk and should, for the moment, be forgotten. However, the ANSI injury definitions seem useful for predictive purposes when supplemented with other data and processes in ways different from the standard rates.

The five basic statistical methods of risk measurement and projection recommended are:

1. Aggregate Long-Term Totals,
2. Frequency-Severity Matrices,
3. Extreme Value Projections,
4. Rates and Probabilities,
5. Control Charts for Short-Term Fluctuations.

The first four methods constitute an approach to informing management of the seriousness and likelihood of long-term losses, including the worst likely potentials.

The fifth method is to test significance of short-term fluctuations, and has already been discussed in Chapter 37. Naturally, the control charts can be used for monthly, quarterly or annual data, and for plants as well as departments.

Aggregate Long-Term Totals.

The size of aggregate long-term losses and potentials, past and future, determine the need for and size of the safety effort. Illustrations in the form of life cycle estimates were shown in a table on page 264, but only for injuries.

The general goals of risk projection can be stated in terms of a summary table, Figure 41-1.

The general table constitutes a framework for collection of data in supporting tables and rates. The problems of estimation are not easy, but neither are they unduly difficult.

Figure 41-1.

Adverse Events	The Past Record			The Risks?	
	10 Years	Last Year	Next Year	10 Years	Likely Worst
<u>Occupational Injury</u>					
Deaths					
Disabling					
Total					
\$ Costs					
<u>Motor Vehicle</u>					
Number of Accidents					
\$ Costs					
<u>Fire</u>					
Number of Fires					
\$ Costs					
<u>Other Damage</u>					
Number of Accidents					
\$ Costs					
<u>Total \$ Costs</u>					

Adverse Events. The list can be expanded to include insurance costs (non-duplicative), off-the-job injuries, tornadoes, earthquakes, or other disasters, customer or public injury or liability, or any other events significant to the organization. The listed items are simply key items from supporting tables which will display other detail behind the estimates. Cost figures, particularly, require good footnotes, and two kinds of notes illustrate the problem, for example:

1. The first note on injury costs might say that Sandia's method of computing standard costs (direct and indirect) was used.
2. A second note might say (if management believes it) that the non-safety losses from oversights and errors similar to those in accidents are likely many times the loss figures shown.

The Past Record. This presumably is a straightforward listing, but if circumstances altered during the last ten years, the data may require definition or modification to make them a valid base for predicting risk. Past and future periods of twenty years should also be explored - the longer the period the less the statistical variability. The purpose is to combat the human tendency to remember the good years (awards) and forget the bad ones (disasters).

Some illustrations of needed supporting data follow.

Detailed Occupational Injury Data. The supporting table should ideally show in greatest detail the relevant categories in a continuum:

Death - multi-death
single death

Permanent Total Disability

Permanent Partial Disability:

Over 1,000 days charged)	
100-1,000 days charged)	data needed*
Under 100 days charged)	

Temporary Total Disability:

Over 100 days)	
10-100 days)	data needed*
1-10 days)	

Less severe:

Medical
First Aid

* The order-of-magnitude data on days charged are useful in constructing a matrix. However, if obtaining such past data is too laborious, the worst value (days charged to an accident, not an injury, can be easily determined for the last 20 years in order to make extreme value projections). (This same comment applies to motor vehicle, fire, and damage data discussed below.)

Cost. Conceptual weaknesses in injury cost data have been alluded to in this paper (see for example, page 176 and 256). However, the Sandia (1971) unit cost method has much to commend it, particularly ease of application to current reports. It includes standard costs, direct and indirect, revised annually. A method of making a gross adjustment for salary level and exact adjustment for length of disability is available.

With data of the above types it is believed possible that useful projections can be made by the estimating techniques presently available.

Detailed Motor Vehicle Data. There apparently are no data available on a fleet operator's losses by size, including his damages, and PD and PL losses (less recoveries). Data needed are believed to be:

Over \$100,000	\$100-1,000
\$10,000-100,000	\$10-100
\$1,000-10,000	Under \$10

Fire Losses. Both matrices and extreme value statistics show promising possibilities, and national background data may emerge when needs are known. Some findings are discussed later. The size categories for which numbers are needed are:

Over \$100,000,000 (theoretical, so far!)	\$10,000-100,000
\$10,000,000-100,000,000	\$1,000-10,000
\$1,000,000-10,000,000	\$100-1,000
\$100,000-1,000,000	\$10-100
	Under \$10

This type of order-of-magnitude classification should become standard for all

summaries or computerized data. Obviously the last, minor category of fire or damage may not be reliably tabulatable, although at closely controlled sites such as those of AEC it may be indicative.

The use of national fire experience to explore the predictive value of small fires for major fires should be a major exploration.

Other damage. Data and class limits similar to those shown for fires are needed.

One company, Lukens Steel, has made outstanding use of damage accident reports. However, the primary emphasis is on the preventive use of individual damage reports, rather than loss rates. On the premise that all accident reports provide important grist for the mill, the damage accident system is a considerable improvement when added to injury data. On a premise that management is cost-oriented, the measure is a valuable addition to management incentives.

A technique to be explored is the plotting of motor vehicle, fire and damage rates on the personal injury matrix. A common denominator for injuries and damage is needed, but seems to be no great problem for this type of exploration of the slopes of curves.

The Risks? Some ways and means of making predictions (rates, matrices, extreme value statistics, quality control charts, etc.) will be described, and others will undoubtedly come into being as the format is used. Both data and technology for risk prediction are now only fair, but knowing what is needed is usually a good half of the battle of acquisition.

The "worst" prospect column is intended to show management what the worst might be at a "95% level of confidence," as the statisticians say. This is sometimes defined as the "probable worst event."

Although "next year" projections may be mathematically the same as ten or twenty year projections, the next year data may be more reliable if derived as a 1/10 or 1/20 fraction of a long-term projection of serious events.

Exposures. The table might be augmented by three lines:

Employment

Property Value

Motor Vehicles (in use)

If these exposures undergo radical change from past to future, suitable adjustments or added footnotes would be needed. Presumably cost assumptions, e.g., "current year dollars" should be stated.

Reference Values. If an organization has proven incidence of adverse events at rates well below comparable organizations, it may be well to insert some reference values in the form of aggregate losses which would be incurred if

normal rates prevailed. The differences between predicted risks and general risk rates are the benefit which helps justify the safety expenditure.

Reference values can include three columns of projected aggregates based on:

1. U. S. average rates or probabilities,
2. "Good practice" rates or probabilities,
3. Organization goals.

The national "good practice," AEC experience, and the organization's data should approach one another.

The reference values could be shown as rates or probabilities, but it would be better to compute aggregates for exposures like those of the organization.

Frequency-Severity Matrices.

This management tool was initially described in Chapter 3.

Figure 41-2 shows the parallelism of Sandia and NSC chemical laboratories. Sandia had but one death in the period, but by chance (bad) shows a similarity to the broader experience. What is Sandia's long-term potential? Not different from NSC members generally? Thus, the background line seems to be a helpful aid to interpretation of rare event data. That is, it seems unlikely that an organization would have a long-term death potential sufficiently different to change the general shape of the curves.

Figure 41-3 shows the parallelism of AEC research and production contractor experience in successive five year periods.

Figure 41-4 shows some recently compiled data from AEC headquarters. Lab A had a five-year fatality experience similar to that of all AEC research for ten years. What is Lab B's apparent long-term potential with no five-year deaths? Likely to be similar? Or likely to be radically different?

Limits in the usefulness of matrices also appear in Figure 41-4 - that is, literal extrapolations may not be in order. Small differences in slope may give 2x or 3x differences in rate (but $\pm 10x$ not likely). Thus the advantages seem to be a visual, plausible projection of the order-of-magnitude of long-term risk and a tool in risk management emphasis.

What is the point? To keep management from being surprised, to be aware of risk. The exact time and place of a major accident will always be a surprise. But the probabilistic certainty of its occurrence should not be a surprise. As aforesaid, the impression is easily formed that management in plants with "good" rates for temporary totals are quite taken aback when the serious accidents occur. The background data were there, but the interpreta-

Numbers of Injuries by Severity
Sandia and U.S. Chemical Laboratories
1960-69

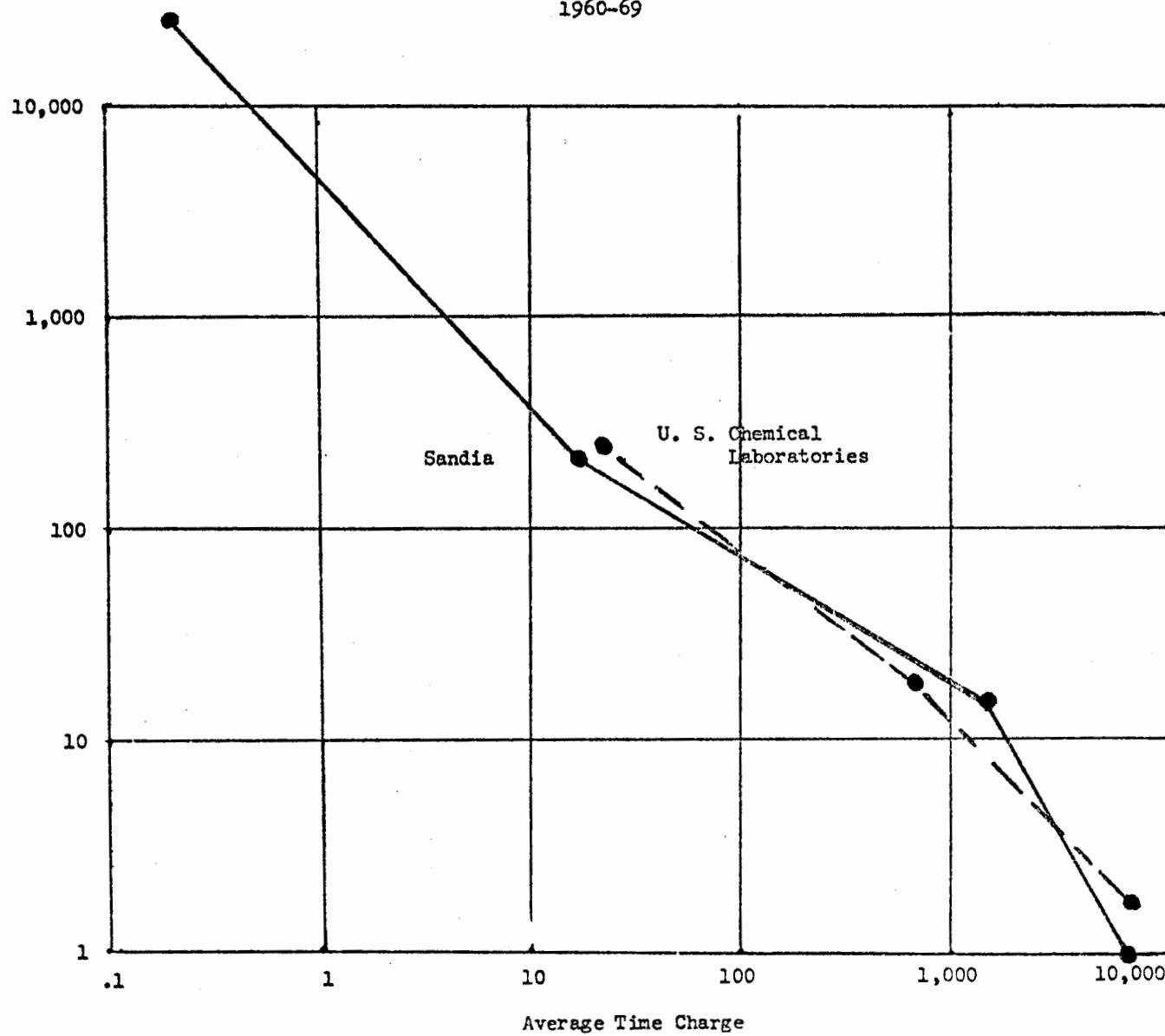


Figure 421 -
Figure 41-2

- 422 -

Figure 41-3

Numbers of Injuries by Severity
AEC Research and Production Contractors

1960-69

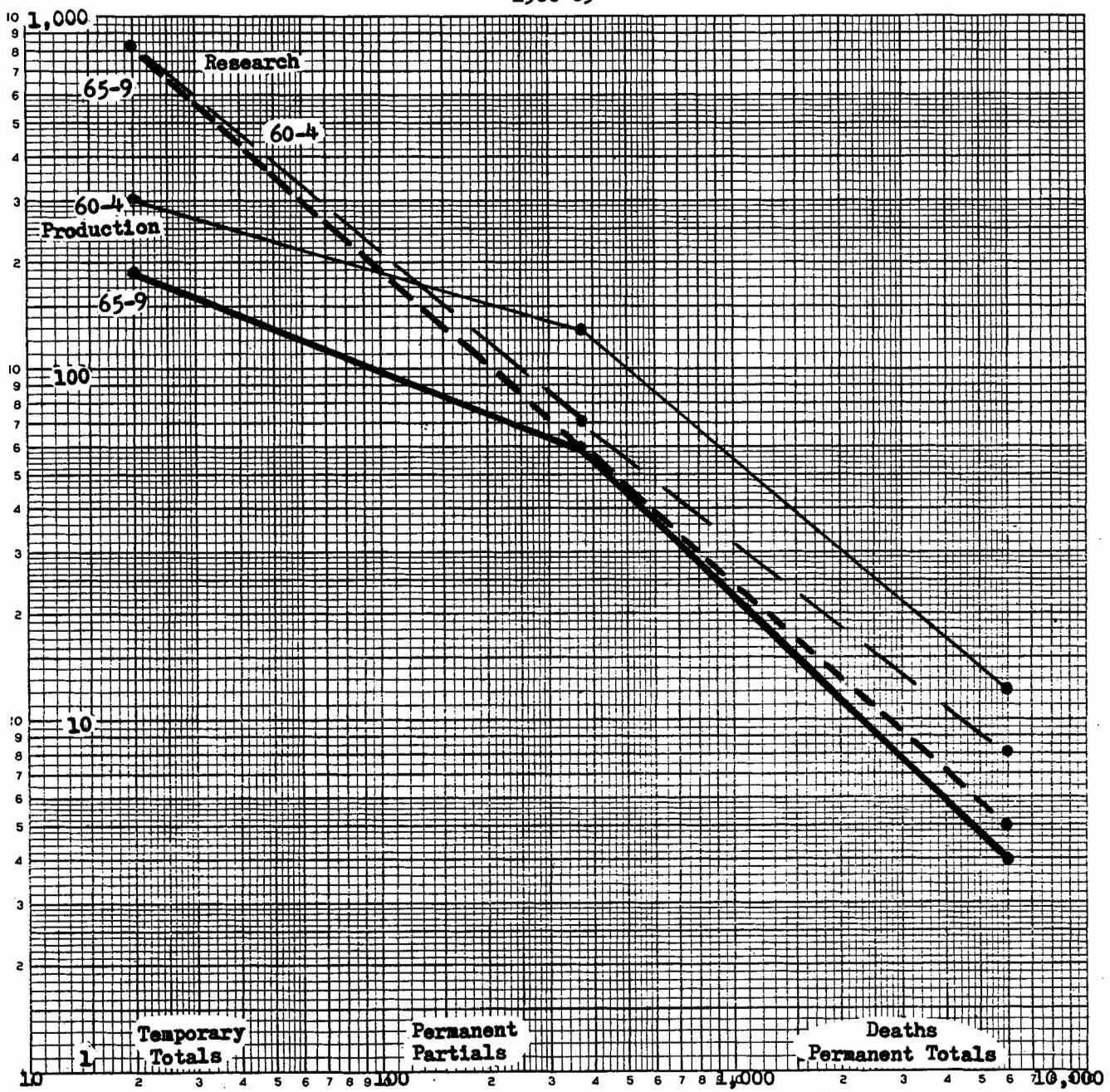
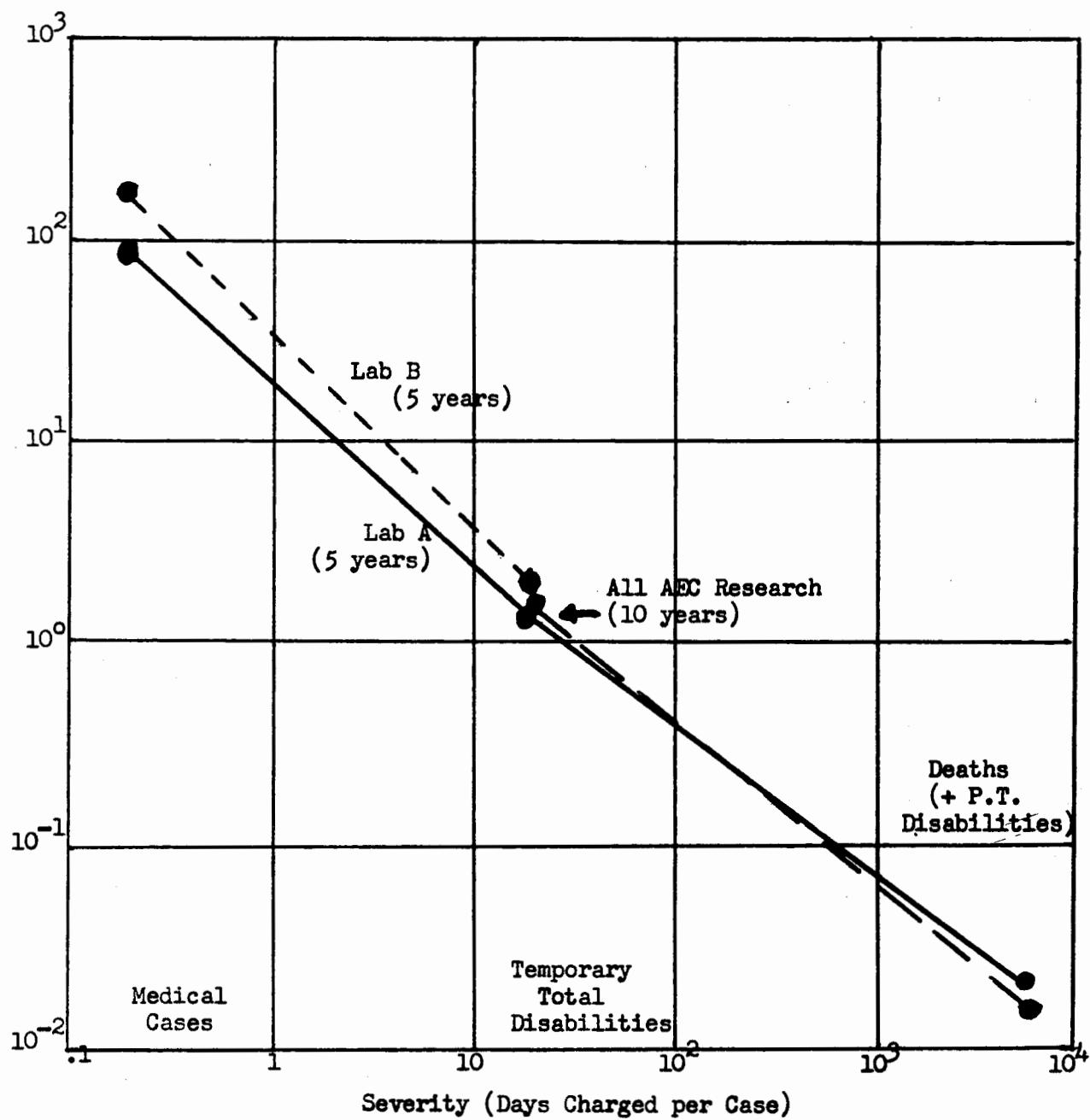


Figure 41-4.

Two Laboratories
One with Death, Other Not
Compared with AEC Research



tions do not seemingly fit what may very well happen next year, the year after, or perhaps tomorrow.

If we go back now to our purpose, it was to help management assess future risk, particularly of the "Vital Few." The matrix is then an aid in two ways:

1. Inferring "truth from uncertainty"
2. Keeping strongly aware of the real potentials for serious events.

Inferring is always a risky business. But at least we can display, rather than obscure, the potential for serious injuries. If our own data is unreliable, better to remain silent than misinform management. The industry background picture, properly used, can be helpful.

Current awareness of serious potentials (in the absence of system safety) is a difficult thing to assess. Past emphasis on injury frequency rate has been pervasive. But if, for serious accidents, the prime purpose of the frequency rate is to predict, the matrix exposes the questionable nature of this assumption. Further, the industry average, visually, "points" in the general direction of "truth." Management is less likely to be lulled. If there are limits and qualifications to the predictive value of the rate for temporary totals (as there most certainly are), these can more readily be discussed than when the potentials are obscured in the standard types of rates.

If it is agreed that the matrix has potential value, we can explore some additional dimensions of the concept.

We can extend the matrix to enter rates for temporary partials, or doctor cases, and examine the degree to which they help predict the less stable rate for temporary totals. (Somewhat irrationally we may create incentive for full reporting of first aid cases, to get a "good" slope for estimating temporaries.)

We can ask what the shape of the line would be if rates for temporary totals were plotted separately for 1-9, 10-99, and 100 plus days disability. Would the predictive value of temporaries for more serious cases be increased? Very likely. And the "vital few" temporaries with over 100 days disability would be exposed for evaluation.

Error rate samples (unsafe acts and unsafe conditions) can be plotted, if converted to a comparable man-hour or per-man rate base. Predictive value of error rates could be assessed and used.

And, in a more pessimistic direction, given background data on multi-death accidents, there is no reason why a matrix could not have some predictive value for the real disasters, at least create awareness.

The value of finely-scaled injury plottings cannot be fully examined

because of lack of data. Where finer plottings are available, the lines appear to be more useful. Consequently, the following possible combination of the class intervals suggested earlier is set out for trial:

<u>Category</u>	<u>Sub-Classes</u>
I	Multi-death
II	Deaths + Permanent Totals (single)
III	Permanent Partials - over 1,000 days
IV	PP - 100-1,000 days + TT over 100 days
V	PP - under 100 days + TT 10-100 days
VI	Temporary Totals - 1-10 days
VII	Medical) combine for plotting as .1-1 day
VIII	First Aid)

During this study a wide variety of data have been tabulated to examine the proposition that trends in minor injuries are predictive of trends in major injuries. As much negative data as positive data have appeared.

Greenberg (1972) used the wide scatter, great variability of minor-major ratios to support a statement:

"one can therefore not propose any fixed ratio between one type of non-disabling injury and disabling injury, for such a number would be meaningless and valueless."

If no fixed ratio, poor predictability.

Presently unexplained trends in minor injuries (intelligent guesses are available) leave at best moderate predictive value. Finer classifications of scale and better national data may be helpful. For the present, the impression is that minor-major trends should be viewed in the context of a matrix before being taken as significant. An exception is, of course, a highly specific type of accident--e.g., minor motor vehicle accidents are believed to be predictive of major accidents, but only in a context. That is, urban bus accidents may predict urban bus accidents, but not rural night-time drunk-driving accidents.

The following specific recommendations have been made for matrices:

1. Use a long-term matrix of frequency rates for various severities, extending as low in severity as possible.
2. Add an even broader criterion from the long-term record of your most nearly comparable industry.
3. Add the shorter-term experience of your organization.
4. Institute some sampling method for assessing the level of general risk

(unsafe acts and unsafe conditions). Insert (by dot) data from intensive studies of errors or unsafe acts and conditions.

5. Get professional statistical help in inferring status and estimating or guessing future probabilities and possibilities.
6. You will probably then want to institute a special study of disaster and serious accident potentials.
7. You will also very likely want matrices for the classes of energy and kinds of operations which produce the bulk of the serious injuries.

Extreme Value Projections.

The theoretical basis for this predictive technique seems to be well established (Gumbel, 1954).

The technique is being used at the National Reactor Testing Station to judge the significance and implications of weekly "worst value" radiation readings. The technique was first used by Phillips Petroleum Company's Atomic Energy Division in 1964, and similar reports were compiled in 1968 and 1970. Figure 41-5 is representative of the technique.

The figure represents "worst value" weekly radiation exposures arranged from low to high and plotted on cumulative probability paper. The "return period" across the top indicates how frequently a value could be expected to recur.

In Figure 41-5, for example, an exposure of 1720 mrem would not be likely to occur in less than 220 weeks, presuming the control system continues to operate as it did in the past.

The largest value plotted (arrow) indicates an event out of the "95% confidence" limits, that is, one very much worth looking into!

Such an "outlier" presumably has assignable cause(s) lying outside the system. It can likely be corrected only as an individual event. Then look for similar situations.

On the other hand, if the straight line projection (1720 @ 220 weeks) is unsatisfactory, the system must be changed.

For risk prediction the chart indicates the likelihood in given time periods for small and large values. This can be a basis for telling management what the "worst potential" is for the next year, or the next long-term period. Also, in risk management, the technique provides triggers for hazard analysis of extreme values.

The method is quick and easy to apply. Dr. Nertney plotted worst value figures for fires and property damage reports in a matter of a few hours. The fire data (blessedly) were sparse, but showed a pattern. The property damage

Figure 41-5.

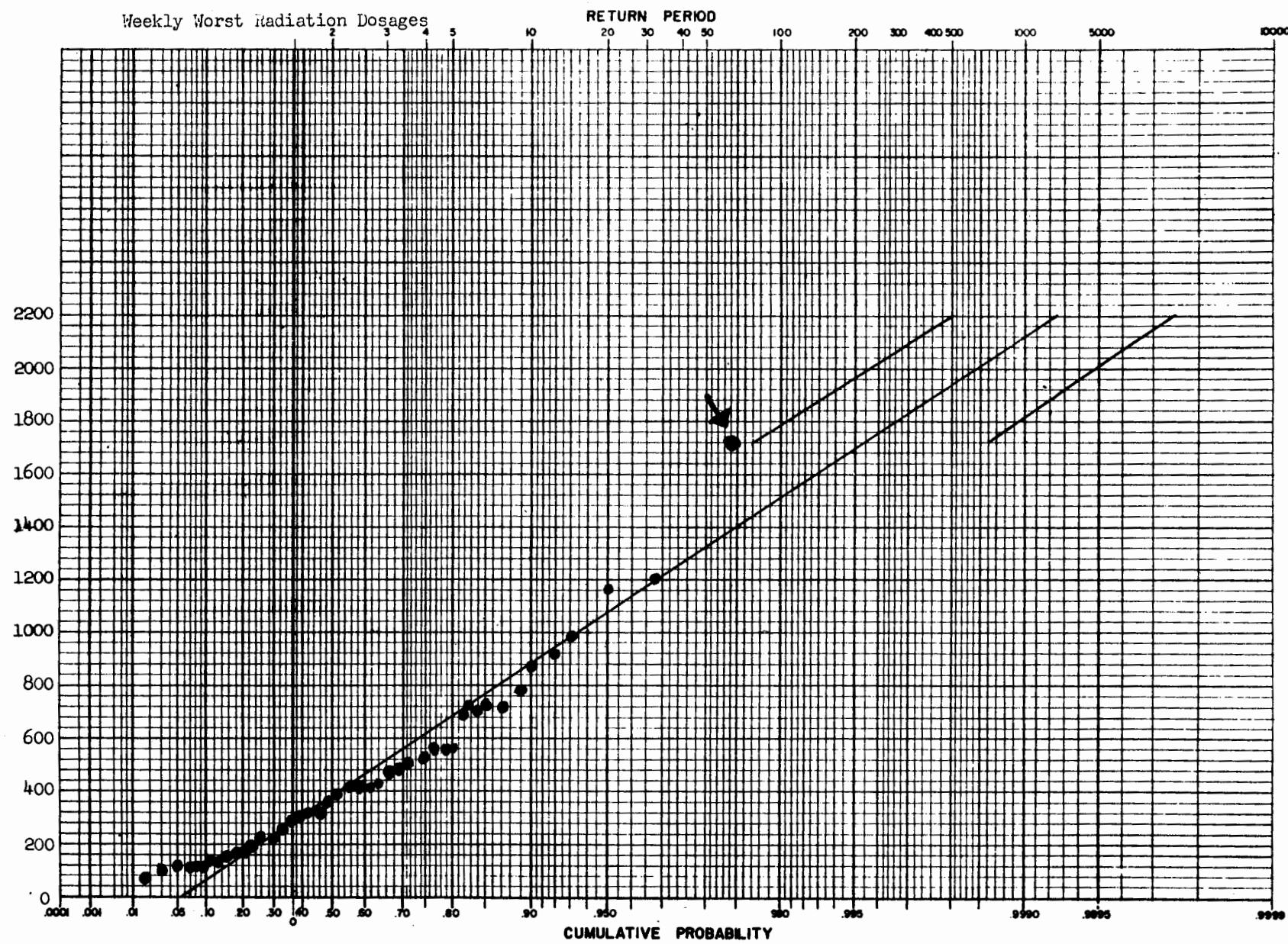
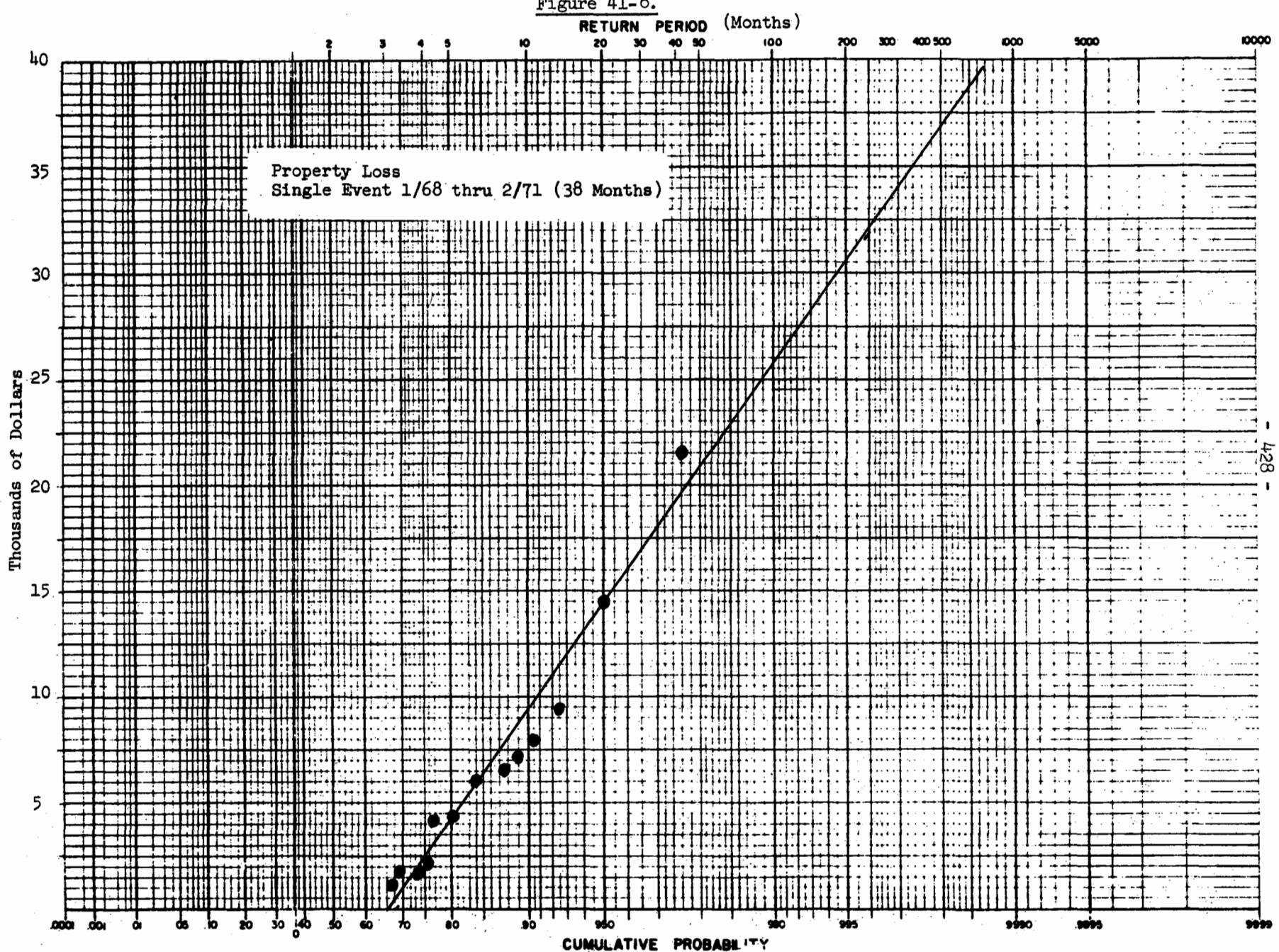


Figure 41-6.



data had more numbers and gave better indications of the potential value of the method. (Figure 41-6) Only true "outliers" could produce a \$40,000 accident in less than 5 years. The search is then for big loss potentials, if the system is acceptable as it stands.

A similar method was used in a national fire study (Livingston, 1967), but the indications have apparently not been exploited in fire-related industries.

The extreme value technique is being experimentally applied in England to predict occurrences and help assess "cost/benefit figures for expenditures on fire protection." (Bennett & Schoeters, 1973)

The first product of the method, the basic projection, is very simple to use, because the cumulative reliability paper automatically does most of the calculations. Proceed as follows:

1. Select a period (e.g., weeks for a year, 2 weeks for 2 years, months for two to five years, or years for 20 years) such as to produce an adequate number of plotting points (N).
2. Rank order the worst values for each of the above periods.
3. Select a left-hand scale which will allow for values two to three times your worst value.
4. Divide 1.000 by $(N+1)$ to get a plotting interval.
5. Begin plotting the lowest value at $\frac{1}{2}$ interval on the bottom scale, and plot remaining values at 1 interval.
6. Fit a straight line. Gumbel's formulae and tables give the ideal method, but an eyeball line usually suffices.

If the data fail to follow a line, or if there are clusters at the low or mid points, look for cause. In a plot of AEC property damage data (Figure 41-7, also prepared by Dr. Nertney for the September seminar) it was necessary to convert the worst values to ratios, because the exposure (AEC total property value) increased greatly during the period, i.e.g, raw data on total dollar losses were not homogeneous.

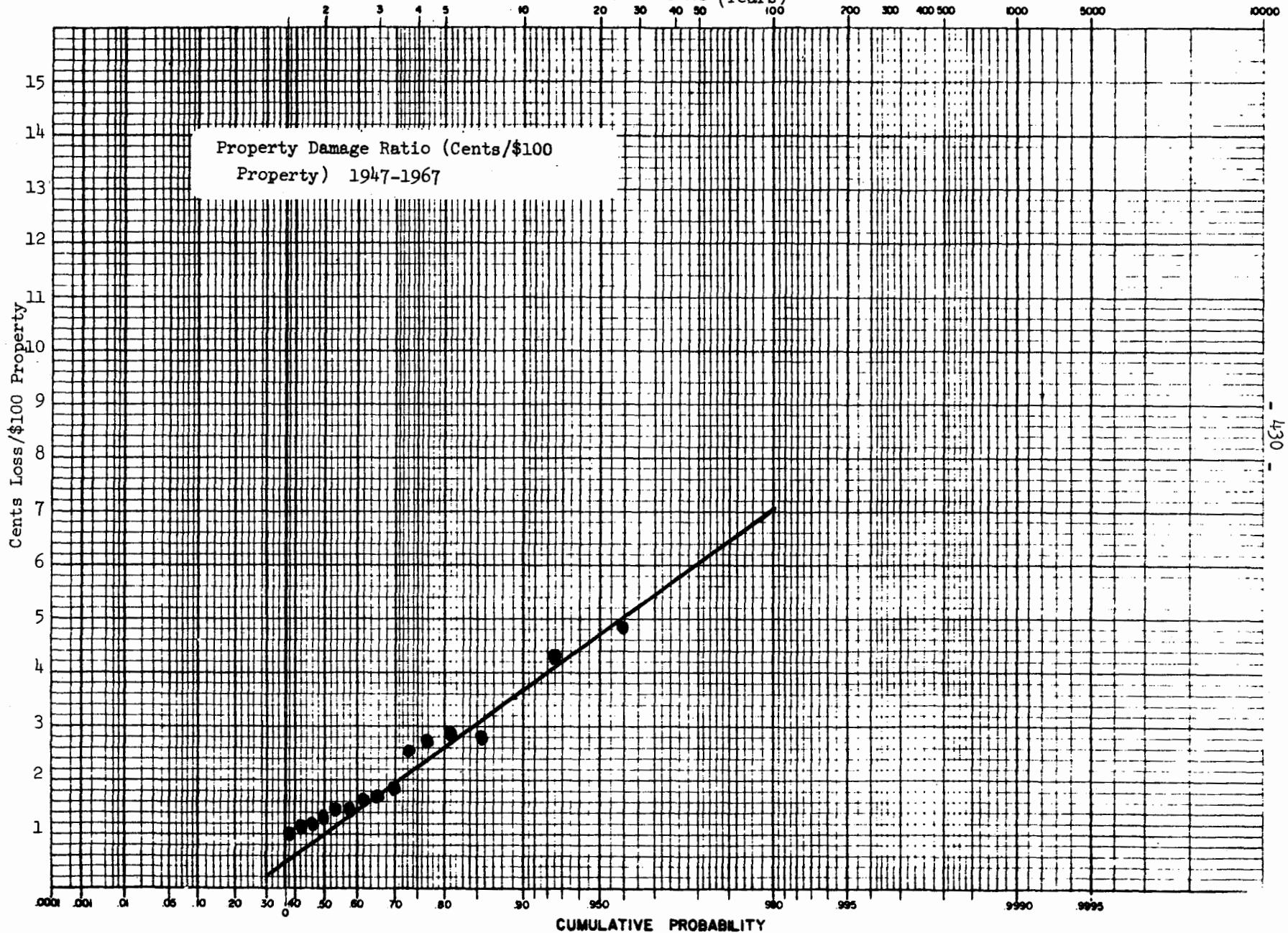
The matter of adding the 95% confidence limits to the chart can be approximated by locating points $0.32T$ and $3.13T$, where T is the return period of the largest value plotted, and draw parallels to the extrapolated straight line.

(As with many statistical techniques, consultation with mathematicians or statisticians in the organization is desirable for early applications.)

Rates and Probabilities.

These seem to require little comment, except to say that a number of projections may be made from internal and external bases and from various refer-

Figure 41-7.
RETURN PERIOD (Years)



ence values. Also, there may be merit in separately projecting dissimilar parts of an organization. Projections may themselves be fractional, that is, 1/100 of a death, or 1/1000 of a million dollar fire. Fractional projections can, of course, be priced out as risks.

Certainly great emphasis should be placed on getting useful bases for a variety of probability or rate calculations - not over-use of man-hours.

Significance Tests.

The injunction to apply common tests of statistical significance to accident data which are distributed as the basis for action has been voiced early (Goode, Mathewson, Littauer, Tarrants) and late (NSC Symposium, Appendix M), but seemingly with little effect.

Much of the data now distributed, in effect, suggests that managers and supervisors become statisticians and make the necessary tests.

The control charts (Chapter 37) and the foregoing extreme value projections are, hopefully, positive examples.

Phillips Petroleum Company at NRTS (Idaho) used "quality control" type charts of errors and injuries for supervisors and they were reported effective (Nertney, 1965). Rapid, intelligible feedback on minor injury incidence seemed to stimulate supervisors to use the normal devices of good administration (non-specific to safety) to bring current rates down to at least the level of the best or lowest values recorded in an uncontrolled situation. Similar results are reported elsewhere.

This service to supervisors was based on tabulations prepared by engineers and was discontinued under conditions of budget stress in a successor organization. If basic accident reports are computerized (as they should be, and are at Aerojet), the machines can cheaply produce the necessary charts using monthly, three-month and twelve-month values as moving averages, and thus give supervisors good signals as to when situations may be moving out of control. Aerojet has reinstated the service (Exhibit 18), and Sandia recently instituted such procedures in its routine reports.

One major criticism of the "standard" rates centers around their statistical instability in measuring past performance and assessing the future, particularly for small units. The rates have been accused of being "vague, unstable, insensitive and of limited reliability." In the typical rate comparisons, the small unit looks like a "hero" one period and a "dog" the next. Which is correct? Probably neither. Is this the kind of data we want to give management to assess performance?

Periodic data have a tendency, well known in statistical circles, to regress toward the mean. This is to say that a "bad" year is most often followed by a "better" year, and a "good" year, is most often followed by a "worse" year, if short-term data are statistically variable. This phenomenon has probably produced many heartaches for managers, and safety professionals as well.

All the time these aberrations were occurring, the mean rate for recent years was probably the best measure of progress or future risk.

The computation of trend data can be quite flexible - that is, a longer term reliable trend can be established with 10 year to 10 year comparisons, or 5 year to 5 year, or in a large organization, 2 year to 2 year. Then both long term and shorter term (annual, quarterly or monthly) trends can be assessed with "quality control" methods.

Standard Injury Frequency and Severity Rates.

It should now be clear why present standard (ANSI) rates are deemed to have very limited value. Can anything of use be salvaged? Of course. For a starter, several principles could be cited:

1. In listing rates show the severity rate first, because it is an index reflecting management concern, namely, greater concern for most serious accidents. (This is a reversal of present general practice.)
2. Footnote the frequency rate as being essentially (95%) a rate for temporary total disabilities.
3. Use very long-term, cumulative experience as primary, and list current experience as indicative.
4. Avoid detailed, rank-order listings. At most use four broad groups, as:

"Good" Well below average

"Better than average" Below average

"Worse than average" Above average

"Poor" Well above average

Within those groups, list units in alphabetical or any non-ranked order.

5. Be wary of small differences in rates - they probably have no meaning.

In interim recommendations to AEC the following additional thoughts were offered:

- * If current assessments of excellence are needed, tabulations should employ the relatively superior award qualification procedures of NSC or ASA. (NB: NSC procedures referred to are not those of the Sec-
tional contests.)

2. Arrange operational data in functional order, rather than rankings by rates. Deemphasize cross-context comparisons unless operations are reviewed for comparability. Discontinue all rankings based on small, unreliable rate differences.

In support of all the above recommendations, the following rationale was stated:

Severity Rates. Management is believed to have the common-sense concept that it is more important to prevent the more serious events, than the minor events. The Pareto principle of the "Vital Few" is relevant. Between the two standard ANSI rates, the severity rate is an easy choice. Concepts of using separate rates or matrices for different severities remain to be tested. Cost data as a method of combining events is not widely available on a uniform basis. In use of severity rates, undue emphasis has been placed on "making sense" out of man-day time charges with a man-hour denominator; the rate could be presented as a weighted index.

Long-Term Data. Perhaps the most serious criticism of commonly used monthly or annual tabulations is the high degree of uncertainty which would surround management actions based on the data. It simply does not make sense to give management a table of numbers in which random variations obscure the meaning. Longer term data, up to the limits of comparability, are an obvious, easily used alternative.

Functional Arrangement. As an alternative to listings by rate rankings, which have highly limited significance and are subject to gross misinterpretation, a listing by process or function is preferred. Since standard rates are useful for only gross comparisons, fine comparisons should be actively discouraged.

However, subsequent tabulation by AEC headquarters indicated that not even five-year and ten-year severity rates were sufficiently stable measures to have broad usefulness. (See, for example, Figure 41-4 for Labs A and B.) Consequently and from other tests of long-term severity rates, the overriding recommendation is to focus on future risk prediction and deemphasize both standard rates.

Further thoughts along the same line will be found in Appendix M, which gives the Symposium's Group III closing points on the frequency rate.

Presumably the foregoing discussions are sufficient to also suggest the limited risk prediction value of rates for minor injuries, such as the Serious Injury Index or the new OSHA rate.

The following citations of discussions of injury frequency rates are exhausting, but not exhaustive:

Magyar, Stephen Jr., "Accident Statistics, Their Meaning and Communication," National Safety News, September 1970.

"Do the Figures Lie?" Report No. Z16.1, Occupational Hazards, September 1969

"Safety Performance Indicator Fills a Management Need," ASSE Journal, March 1969

Miller, Gene, "Going Off the Record?" National Safety News, April 1968.

Van Zandt, G. H. Perry and Blanchard, R. G., "A Debate, Resolved: That Injury Frequency is an Accurate Measure of Safety Performance," NSC Transactions, Vol. 19, 1967.

Attaway, C. D., "Computing a True Accident Frequency Rate," ASSE Journal, Oct. 1966.

Cater, Bernard, "An Argument for the Revision of ASA Code Z16.1 Part 1.2.4.-Temporary Total Disability," ASSE Journal, January 1963.

Turner, A. W., "The ASA Disabling Frequency Rate is Not a Good Measure of Safety Performance," ASSE Journal, January 1963.

* * *

Essentially, the matrix says that rates can be useful if they first are broken down to expose the data to scrutiny, before hiding the nature of the numbers in the present standard rates. A prior report on Phase III included for one site:

The conventional occupational injury and accident rates and cause coding are largely irrelevant to the major safety concerns of the Lab. The data collected are not predictive of major trouble and have little apparent value in decision making.

* * *

It is rather well known that the mere act of observing sometimes affects what is being observed. The facts of observation and use, or misuse, of frequency rates have certainly had effects on tabulatable temporary total disabilities - so much so as to impair the usefulness of the data and discredit safety professionals. The adverse effects of award-oriented data collection on the quality of medical treatment are not always recognized, but some industrial physicians urgently wish that adequate, proper medical treatment were a first concern, and awards effects second in importance.

42. MANAGEMENT ASSESSMENT METHODS

Aside from routine assessments, and improved assessment measurements and predictions in the ways outlined in earlier chapters, the formal management assessment focussed on two principal methods:

1. Preparation of "Priority Problem Lists,"
2. Construction of a "War Room" to visibly display all indications of adequate or less than adequate operation of the safety systems.

Priority Problem Lists.

Management should, at all times, know what its most significant assumed risks are thought to be. The usual second order effect of such a list is action to reduce risk.

The "Fire Safety and Adequacy of Operating Conditions" lists prepared in early 1971 at all AEC sites provide an excellent illustration of the need and value in PPL's. The needs revealed were significant and deserved correction. Appropriations as well as allocation of one-half of regular, budgeted plant project funds were directed to the needs, and great progress is being shown in periodic reports. Rank-ordered priorities are being applied to corrections at an encouraging rate. Any delay for budget reasons becomes an assumed risk for the present, but possibly adverse public reactions of "assuming risks" are more than balanced by the record of steady reduction in risk. This project had more limited scope than the full range of safety. While in general well executed, the compilations suffered some from the crash nature of the project.

The MORT Trial contemplated the preparation of PPL's on a continuing basis, and as a two-channel process through the line organization as well as the safety department. (Such a process avoids some of the problems associated with a ^{S:51} crash project.) Use the FMEA form (Figure 24-5) to list and rank PPL's.

The PPL's obtained earlier and informally from safety engineers at two AEC sites did, in fact, consist of matters deserving of management attention.

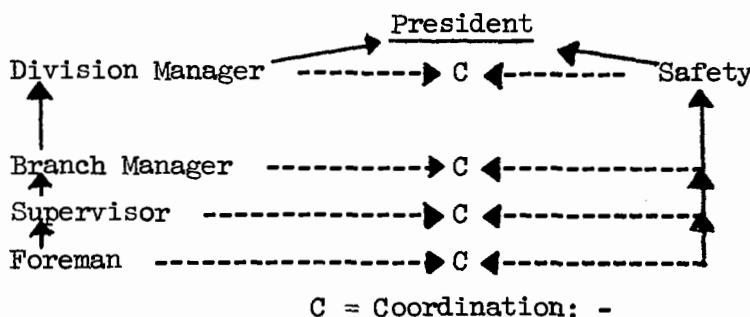
The absence of PPL's results in major problems going without formal review, until an accident occurs. PPL is not the same as the "worst credible catastrophe" used in AEC nuclear safety plans for advance planning and review. PPL is the residual after review and reduction, and in on-going operations.

PPL's give a final thrust and force to a monitoring program. The need for PPL stems from repeated instances of management surprise after disasters, although underlying causes were more or less well known in the organization. Further, it is easy in any organization to find serious problems which are being lived with on a day-to-day basis. Finally, management is entitled to know its assumed risks explicitly, and have its opportunity to develop better fixes.

An exercise in a MORT class at Aerojet was quite revealing. Despite Aerojet's good safety program and its low accident rates, a class assignment produced first draft, individual lists of problems, most of which unquestionably deserved top management review. In addition, discussion revealed that only about one-third of the problems had a "5-10 page or other document which was the kind of thoughtful study you'd be glad to hand to top management," and that top management probably had inadequate, marginal or no information on one-half to two-thirds of the problems. Experience at other sites suggests such a situation is all too typical of even good safety programs. (Indeed, a class exercise with AEC Field Office safety directors produced almost identical results in proportions of studies and top management awareness.)

An experimental procedure for developing PPL's through redundant line and safety channels with cross-checking at successive levels was initiated at Aerojet, as illustrated in the following figure:

Figure 42-1. Priority Problem Lists
(Worst Potentials)



C = Coordination: -

But independent lists may differ.

Thus far the lists have been unstructured. They may consist of broad, generic problems or highly specific problems. One man's trial effort organized specific problems under broad categories of level from disasters to serious.

It is intended that a final list be rank ordered by estimated consequences (probability x severity = risk) rather than by severity alone.

Obviously, such lists are "dynamite" - why wasn't it corrected? who is to blame? etc. But the problems on the lists are "cases of dynamite" - many will explode, given time.

AEC's "FS&OC" already provided a fine example. Nevertheless the actual development of the PPL lists has been a delicate operation, and has not been a hurried exercise. Much study went into the lists, and ample opportunity was given to managers to correct subproblems or aspects as possible.

The author's summary of early phases probably indicates the kinds of problems which will be typical, and a useful processing method:

The Division requested 37 management people in direct operations and their internal support groups to provide their views of the priority problems.

The raw materials were not forwarded through successive layers of management as raw material for their estimates. The time constraints and the delicate nature of this initial sub-project suggested that initial classification and analysis, coordination and consensus results should be handled at a level which was aware of the final impact (i.e., a report to the very top levels of AEC on its assumed risks) and the process whereby this might be feasible and practical without killing anybody - literally or figuratively.

Consequently the responses were first analyzed and classified by (1) a management advisor, (2) the project consultant, and (3) the safety representative on the project.

The raw material received was depressing reading; many sub-problems were reiterated in various ways.

The initial classification of raw material by management staff showed the following tabulations of items:

Manpower	26	Industrial Safety	10
Morale	23	Aged Plant Equipment	9
Fuel Handling	13	Audit & Surveillance	8
Scheduling	12	Management Attitudes	6
Procedures	11	Fiscal	4
Training	10	Support Performance	4

This analysis and grouping suggested a format for analysis and final output. From subsequent trials and discussions, the following protocols emerged as an embryo method:

1. The raw material should be tabulated by knowledgeable staff under primary headings which emerged from the material. At this stage, no idea should be omitted, but cryptic notations can be used. (Note that such a process is reviewable and auditable)

2. The above analysis was then taken as initial material for step 2 - development of an analytic framework. This amounted to the following format:

Col. 1: One or two word labels of major problems (as cited above)

Col. 2: "Sub-problems or manifestations" - the latter being a few-word report of the raw material. This was not, and need not be a rigorously defined listing - as a matter of opinion, much could be lost if this step was "hard" or rigorous. The flavor should be retained.

Col. 3: Considerations. This seemed to consist of several kinds of material:

- a. It was a place to set down solutions suggested by responders.
- b. Facts of life (e.g., nuclear matters need, first, scientist-engineer bases, not operators)
- c. Sub-sub-problems revealed in raw material.
- d. The analyst's relevant observations or questions to be answered.

Col. 4: Possible actions: This in turn seemed to consist of several kinds of material:

- a. Specific, relevant actions
 - i) in being, or
 - ii) planned, or
 - iii) possible
but generally not known to the responders.
- b. Management actions or plans not known to lower levels (including immediate associates)

c. Interim actions to "fix" aspects, but not related to a general study of a major problem. The question then being raised as to need, feasibility, and resources for a major study (defined here as a MORT-formatted study.)

d. At this point it became apparent that there were iterative cyclic aspects: e.g., problem = "don't know where to make knowledge and skill available"; response - "make suggestions"; response - "no one pays attention"; response = acknowledge and commend effort, and report disposition of all. A graphic or representative (footnote) method for disposing of successive extensions of problems was needed, but at this stage the purpose could be served by simple arrows and symbols.

Col. 5: Trade-offs - 1st level above. The trade-offs made at the next highest level of management then needed to be identified, not only as prior level constraints, but as to the assumed risks implicit in constraints or decisions.

a. The constraints can be time, budget, risk or performance.
b. The trade-offs may be distant in time or causal relation.
c. At the time of an accident/incident the general tone of reports is that immediate management should have "done it better." With this, the role of prior constraints on "doing it better" seem to be "excuses" and will be (1) not proffered, or (2) not accepted. All the time, the "impact statements" prepared after budget-schedule-performance changes probably provided the superior managers with assessment of the probabilities.

Col. 6: Trade-offs - levels above 1st. Many constraints are imposed by decisions two or more levels higher in the organization. These are successively more immune to conscious evaluation of risk, are often imposed by staff rather than line, and are largely unmentioned when an incident occurs. Thus the topmost level of management says, "I was uninformed." The new system is designed to do two things:

a. Provide a frame of reference whereby lower management reminds upper management of "impact statements" which assessed risk.
b. Provide upper management with an assessment of the risks it is, in fact, currently assuming.

In the course of the above analysis, several generalities emerged:

- i) "Major" problems were often associated with a variety of minor studies and fixes. Thus raising, in a prominent way, the question of need for a "major study." The general experience (in analysis) suggests that (1) there are kinds of solutions not frequently conceived or studied in a series of minor fixes, and (2) these may be more likely to be solved in a "major study," e.g., a major study warrants more extensive information search, more in-depth analysis of human factors, and greater investments in cures. On the other hand, a general problem such as morale is amenable to many specific fixes.
- ii) Not unexpectedly, the problems identified by responders are inter-related, that is, manpower or morale are affected by procedures, training, surveillance, et al. Thus, a second level of analysis was indicated, namely that responses be reclassified closer to the point of action, e.g., morale aspects of procedures, training, or audit be handled under the latter primary headings (where other aspects of procedures, training or audit could be controlled).
- iii) Responses affirmed not only need of priority problem analysis

to sort, arrange and respond, but also the need to communicate past, present and future actions downward - particularly for morale, or other, similar diffuse problems.

3. Step 3 - Insertion of informal management views of top problems and initial responses to first draft analysis above.
4. Step 4 - Analyst reworking of raw material in terms of above principles. Specifically this includes regrouping of original responses under primary work-oriented headings, that is, under "morale" there are only cross references to procedures, audit, training, support division performance, etc. On this basis, morale could continue (if responders thought so) in the number one position, even though solutions were cross-referenced to specific aspects.

After the initial summary at Division level, a number of months were needed whereby Division management did as much as was within its power to correct problems. The list with study was then forwarded to the President for review. Meanwhile, the Safety Division has conducted its studies and analysis and produced its list. As might be expected, the safety list is more oriented to specific major problems in safety engineering. The project is, of course, continuing and many improvements have been made. (Further discussion, page 444.) PPL

The War Room.

From the number of Safety Program Improvement Projects (SPIPs) described thus far, it should not be surprising that it became increasingly difficult to maintain an overview and assessment of the work. In order to maintain visibility for the analysis and results, not only for management, but to brief others on the plans and progress, a "Division War Room" display of the working papers was organized on a blank wall some 20 feet in length. (The display might have been called "Safety Room" or "Safety Control Room.")

Although the "War Room" was a working room and not a polished display, it served its purposes: (1) management information, (2) a working focus for the MORT team, and (3) a briefing room.

The general organization of the material is shown in Figure 42-2.

Basic Schematic - The Work Process Schematic, Figure 29-1, p. 294.

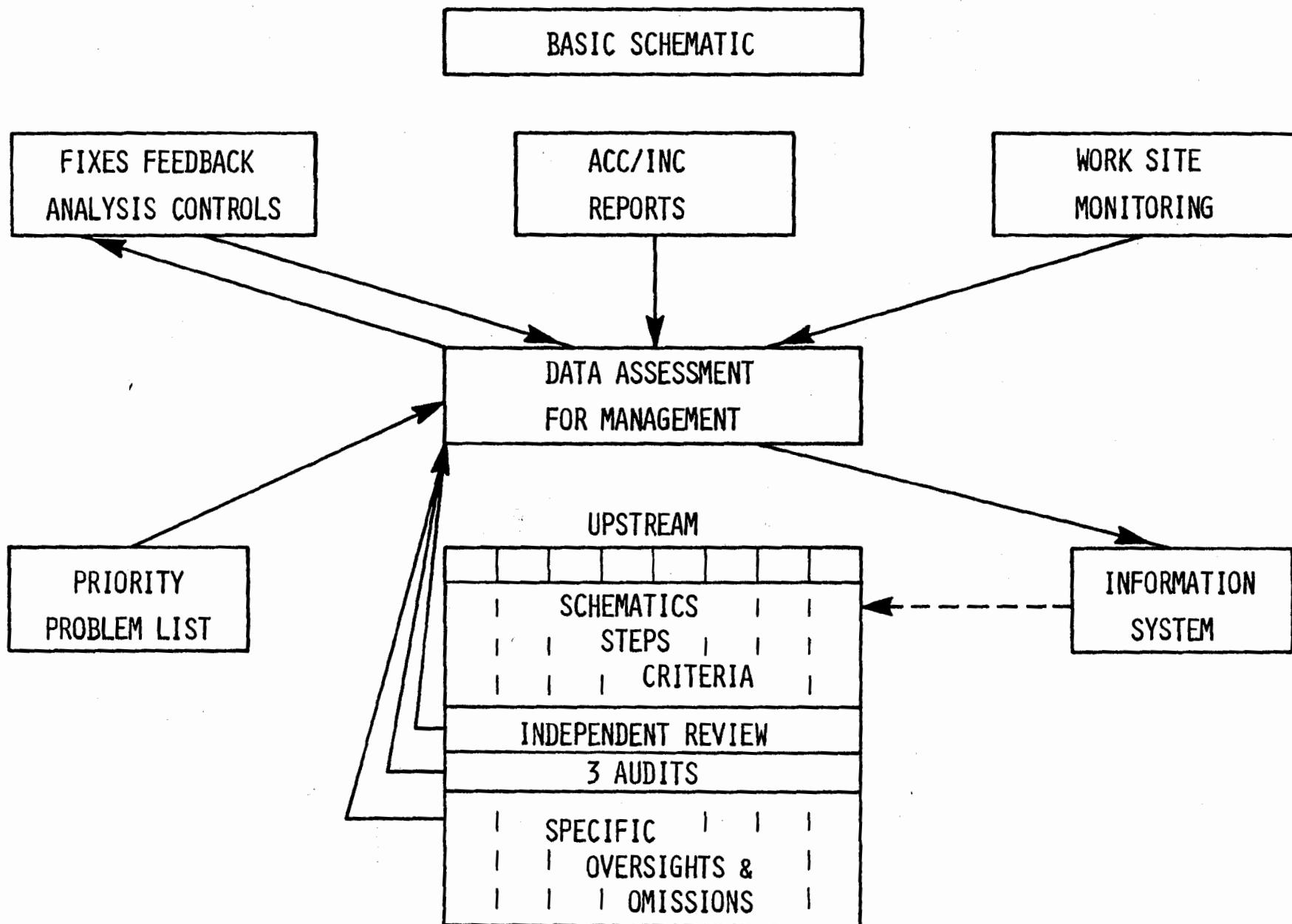
Data Assessment for Management was the focal panel. This meant (1) data reduction by Safety and R & QA (fewer isolated, random reports) and then (2) reduction by Division staff (following techniques in Chapter 41).

Accident/Incident Reports used the control charts, matrices, rates and extreme value projections described in Chapter 41.

Work Site Monitoring - the general plans developed in Chapter 37, plus reports of actual monitoring as they came in - control charts, surveillance reports, etc.

Upstream Monitoring - also from the plan developed in Chapter 37. This

Figure 42-2
WAR ROOM



took over half the display because each process and subprocess for personnel, procedures and hardware had to be separately displayed.

1. In the upper section, the audit results were shown (good and bad) in the format - schematics, steps, criteria.
2. An intermediate section showed the status of criteria and implementation for each pertinent review agency.
3. Three audit schedules and completion were shown: (a) self-audit, (b) independent audit, and (c) customer upstream audit, e.g., where a Division uses outputs of Engineering and audits its supplier.
4. In the lower section each report of a specific oversight and omission was posted on a 3x5 card, and remained posted until it had an item fix and a system fix - the latter being a correction of the "reason why something went wrong."

PPL and FS&OC status were posted.

Fix Control (based on feedback and schematics, for each information input) and special analyses and in-depth studies had a panel.

Information System - that is governing policies, procedures, manuals, literature, monitoring studies, case records, etc., were assembled.

In addition, on other walls, were displays of model processes (e.g., MORT) on which projects were plotted, SPIP progress charts, and MORT Team assignments and projects.

A prototype display for the whole corporation was prepared to show summary progress along the same lines in each division of the company and in each branch of the safety division. In addition, schematics, etc., were displayed for specific safety division functions.

The next steps will be to reconstruct simpler division and corporate displays, much condensed, but supported by file data in the room.

Ultimately, the display may be condensed to an "Executive Instrument Panel" for the safety function.

The exercise fulfilled its original purposes, and was helpful in organizing and directing the work.

* * *

Gausch (1972) contrasted the subjective nature of many safety decisions with science-oriented, quantified management decision methods coming into use. The Decision Table is a simple method of beginning to bridge the gap between safety and management. After postulating a company-wide evaluation (comparable with the PPL), Gausch illustrated the condition table and action table as shown in Figure 42-3. The upper condition table is comparable with scaling mechanisms shown in Chapter 2.

VIS. S. 251

Figure 42-3. Hazard - Action-Table

Frequency	Severity			
	Negligible	Marginal	Critical	Catastrophic
Extremely Remote	█	█	█	█
Remote	█	█	█	█
Reasonably Probable	█	█	█	█
Probable	█	█	█	█
"Actions"				
Forget It	█			
Long-Range Study		█		
Correct, (1 year)			█	
Correct, (90 days)				█
Correct, (30 days)				█
Shutdown				█

This type of decision aid should reduce the inertia often encountered in dealing with numbers of major problems, since the table provides a simple focus for action decisions.

The Decision-Action table should be a neat way to move error reports through a fix process. Action dates can be earlier or later dependent on manpower. The results should be an orderly record of work in progress and action.

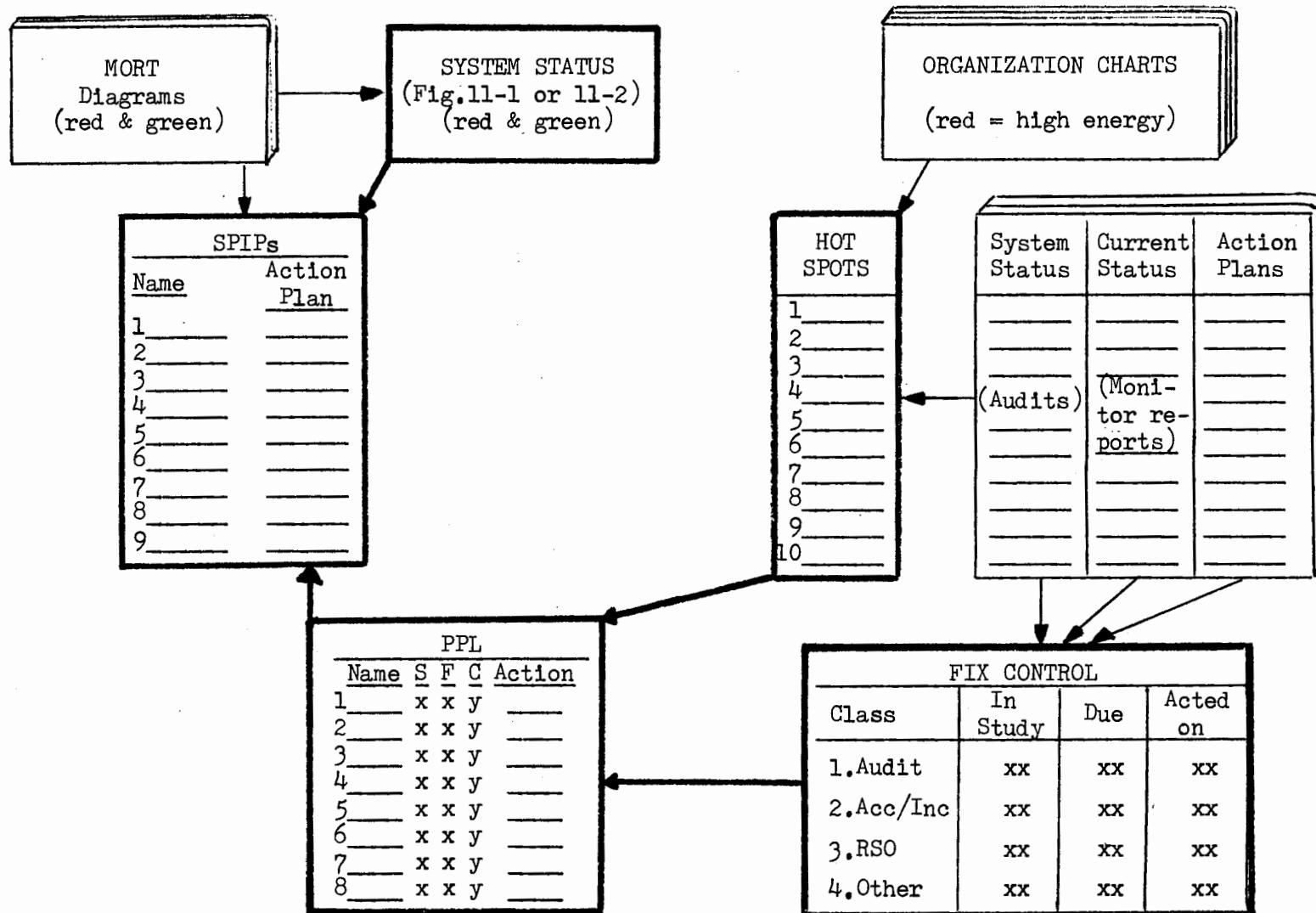
A method of organizing a brief report to the president or chief executive officer is illustrated in Figure 42-4. The MORT diagrams are marked up to reflect program strengths and weaknesses, which can also be shown in brief on the Safety System (Figure 11-1 or 11-2). From these projects some are selected to form the Safety Program Improvement Projects.

The organization chart can be marked up to show the "hot spots"--units or places with high-energy and/or poor accident rates. We can draw on audits to show system status for each hot spot, monitoring reports for current status, and action planned.

The Priority Problem List and the Fix Control (grouped data on the latter) are presented.

Such a format is flexible--it can be briefed down to essentials or expanded as desired.

Figure 42-4. Preparing the "Report to the President"



The data handling model presently under trial use at Aerojet employs the following analytic elements previously described:

1. The frame of reference for management assessment is established in three ways:
 - a. Policies, goals, constraints, commitments (e.g., to customers), scope (damage, injury, public impact, program impact)
 - b. Program ideals (such as the three trees shown in Exhibits 3, 8, and 12, or MORT itself)
 - c. Specific Aerojet directives (see Figure 20-3, page 194 for a model).
2. Information inputs from Safety and Reliability in the following principal areas:
 - a. Standards, codes and regulations,
 - b. Incident reports,
 - c. Audit and monitoring reports (see Chapter 37).
3. The "hot spot" lists may be organizations, places, or processes (such as shipment of radioactive material).
4. Analysis on a non-duplicative basis by Safety and Reliability--see energy classes (page 36), analysis methods (Figure 24-5, page 251, and either Figure 21-2, page 216 or Figure 21-3, page 219).
5. Data reduction following Figure 42-4 to provide for each level of authority:
 - a. Audit and monitoring results, in terms of
 - (1) System satisfactory,
 - (2) System improved,
 - (3) Errors, oversights and omissions.
 - b. Priority problems (residual risks)
 - (1) Action status (by suspense dates),
 - (2) Specific risks to be assumed or returned for further improvement.

In this manner the original exercises in preparing Priority Problem Lists and building a War Room are steadily moving toward quantified and analyzed bases for management of safety and risk.

IX. SAFETY PROGRAM REVIEW

S, B.

Safety Program Review is postulated as a major facet of management assessment of risk in both the general risk assessment model (Figure 21-1, page 212) and in the process of data flow for risk reduction (Figure VIII-1, page 346).

The general scheme whereby such review can be conducted is outlined in revised MORT, as follows:

SAFETY PROGRAM REVIEW

1. Define Ideals
2. Descriptions and/or Schematics
3. Monitor, Audit, Compare
4. Organization
 - a. Scope
 - b. Integration (or Coordination)
 - c. Management Peer Committees
5. Staff
6. Services

Safety program audit has already been preliminarily discussed as an aspect of Monitoring, Chapter 37.

Ideals.

The ideals toward which a safety program is to be developed, and against which a program can be measured, should be articulated. MORT constitutes one such ideal. It is not so much important that MORT ideals be accepted, as that an organization's or safety professional's ideals be stated and described with comparable specificity. If a MORT ideal is not attainable or incorrect, simply state the alternate provisions which are tenable.

What should management know about (and require) of a safety process?

1. Essentially the management side of MORT:
 - a. especially higher ranked material?
 - b. especially a risk assessment system?
 - c. especially a hazard analysis process?
2. Plus?
 - a. a safety precedence sequence?
 - b. energy, barrier, change and error?
 - c. error tolerance limits?
 - d. effective supervisor approaches?

Ideals are the working platform from which improvements are projected.

Descriptions and/or Schematics.

It seems fundamental that the safety program ideals and actual performance be documented in fairly complete, even if informal, operating manuals and schematics and that program operating data be available and evaluated. But such is not very often the case. Thus management has little assurance that

the program has a plan, is operating according to the plan, or how any program plan compares with a higher-level scheme of protection.

The suggestions: "Build an Executive Instrument Panel" or "Build a War Room" for any problem, seem well founded. As matters stand, we don't have the beginnings of a wiring diagram for most safety programs. Little wonder they are poorly understood and that management is accused of failing in support. What is needed is not a literary masterpiece, but a conceptual picture of the safety system (and later some numbers).

Almost universally in this and other studies there has been a major lack of outlines and schematics which substantially describe a program. (Lengthy procedural documents have the same index of confusion, gaps, and overlaps found in general in this study.)

The substance of this text raises many questions of safety program definition and substance. (Early examples of simple program schematics are shown by three figures in Chapter 28, Independent Review.)

The development of schematics, steps, and criteria in operating divisions revealed many safety program gaps and deficiencies. But, when these same analytic techniques were applied to safety division operations, similar defects were quickly apparent. It would seem that program definition and measurement in safety should be a prime condition for proper working relations with the operating organization and for safety budgets.

Fundamental to understanding of hazard control processes is a clear understanding of major differences in project forms of organization (e.g., much of NASA) and on-going functions (e.g., much of AEC and industry). What safety discipline and schematic is a given unit using? Universally, this major distinction is ill-defined, both in system safety and occupational safety. And, when a project form of organization is used without appropriate safety provisions, as an exception in an on-going program, trouble arises. (See, for example, page 66, Figure 5-1.)

Monitor/Audit/Compare.

Measuring, as with ideals, is a concern of almost this entire text. Note, for example, on page 369, how an accident can raise questions about safety program, as well as about management. See the section on program audits in Chapter 37 and also there examine the safety role in monitoring. Are these functions fulfilled?

Other measurement systems have been suggested (Johnson, 1964; Planek, 1967; Attaway, 1969; Diekemper and Spartz, 1970). All express concepts and philosophies of measuring, as well as educating management.

Further, from an earlier report:

Program evaluation should not be divorced from program design. Measurement devices should be built into program, rather than retrospectively developed. Thus they also become a part of recycling program improvement. Planek's Programming Planning Model (Appendix G) and the NSC Measurement Symposium (Appendix K) stress the point and offer guidance.

Evaluative research on programs can be of great practical value. Summarizing the literature, Caro (1969) enumerated some views on key aspects:

Objectives of evaluation:

1. Extent to which the program achieves its goal,
2. Relative impact of program variables,
3. Role of program as contrasted to external variables.

Categories of evaluation:

1. Effort - amount of action
2. Effect - results of effort
3. Process - how effect was achieved
4. Efficiency - effects in relation to cost.

Funding of external measurement, as well as internal scientific resources, should be utilized in conducting evaluative studies. Frequently inexpensive program evaluation schemes can be integrated into program plans, and this should always be an objective.

There is nothing wrong, and a lot that is good, in measuring efforts, first order effects, and program processes and efficiency, provided no one loses sight of the ultimate measure--accident reductions. A variety of such measures is diagrammed by Planek (Appendix H).

Tarrants (1965 and 1967) has urged evaluation and offered numerous suggestions, particularly on the need for error data as measures. A good example of use of work sampling and other measures to evaluate a Safety Observation training program (Satterwhite, 1966) showed that the program under study was not effective; however, the collateral recommendations which emerged from the study repaid the careful measurement effort. Other examples have been given.

In any measurement scheme the general organization goals, values and performance must be evaluated. From an earlier report:

Perhaps the best example of Lawrence's problems is the Nobel-prize-winning feat of developing the hydrogen bubble chamber. This type of project not only probes boundaries of existing knowledge in physics, but also crowds boundaries of safety technology (exceeded previous technology), and only appropriate safety precautions could make feasible the research process itself.

The major emphasis of Lawrence's safety program is on support and assistance to scientists so they may fulfill experimental requirements with safety. Exotic hazards to be controlled are a far cry from the more conventional hazards of a production process. The philosophy is not really different from the industrial concept--production with safety. At the extremes of risk management for high energy physics research it is even more clear than in industry that the work simply cannot be done without safety--creative, imaginative safety.

Management leadership and responsibility criteria used in judging a Federal agency safety competition were listed earlier. The additional criteria used in this competition, while not considered to be up to MORT standards, do present a variety of useful questions (Johnson, 1964).

Maintenance of safe working conditions

1. Do program documents provide for a regular and orderly procedure of safety inspections?
2. Does each echelon from units to agency headquarters utilize inspection schedules?
3. Are deficiencies noted and official recommendations submitted?
4. Are inspection reports given appropriate and timely follow-up reviews?
5. Are inspection procedures implemented objectively and qualitatively as well as quantitatively?
6. Are accident reports used to identify and correct unsafe conditions?
7. Are provisions made for the supply and use of adequate and approved protective clothing and equipment?
8. Is a safe and healthy place to work provided including safe equipment, safe tools, and guarded machinery; physical conditions such as ventilation, light, and noise?
9. Are operations and process planned and arranged with careful attention to safety?

Establishing safety training and education

1. Has the agency provided broad guidelines and instructions for general and specific safety training of personnel?
2. Does the agency provide a systematic quality program designed to keep caution alive in the minds of personnel?
3. Is safety training integrated into broad agency training of supervisors?
4. Is safety training included in orientation of new employees? Is safety stressed as an integral part of on-the-job instructions?
5. Are special safety training programs developed and disseminated throughout the agency?
6. Is a systematic and energetic follow-up made of safety training programs to evaluate training effectiveness?

7. Is special career training given to agency safety personnel designed to improve their performance as safety advisers?
8. Are safety contests and award programs utilized to promote safety education?

9. Are accident reports used to identify training needs?

Accident record system

1. Does the agency possess a firm policy and definitive procedures and instructions for reporting accidents?
2. Are reporting procedures compatible with the Bureau of Employees' Compensation laws and administrative directives for reporting injuries?
3. Does the reporting system prescribe internal checks to insure efficient processing of reports prescribed by law?
4. Does the reporting system prescribe that accident reports be reviewed at and approved by higher levels of supervision?
5. Does the reporting system require thorough and complete investigation of accidents?
6. Are accident reports combined for analyses and identification of common factors of causation, accident agency, and activities?
7. Does the accident reporting system prescribe for the periodic review of accident data and causation analysis?
8. Does the agency disseminate accident data and causation analysis to subordinate echelons?
9. Does the reporting system provide for accident analysis at installation and regional levels?
10. Are BEC and agency injury reports reviewed for comparability of information?

Medical and first-aid systems

1. Does the agency provide adequate and timely first aid and medical treatment of injured personnel?
2. Does the agency conduct health and sanitation surveys?
3. Does the agency conduct a preventive medicine program for its personnel?

Scope and Integration.

Evidence of the wisdom of several organizational principles is mounting:

1. The scope of the safety program should include all forms of hazards.
2. The staff support for safety should be integrated in one major unit, rather than scattered in several places.
3. The staff safety unit, in order to be capable of independent review, should report to top management without unnecessarily impeding layers of organization.

The AEC pattern of Divisions of Operational Safety fulfills these criteria.

As safety programs take on a greater systems and operational flavor, the location of safety units should not characterize safety as an "industrial relations, personnel, health, medical, or insurance" problem.

Where some safety functions are split off (e.g., nuclear criticality at some sites) and/or where relevant technologies such as system safety analysis or human factors capacities are organizationally remote, specific action (e.g., a "safety council" or study and improvement of day-to-day working arrangements) should be used to insure that the organization uses its competencies.

The common industrial separation of safety into "personnel" and "product" functions is probably a major obstacle to a proper view of "operational" safety, and has seemingly put professional blinders on the separated groups. Certainly occupational safety is not a "personnel" function, and simultaneous placement of product safety in design groups frequently denies management the values of independent, professional review of operational safety.

Organizational Placement.

From studies, the common placement of the safety function is two or three organizational layers down from the Chief Executive Officer, seldom one. And further, occupational safety is largely seen as a "personnel" function.

During this study an interesting conversation occurred with two vice-presidents of a large R & D laboratory.

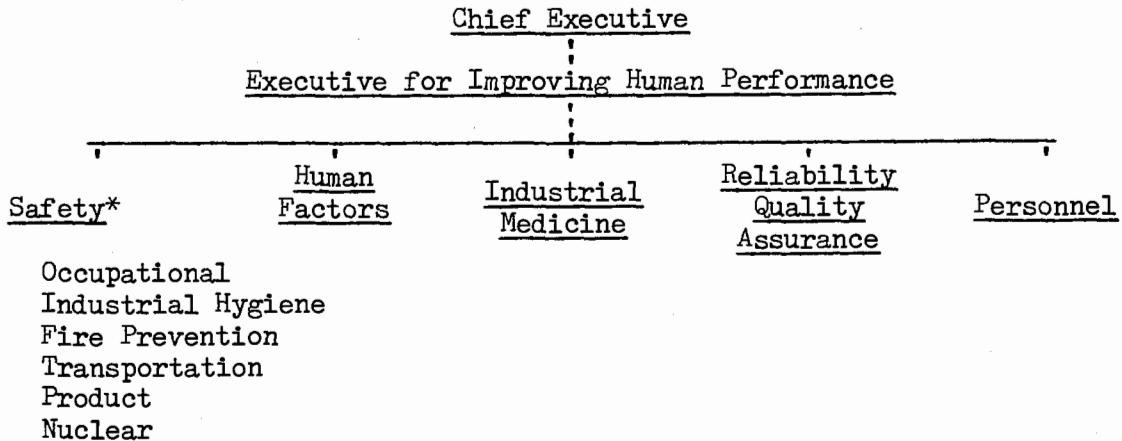
By way of indicating their qualifications, each V. P. was directing an advanced technology division with some 1,000 employees. One was the "senior v.p." and had managed refineries for a major petroleum company. In this informal discussion, a principle emerged in their minds, namely, the safety function should report directly to the President. However, as the discussion proceeded, they said, in effect, "The trouble with such a proposition is that the safety directors we see, probably typical of the group, have not gone through the usual succession of expanding managerial assignments which develops the managerial capacities required of a person who reports directly to a president. A president gives little guidance. He's too busy directing the company as a whole. Consequently the safety function should report to the president through a senior executive who (hopefully) avoids the improper stereotypes you have described."

In NASA's Manned Space Flight Program, safety and reliability and quality assurance were last reported as grouped (their functions and methods are similar), reporting to one director.

One multi-plant company has common managerial supervision over safety and human factors, with a strong program in the latter area.

If organizational arrangements have significance, and they probably do, the following format seems to convey the operational nature of the functions, to group five closely related functions, and to emphasize the service and independent review status of the functions vis-a-vis line management.

In consequence of all of the above observations and organizational approaches, a possible form to be examined seems to emerge:



*The specialties may sometimes be separate units, but retention within the above framework seems to have advantages.

While the above guidelines for safety organizations seem well supported in the author's experience, a more flexible and studied approach may well supplement, reinforce or contradict the guidelines, particularly in varied industries and corporate types. Gausch (1972) draws on organizational sciences as well as experience to suggest studied approaches which reflect the actual inter-relations of functions and units, both formal and informal. Certainly, Gausch's stated goal of achieving an effective synergy of unique interdependent units is excellent.

Gausch correctly emphasizes that effective day-to-day working arrangements may be quite different from the formal, advertised relationships. However, audits of such relations almost invariably show serious deficiencies as well as some substantial advantages. So audit or study would be a common ground for developing program or organization improvements.

Safety Staff Organization.

The matrix has been frequently used as an organizational tool--discipline vs function. The concept is shown in Figure IX-1. The disciplines will vary widely, dependent on the organization.

The functions of Research (in a discipline), Literature Search and Analysis are usually best organized by the disciplines.

Field Service in a geographically centralized unit may be similarly organized; if geography-distance is significant, it can be organized as a geographically decentralized function representing the entire organization.

Information and Program Development are seemingly seldom well done if

Figure IX-1
SAFETY ORGANIZATION MATRIX

<u>Disciplines</u>	<u>Functions</u>					
	Research and Literature Search	Analysis*	Field Service	Training	Information**	Program Development
Industrial						
Fire						
Ind'l Hygiene						
Radiation						
Nuclear						
Waste Mgt.						
Environmental Impact						
General						

* Includes Standards and Recommendations

** Data collection, reduction, retrieval

left as collateral functions of the disciplines. Distinct staff units and assignments are needed. Pinkel (NASA) goes so far as to suggest that the safety information function be established outside the safety office to insure independence, and clear measurements of high quality information services.

The Program Development function may also be the focal point of the research orientation, as well as having the basic system design and improvement role.

In addition, if the Safety Review function is emphasized (as at Aerojet) a unit to coordinate the work is valuable.

Search-out and application of new technology is handled as a collateral function in most safety departments (other than some nuclear criticality staffs). Handled in this manner, the function is grossly under-staffed and under-emphasized. There is little enough time for search-out and practically no time for application. Thus many technologies, particularly analytical and behavioral, remain undiscovered and/or unused by safety staffs. Two solutions are suggested for management action and evaluation:

1. Require safety professionals to budget time for professional growth, and to expose themselves to non-safety technology (5-10% of time).
2. In a safety staff of any size (e.g., five or more professionals), require allocation of one man to the function of technology acquisition and application.

These approaches may result in more hazards undetected or uncorrected in the short run, but should produce greatly improved safety performance in the very near future.

In thorough accident investigation, particular attention should be given to non-use by safety personnel of available technologies, and this suggests some independent accident investigations by non-safety professionals.

Yardstick criteria as to numbers of professionals on a safety staff seem to have slight value, as do yardstick budgets. Too much depends on functions included and management expectations.

The collection of data on program holds the possibility of providing management with objective measurements of activities and gaps in programs whereby manpower requirements can be assessed.

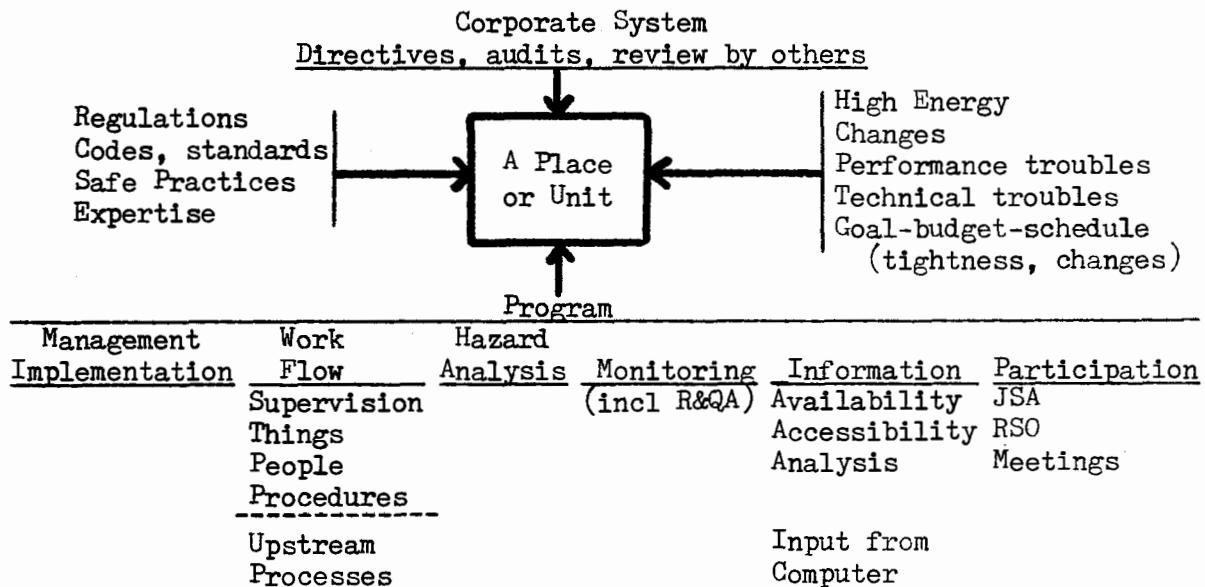
Such data can also help in measuring the coverage of key functions. Specifically, under conditions of austerity, the proportionate emphasis on key functions can be judged, and shifts from lower priority functions can be planned. For example, in one budget-reduction case, "quality control"

type feedback of safety information to supervisors was discontinued even though it had been highly effective. In several other cases, nothing was being spent on work sampling or critical incident studies. More balanced emphasis in manpower allocations should be given to functions which not only provide strength in the program, but also simultaneously monitor systematically.

In discussing monitoring, a difficulty in scaling, measuring or describing the role of a field safety engineer was reported. Later, a careful analysis of actual and possible roles not only clarified his present duties, but suggested key roles basic to planned audit of high energy functions, using a new, four-way viewpoint for audit: Is the unit (1) in the system? (2) complying with codes and practices? (3) impacted by safety program? (4) impacted by changes, delays, performance troubles, etc.? (See Figure 5-1 and Exhibit 16.) Subsequent trials supported the usefulness of the concept. Reports organized by the method were perceptive and forceful.

Figure IX-2

The audit schematic indicates that the field safety engineer will endeavor to assure the director and line management that a specific organizational unit has an adequate system and is not failing from four viewpoints.



Peer Committees. Special-purpose and on-going committees and boards are having great value at the three AEC research sites, as well as elsewhere. Not only is advanced technological skill utilized, but involvement has improved safety attitudes within scientific and engineering groups. Seemingly implicit in case histories of effective boards and committees is a positive, action orientation toward real-life problems. On-going groups sometimes bog down in lesser problems and many have histories of ineffectiveness. One measure of a safety program is the amount, quality and effectiveness of peer

committees at various levels.

Professional Staff.

The best description of the scope and functions of the professional safety position is contained in a statement adopted by the Board of Directors, American Society of Safety Engineers, October 22, 1966. It describes many aspects of the kind of safety system envisaged in this monograph.

Useful analyses of the organizational role of the professional are also provided by the observers from the British Chemical Industry and by Currie in his Safety Task Checklist.

The attitudes and concepts of effective safety directors about organizational, technical and behavioral concepts were shown to be different than those of less effective safety directors (Bracey, 1970). The study examined the strength and conviction of safety directors on organizational factors--position, management support and power--and technical (engineering) and behavioral variables. Effectiveness was associated with stronger convictions on both technical and behavioral variables, as well as position and power. However, management support scored low for all groups.

There are deep-seated problems in these and similar findings. For some years various top management men have commented privately on the seemingly mediocre (even poor) promotability of safety professionals (and even previously promising management trainees rotated through the safety function). Greenberg (1972) has commented forthrightly on the often low educational experience, promotability and organizational status of safety professionals.

Given the congruence of safety and general performance, and the excellent ASSE statement of scope and functions, such a situation seems strange. Safety engineers ought to be highly skilled and very promotable "trouble shooters" for the performance process.

Could the common mode of safety practice ("management by objection") be a factor?

Is a staff role in personnel too great a divorce from operational management?

Could the search-out and application of organizational techniques more congruent with management methods be a helpful factor in moving toward both lower accident rates and greater personal progress?

Does the basic task of simply applying codes, standards and regulations stifle and atrophy creative abilities?

Are unevaluated promotional gimmicks and stunts a disqualification for real-life performance measurement?

Safety personnel should be judged according to the usual management criteria, as well as safety criteria. Use of training opportunities, and creation of training opportunities is also a useful criterion.

Aspects of Practicability.

Trials at Aerojet produced encouraging cases of professional assimilation of improved methods--in accident/incident investigations, in production of fault-detecting schematics, in monitoring, in studies of major problems, and in building acceptance and management understanding.

There is a belief in some elements of NASA and AEC that a higher goal also requires "new kinds of people." These are not "in place of," but "in addition to" present safety staffs.

An examination of the safety staffs of NASA and AEC reveals that the professional staffs are already utilizing many relatively new specialized professionals drawn from:

1. Nuclear safety (or aerospace or system safety),
2. Health physics,
3. Industrial hygiene,
4. Fire safety engineering,
5. Human factors engineering and psychology,
6. Mathematics and system analysis,
7. Reliability and quality assurance,
8. Management (of many disciplines).

As an interesting fact, there is a significant number of biophysicists in the field. Thus, the observation that the work may need "new kinds of people" seems to be already evident in practice. In safety research areas, those active show a very wide spread in the sciences.

Staff Services.

The service concept and the proposition that "failure mirrors failure," articulated in Chapter 20, Management Implementation--specifically in Figure 20-4, page 197--are probably as powerful as any ideas in planned upgrading of the safety program and the safety professional.

The hierarchy of services outlined in Chapter 20 is a conceptual point of departure for safety program review. Initially, the concept of safety services can be applied in intensive investigations of major accidents. By way of example, the following questions can be used for the problems (immediate and distal) revealed by the investigation:

Research

1. What relevant research had been conducted or was in process in the safety unit? Elsewhere in the company? Outside the company?

Exchange of Information

2. What relevant exploratory or standards-setting meetings had been held? Were any state-of-the-art studies completed or under way?

3. Was relevant information on design criteria (e.g., past accidents) proffered during design? Would such information in digested or analyzed form have been quickly available if requested?

Standards and Recommendations

4. What codes, standards and recommendations were relevant? Were they known to process designers and planners? To operations personnel?

Training

5. What relevant safety training had been given to designers? Managers? Operators?

Technical Assistance

6. Same as 5.

Measurement of Performance

7. Had the planning process been audited? Deficiencies corrected?
8. Had the managerial process been audited and corrected?
9. What feedback on error had been provided to operators? Supervisors?

Looking forward, the question is how efficiently is the safety unit organized to economically produce such services at points of need? Levitt (1972) has argued effectively for a "production-line approach to service." Examples of such an approach would seem to be evident in several Aerojet arrangements;

1. The independent review system is intensive and sophisticated, but cheap and easy for customer use.
2. A specific illustration of the above is found in Exhibit 9 whereby review by the safety office is made more nearly comprehensive, predictable and producible at low routinized cost.
3. The provisions for low cost service, e.g., information search (page 262).
4. The field safety engineer's audit specified in Figure IX-2 is more nearly measurable and reproducible on a mass basis than the unstructured, variable search-out typical of the profession.

In short, a view of safety services as the essential output of the safety unit will allow us to replace high cost, variable and erratic elegance with lower cost, predictable products more nearly attuned to customer needs in the field, and more likely to deserve budget support.

* * *

In summary, a superior safety program will be moving away from crisis, "brush-fire" approaches toward:

1. Planned and measured programs,
2. Low cost, high volume safety services,
3. Professional growth evidenced by acquisition of management skills and modern methods.

The smaller the safety staff the more method is needed.

X. TRANSITION

A transition from "present best practice" in occupational safety to a higher level of practice having the possibility of an order-of-magnitude reduction in risk is a process of many changes--perhaps 50 or more concepts, if MORT is any measure. Such a change (or changes) is impossible and impractical if undertaken as a massive, directed effort. The transition could occur only if dozens of innovations were tackled on a "bite size" scale, found promising, and were persuasive and effective in an organization.

Why Bother? Because present "good" may not be "good enough." The pace of change may overwhelm us, with rising accident rates, and even disasters. The pace of safety improvement must keep up with social and technological change or the troubles most likely will get worse.

On the positive side, there's the potential of better management of safety and anything else.

How Much Transition? The process of transition to better programs can be visualized in at least four levels of effort:

1. Full-scale application to an organization,
2. Full-scale application to a major project,
3. Expedient application to current problems,
4. Personal use by the safety professional.

Each of these levels of effort will be discussed, but first some problem areas should be mentioned.

Some Problems. There are major problems which should be made explicit. They include, at the least:

1. The systems and technologies still need development and further technology acquisition.

The answer seems to be willingness to try out ideas, enlisting the broadest possible cross-section of the organization in the developmental effort to take full advantage of all competencies, and willingness to modify ideas based on actual trial experience.

2. The technology at this point seems complex.

One answer is simplification, of course; thus far the study effort has been encyclopedic in scope. Initial trials distilled and digested some concepts and principles. But the main answer is: keep specific projects simple and small.

3. Time and budget are restricted.

The effort must be in small, controllable increments, and the over-

all effort must be manageable, on a back out basis if necessary.

4. Keep the store open! The AEC sites have missions which demand good, continuous management for performance as well as safety.

The effort will have to involve small amounts of time of numbers of key people, and not disrupt the present, on-going and effective programs. However, the programs which have given AEC and its contractors, or similar industries, good records are not precisely defined nor are they "proven" (inasmuch as they have not been defined or evaluated in the detail suggestive of scientific proof). For example, the values of safety meetings were in question at all three MORT trial sites, but are continued without evaluation and with some indications of ineffectiveness. Trial of new approaches should not be very dangerous--what is dangerous is inertia.

At the same time, it is not wise to substitute new programs for old without temporary double-tracking. But, undue caution on innovation is probably as accident-producing as experimental failures, if incidents and lack of proof of present programs are considered.

Time taken from present program for innovation is always a potential problem. However, if innovation is to be rapid and effective, what is suggested is more small, clear-cut, incisive and quick trials, rather than potentially stifling adherence to traditional method.

As a matter of fact, the dynamic impetus for innovation may more than compensate for program transition, e.g., again, Job Safety Analysis which often stimulates the enthusiasm of employees.

5. Selling is always a problem.

The "innovation diffusion" techniques believed applicable to selling safer behavior can be used. Start with influential innovators and help them evaluate and test. No directives. Acceptance is easier in a stable environment. If the organization is in a state of change, e.g., a reorganization or a new location, wait for stable relations before working for more changes.

6. The concept of error at management levels will take some extra selling!

"Pacify" may be the complement to "simplify." People make mistakes--if they do anything. Maybe information or technology wasn't passed on--an oversight. Or perhaps time or other reasons prevent use--an assumed risk. Maybe the technology doesn't exist, or is just emerging; maybe imagination wasn't good enough by 20-20 hindsight. Live and learn, but let's learn. Objectivity about oversights and omissions is delicate and difficult, but the alternative is the present silence

in accident reports regarding possible management improvements, and consequently some misplaced safety efforts.

7. Competition with Safety Staff. Some objection to MORT projects has been encountered among safety professionals because, "When the concepts are implemented line management and technology groups will have a major share of the safety job." This seems as intended, at least by the author, but the possible objection should be noted.
8. Reading a book or training a few people will not bring about transition.

Dialogue, leadership, a catalytic agent and technical assistance are needed.

Full-Scale Application to Organization

The following general approaches seem worthwhile:

1. Many, small exploratory, permissive, self-adapting projects.
2. A small amount of time (say 4 or 5%) of numbers of people to develop better managers, better problem solvers with safety as content.
3. Maintain an experimental orientation (but not hard-nosed research at this time--too costly and too many years for rigid proofs). This is a trial of a possible synthesis. Move to research evaluation when earlier trials suggest value.
4. Breakthrough is sought--use Juran's management guidelines for this process.

Some requirements for a trial application seem to be:

1. At a site--
 - a. A management team that wants to try out new approaches.
 - b. A focal point for stimulation and any needed coordination in a close associate of the top manager.
 - c. A focal point for technology acquisition and trial close to the safety director. Transition cannot be staffed by already busy safety people. In effect, a New Program Development Unit must be created, and staffed full or part-time with innovation-minded, creative people.
2. At the AEC Operations Office--a management innovator.
3. At AEC Headquarters--
 - a. Bright, young, technology acquisition people--technical assistance from the national level will be needed.
 - b. Budget and staff for national problems (e.g., information systems).

Given these approaches and requirements, a great deal of progress should be apparent in twelve months.

All good plans will be local plans. But an outline based on Aerojet trials may be helpful in preparing a good local plan.

I. A preliminary evaluation of needs and interests. Perhaps a briefing of key people.

II. Management endorsement of a study--plus assignment of a study team, at least one from management and one for safety.

III. Study and Plan

1. Review and compare present program against MORT standards,
2. Plot major, apparent or likely needs against some broad headings (e.g., the Safety Program Improvement Project list in Exhibit 17 or use the Table of Contents of this text). Rank order possible projects under each major heading.
3. Select a limited number of priority projects, such as:

Hazard Analysis Process. Try comprehensive information search on several new projects.

Work Flow Process. Try Job Safety Analysis.

Monitoring Systems. Try a "critical incident" study in one major high energy area. Try an audit of an upstream process (e.g., engineering).

Accident Investigation. Try MORT analysis on the next few serious incidents or accidents.

Probably a few more such projects will suggest themselves.

4. Prepare a brief description of each project.
5. Plan to spread the work--i.e., the safety engineers assigned to try MORT may not be the ones who help start JSA.
6. Consider whether projects are to be spread through the entire organization, or tried in the area of one, very interested manager. (The latter was Aerojet's approach.)
7. Prepare a plan. Include a Steering Committee and a Technical Committee.
8. As possible, let timing be flexible. It's good to start a project after an incident shows need.

IV. Obtain management approval, including the appointment of a MORT Team--at least one close associate of the manager of the area of study, and at least one from the New Program Development Unit.

V. Go to work.

Full-Scale Application to a Project

Select a major project--such as a new plant or process.

Compare the project plan with MORT to see what needs to be done.

Provide staff for the MORT analysis, if project staff cannot do the work.

Keep a docket on work, costs and perceived benefits.

Keep records on deviations from plans--cost or schedule over-runs, rework, delays due to poor plans, accidents, etc.

Compare the record with scheduled and actual performance for two or three previous, comparable projects.

Expedient Trials

Compile a list of major problems in the organization.

Try MORT analysis on some of the most difficult problems.

However, be warned that conclusions based on MORT may not be accepted by managers of even a high energy process or machine, unless there's been trouble. If a stable system has been operating well, incident reports from a broader experience base will be needed to convince managers of the nature of troubles and the need for controls.

Or, as an alternative:

1. Identify the managers who are Innovators.

Among these which have problems?

2. Other managers with serious problems?

3. Roughly grade the whole organization on MORT diagrams.

4. Select a limited number of SPIP's.

Perhaps: 1. Analyze one serious accident with MORT

2. Step up one Hazard Analysis Process (follow the book!)

3. Do a small critical incident study in one place

4. Start or extend JSA

5. Make a monitor plan for a hot spot

6. Start the PPL

Personal, Professional Use

If organizational trials of MORT are not feasible, use MORT as one guide to growth:

1. Review MORT to see how much you accept. Where you disagree, jot down your contrary views.
2. Use MORT to analyze a problem or an accident (use GETTING STARTED recipe on page 23).
3. Use MORT to classify new methods ideas in the current literature.

Appendices

APP.

- A. Early MORT Analyses
 - 1. H I L A C
 - 2. Environmental Chamber
 - 3. HE Press
 - 4. MAPP Gas
 - 5. Falls
 - 6. Initiators
- B. A Few Useful System Concepts
- C. Example of Analysis of Value Aspects of Alternatives
- D. Discussion of Critical Incident or Incident Recall Techniques
- E. Sample data on error rates
- F. Procedure Review Criteria
- G. Participation and Motivation
- H. Innovation Diffusion
- I. Acceptance of Proceduralized Systems at Aerojet
- J. Modified Air Force Accident Investigation Checklist
- K. NSC Symposium on Measurement of Industrial Safety Performance

The "High Level Spill at the HILAC" was extremely useful as an initial trial of the MORT method because an excellent and detailed report had been prepared and published by Lawrence (Garden, Dailey, 1959). Further, the case illustrated the interaction of two different kinds of energy, and the concept of successive barriers.

For necessary background, excerpts from the report are provided:

"**ABSTRACT.** On July 3, 1959, an incident occurred in the Hilac Building when the turning of the wrong valve resulted in pressurizing a helium cooling box, with a resultant 'blowout' of a thin foil. The burst of He gas disintegrated experimental foils made up with 10^{11} dpm of Cm^{244} . The resultant activity was quickly dispersed as airborne particulates throughout the building. The 27 people in the building were evacuated within 10 minutes under surveillance of the Health Chemistry personnel; wherever clothing proved to be contaminated it was removed, and in cases where nose swipes were pertinent they were taken.

"Although an assumption of a combination of the worst conditions could conceivably have resulted in 1 man's inhaling between 2 and 4 times the calculated allowable inhalation for short bursts, evaluation from air analysis and medical tests indicate that it is unlikely that anyone actually did receive this amount.

"The building was closed during decontamination procedures, which required about 30 people for 3 weeks in direct decontamination work and 30 people for 3 weeks in indirect work.

"The cost of labor, material and other charges related to the spill amounted to about \$30,500 without overhead; equipment loss was held to less than \$2000. The lost time of operation of the hilac has been evaluated at \$26,000, so that the total loss from the incident amounts to roughly \$58,500.

"The primary cause of the accident has been determined to be an error by the experimenter. Steps have been taken to help insure against any recurrence of an uncontained radiation spill at the hilac, and to decrease the danger of exposure to personnel in the event that a spill should occur in the future."

"**CONCLUSIONS.** It is clear that the primary cause of the hilac curium spill was an error by an experimenter at the hilac. Failure to operate certain valves properly caused an overpressure on a 0.1-mil nickel foil 'window' of a helium cooling chamber, so that it ruptured; the resultant outrush of helium shattered and dispersed the curium target that was just outside the chamber.

"It should be pointed out, however, that the chamber that blew out contained two foil windows of identical type - one separating the atmosphere from the helium and the other separating the helium from the accelerator tank vacuum. In all previous ruptures, the foil on the vacuum side was involved, since

*HILAC = Heavy Ion Linear Accelerator

it is always under one atmosphere higher pressure than the other foil. The result in such a case is a small explosion into the tank, so that the target is not affected. That the foil at the much lower pressure differential failed in this spill indicates a very unusual situation.

"The cost, for which an upper limit of \$58,500 has been given, is regrettable and serves to indicate the financial justification for carefully implemented operating procedures and, where possible, design of experimental equipment in such a way that mistakes cannot result in spills. The time lost to research -- three weeks -- is also an important consideration.

"Although the field of research is one for which it is admittedly very difficult to set down routine-type safety procedures, the foregoing information makes it clear that it is incumbent on the Atomic Energy Commission, the Lawrence Radiation Laboratory, and the researcher himself to insure that everything possible is done to prevent an occurrence of this nature. This means that the research programs should be reviewed carefully for possible improvements in health and safety measures, and that all possible efforts should be made to carry out suggestions made by the appropriate groups.

"The investigating committee commends the personnel of the hilac for prompt and effective action following the spill, and the members of the Health Chemistry department for the efficiency and thoroughness with which the radiation problems were handled. In particular, the Decontamination Team is to be commended for substantially reducing both the loss in research time and the cost of unusable equipment by painstaking efforts and by application of advanced decontamination techniques."

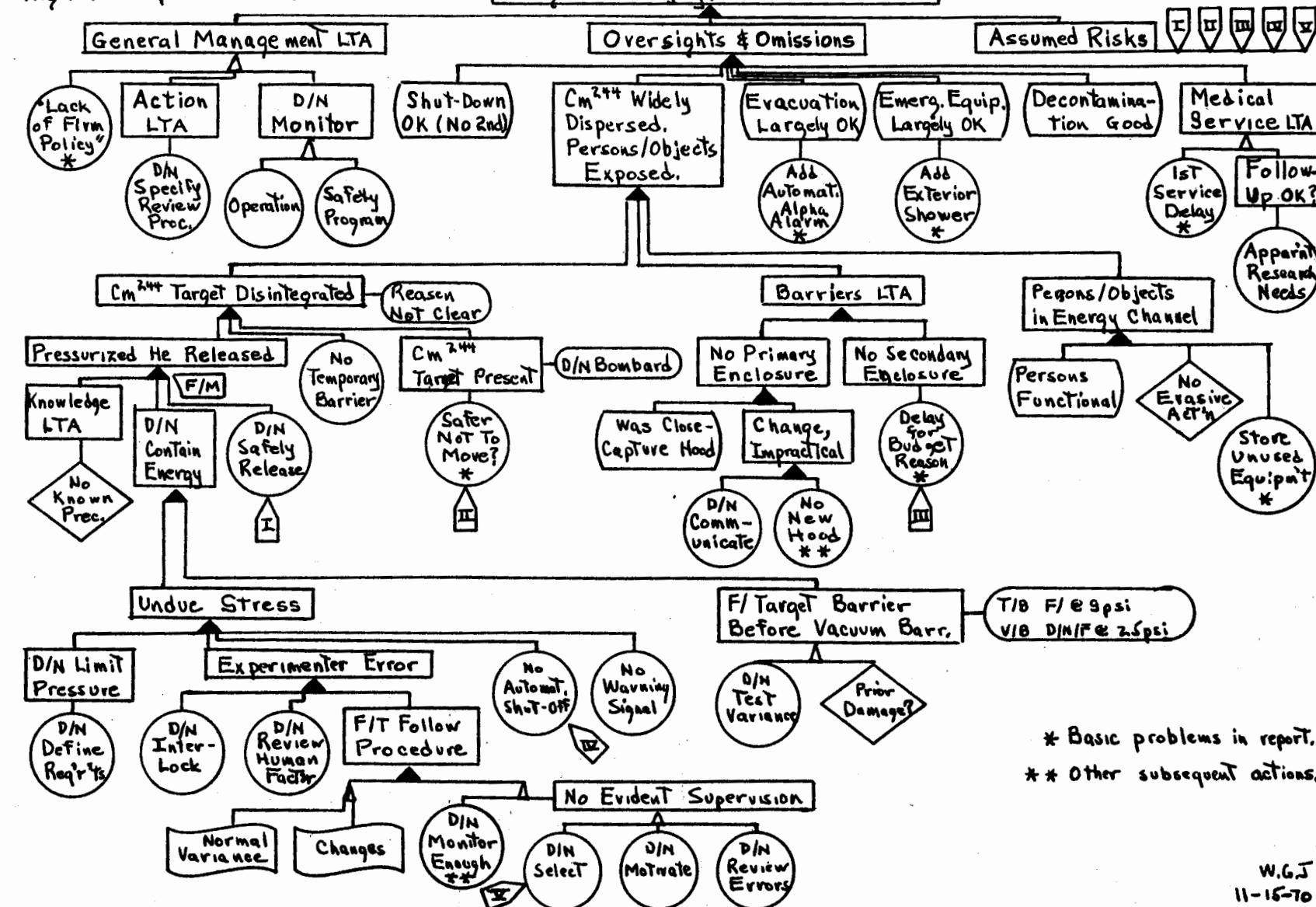
"RECOMMENDATIONS.

1. A more clearly defined and forceful attitude regarding health and safety measures should be evidenced. The magnitude of contamination from this spill can probably be attributed, at least in part, to lack of firm policy.
2. Arrangements for obtaining the services of a physician quickly in case of a radiation incident should be made more workable. Although procedures have been set up for such an emergency, about an hour and a half elapsed before an M.D. could be reached for advice.
3. There should be more storage space for apparatus not being currently used. The presence of large amounts of extraneous equipment in the experimental areas greatly complicated the task of decontamination. Good house-keeping practices should be conscientiously enforced.
4. A shower with catch basin should be provided near an exterior door of the building for removing surface radioactive contamination from personnel involved in spills. The existing shower is designed for removal of chemicals and was in the area of greatest contamination. Hilac personnel found it necessary in this case to travel more than a quarter of a mile to shower.
5. An automatic alarm system actuated by an alpha air monitor should be installed.
6. Primary enclosures, i.e., enclosures around individual pieces of experimental equipment containing radioactive materials, should be provided.
7. Secondary enclosures should be provided to isolate reasonable work areas. These areas should be individually ventilated."

In the Hilac Tree Figure the RECOMMENDATIONS of Lawrence were keyed by *. Additional actions later taken by Lawrence were keyed **.

Mort
"High level Spill at HILAC"

Certain Costs, \$ 58,500; Others Substantial
Long-Term Injury? Research Time lost



* Basic problems in report.
** Other subsequent actions.

W.G.J
11-16-70

Notes for Tree on High Level Spill at the HILAC

(1) The consequences, as estimated, did not include medical treatment costs and overhead which would be substantial. The possibility of long-term radiation damage to personnel could not be excluded. And, the research consequences were not fully measured by down time.

The event could occur only because (2) General Management was "less than adequate," (3) there were Omissions and Oversights, and/OR (4) there were Assumed Risks.

(2) General Management was "Less Than Adequate" (LTA) because there were three problem areas:

- (a) "Lack of Firm Policy" as noted in report
- (b) Action -- i.e., did not specify a hazard review procedure.
- (c) D/N Monitor:
 - (i) General operations to detect error or problem sources
 - (ii) The safety program itself.

These are OR events -- any one can lead to trouble.

(4) The Assumed Risks are transferred from Omissions and Oversights whenever a decision is made that a solution to a problem is not available or is impractical. Normally such decisions are management decisions, but in this case the experimenter was allowed to assume risks for management.

(3) The first level of analysis of events which determined outcome covers an ameliorative stage after the accident occurrence (4). Most events were o.k., but a few problems were identified.

(4) The Cm^{244} could result in exposure because all three (AND gate) events occurred:

(5) Persons/Objects were present (persons functional; some objects not functional) and no evasive action was possible.

(6) Barriers were LTA because:

- (a) The primary enclosure was made impractical by a Change, and no new

hood was constructed, because (a1) the experimenter did not communicate and (a2) the Health Chemistry group did not monitor continuously.

(b) A separate exhaust for this cave's air was postponed due to "end of the fiscal year" reasons -- an assumed risk.

(7) The target disintegrated (reasons not clear) when it was struck by pressurized helium. A temporary barrier was theoretically possible since the target was not to be bombarded.

(8) The highly radioactive target was left in place as a so-called safety measure (which could be questioned) -- another assumed risk.

(9) The pressurized helium could be released toward the target because there was (a) no known precedent for such an event, and (b) there was no safe release, e.g., a rupture disc at <9psi, and pointed away from target. Since such release may not be practical, its absence becomes another assumed risk. A general Failure to Monitor and Review experiments (F/M&R) is noted.

(10) The equipment did not contain the energy because there was undue stress (11) and because the target barrier failed at 9 psi while the vacuum-side barrier did not fail at 25 psi. If this sequential failure of barriers was to have worked, the range of variability of the foils would have to be tested. Or, there may have been prior damage to the foil which failed (a lack of information). Knowledge LTA occurred because of no known precedent. There may have been an additional failure in the knowledge area -- namely, to communicate or specify the principles represented by pressure vessel codes; in view of potentials, the principles were applicable, even though the pressures were nominal.

(11) Undue stress occurred as the result of a combination of four failures (an AND gate)

(12) Did not limit the pressure available, presumably because of failure to define the maximum pressure needed; therefore no control of supply or no regulator, or both.

(13) The apparatus had no sensor and automatic shut off -- presumably

another assumed risk.

(14) There was no audible and visible signal.

Note -- (13) and (14) should be shown at the left of Experimenter Error since the Hazard Reduction Precedence Sequence places these devices ahead of human error.

(15) The experimenter error (opened supply and purge valves; then closed purge valve and D/N open return valve) could occur because the valves were not interlocked, and there had apparently been no human factors review which might minimize error. In addition, there had been previous similar experimenter errors, without analysis and correction.

(16) The human error would occur because there was expectable human variance OR expectable change in persons or interruptions, AND lack of supervision or adequate monitoring.

(17) The "lack of evident supervision" seems apparent from:

(a) The lack of selection criteria for functions -- i.e., experimenters selected for scientific capability, rather than mechanical reliability, and no offsetting provision of operators or a "second man," — a risk is assumed in the process.

(b) A lack of safety motivation in the experimenter seems apparent.

(c) Prior errors of the same type were not detected and therefore not reviewed.

(18) Monitoring by Health Chemistry was later stepped up to a more or less continuous basis.

The HILAC Tree illustrates how two or more sources of energy can be analyzed for barriers between.

Any problem not marked * or ** is a problem made explicit by the tree analysis -- there are sixteen such problems. Some might be impractical to solve, in which case they become assumed risks.

A1 - 7

Outline Form of Tree for High Level Spill at HILAC

Certain costs, \$58,500; others substantial.
Long-term injury? Research time lost.

S. Oversights and Omissions

AR. Assumed Risks

G. General Management LTA

S. Oversights and Omissions

SA1. Cm244 widely dispersed; persons/objects exposed

SA2. Amelioration

a. Shut-down o.k. (No 2nd)

b. Evacuation largely o.k.

1. Add automatic alpha alarm*

c. Emergency equipment largely o.k.

1. Add exterior shower*

d. Decontamination good

e. Medical Service LTA

1. 1st service delayed*

2. Follow-up o.k.? Apparent research needs.

SA1. Cm244 widely dispersed; persons/objects exposed

SB1. Cm244 target disintegrated - Reason not clear

SB2. Barriers LTA

a. No primary enclosure

1. Was close-capture hood

2. Change made it impractical

(a) D/N communicate change

{b} No new hood**

b. No secondary enclosure

1. Delay for budget reason* ----- Assumed Risk III

SB3. Persons/objects in energy channel

a. Persons functional

b. No evasive action possible

c. Store unused equipment elsewhere*

SB1. Cm244 target disintegrated

SC1. Pressurized He released

SC2. No Temporary Barrier

SC3. Cm244 target present - D/N bombard

a. Safer not to move?* ----- Assumed Risk II

SC1. Pressurized He released

a. Failure/monitor

SD1. Knowledge LTA

a. No known precedent

SD2. D/N contain energy

SD3. D/N Safely release ----- Assumed Risk I

SD2. D/N contain energy

SE1. Undue stress

SE2. F/target barrier: F@9 psi; vacuum barrier D/N F@ 25 psi

a. D/N test variance

b. Prior damage?

SEL. Undue Stress

- SF1. D/N limit pressure
a. D/N define requirements

SF2. Experimenter error

- SF3. No automatic shut-off ----- Assumed Risk IV
SF4. No warning signal

SF2. Experimenter error

- SG1. D/N interlock
SG2. D/N review human factor
SG3. F/T follow procedure

- a. Normal variance?
b. Changes?
c. D/N monitor enough**
d. No evident supervision
(1) D/N select ----- Assumed Risk V
(2) D/N motivate
(3) D/N review errors

AR. Assumed Risks

- I. D/N safely release He pressure
II. Safer not to move Cm244 target
III. Secondary enclosure delay for budget reason
IV. No automatic shut off He pressure
V. D/N select experimenter for operational reliability.

G. General Management LTA

GA1. "Lack of firm policy"*

GA2. Action LTA

- a. D/N specify review procedure

GA3. D/N Monitor

- a. Operations

- b. Safety program

* Basic problems in report

** Other subsequent actions

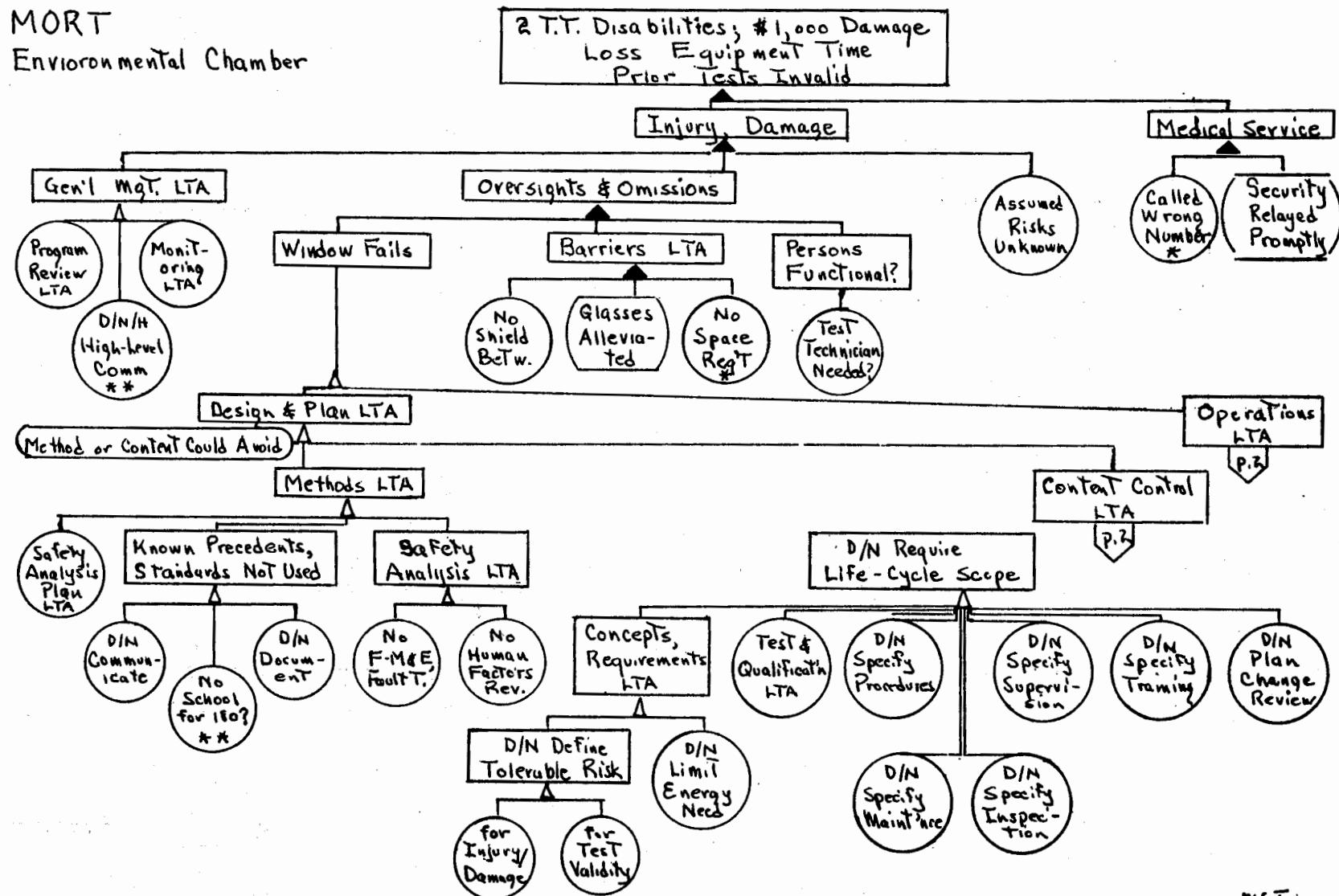
Environmental Chamber

The explosion of an altitude chamber resulted in temporary total disabilities to two employees and \$1,000 damage. The accident could easily have produced fatal injuries.

Excerpts from two standard Form 92 reports on the injuries and a Form AEC-283 report on the damage show as follows:

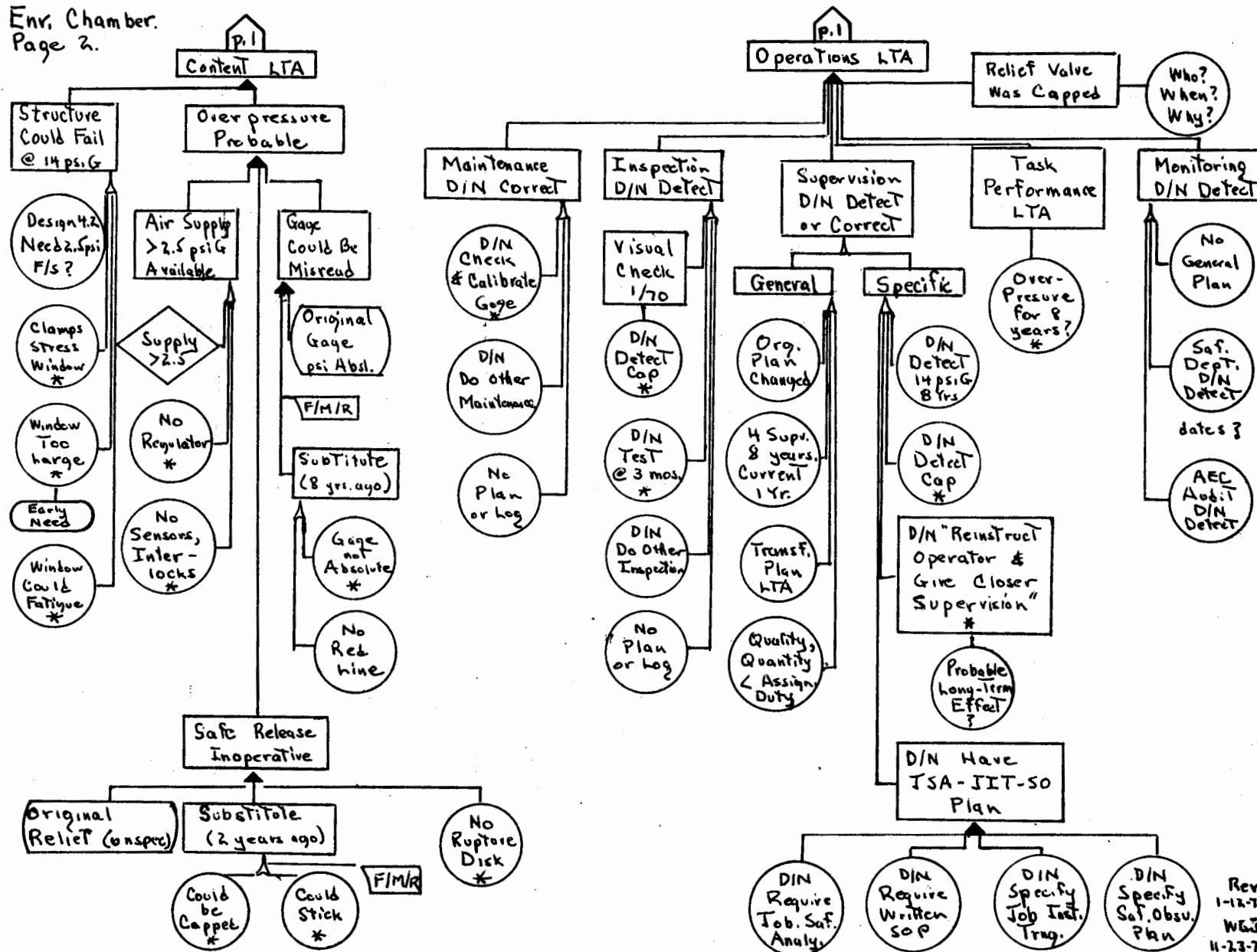
1. "Requirements called for testing electronic equipment at pressure corresponding to sea level and 250,000 feet altitude."
2. "Employee was observing test of electronic receiving unit in a pressure-altitude chamber to provide sea level pressure. Operator erroneously overpressurized chamber beyond its rating and 38" x 38" x 1 1/4" tempered glass front blew out of chamber, and pieces of it struck employee."
3. "A pressure of 14.7 psi gage was being applied instead of 14.7 psi absolute (2.5 psi gage). The chamber was designed to hold 4.2 psi gage at this altitude."
4. "The pressure was being increased gradually from 12.2 psi absolute to 14.7 psi absolute. When approximately 14.0 psi gage pressure was reached, the door frame and glass ruptured."
5. "Lack of proper instructions. Personnel were not aware of the difference between gage and absolute pressure. Safety pressure relief valve had been sealed shut."
6. Preventive action:
 - (1) "A manometer indicating pressure in terms of feet and mm will be installed on each chamber."
 - (2) "Pressure switches will be installed which will shut off air supply at a predetermined pressure."
 - (3) "Factory set and sealed pressure relief valves will be installed."
 - (4) "Vacuum/pressure rupture discs will be installed."
 - (5) "Consideration will be given to replacing pressure regulator valves with an improved type."
7. Additional action:
 - (1) "All tests involving altitude chambers will be reviewed and evaluated by a responsible engineer in charge of the equipment."
 - (2) "All operators of altitude chambers will be retrained in gage pressure, absolute pressure, and altitude concepts."
 - (3) "Personnel will be directed not to place themselves in front of doors or viewing ports of altitude chambers."

MORT
Environmental Chamber



WGS
Rev. 1-12-71 11-23-70

Env. Chamber.
Page 2.



A2 - 3

Rev
1-12-71
WGU
11-23-70

8. "New pressure monitors are being obtained, pressure relief devices are being installed, and each setup will be reviewed by the project leader.

"Meetings with responsible organizations are being held to determine appropriate Laboratories-wide system for R&D pressure vessel safety. A letter is being issued by the Safety Engineering Department to all technical organizations, reviewing incident and making safety recommendations that are applicable to hazardous tests."

A detailed internal report provided additional information, such as:

1. Difficulty in getting equalized pressure on clamps around door.
2. Ten years of operation may have overstressed and fatigued glass.
3. Switched gauge about eight years ago from absolute pressure to gauge pressure.
4. Two years ago the pressure relief valve was changed. A spring type refrigerator valve set at 14.6 psi was modified to relieve at 5.0.
5. The equipment was visually checked about five months earlier.
6. No one knows when or how relief valve was capped.
7. In a subsequent test the valve did not open until 240 psi was reached, and later opened at 57-60.
8. In the future reliefs and sensors should be checked at three month intervals.
9. Gauges should be checked and calibrated "frequently and periodically."
10. Viewing ports should be of minimum size.

At a later date a three-day training session in pressure vessel safety was conducted for 180 people.

The accident is graphically analyzed in the Exhibit attached.

Any basic problem (circle) marked * is a problem identified in the reports.

Any circle not so marked is a problem raised by this analysis.

The analysis on page 1 seems to require little comment.

On page 2 the left hand section, Methods Less than Adequate, reflects the apparent lack of system safety programs which could control events of this nature on all types of equipment.

In the Methods Section is noted the school subsequently conducted. In the absence of a prescribed hazard review procedure, a series of schools on all major hazards is an approach of questionable effectiveness. The solution to this type

of problem seems to lie in review procedures which bring events of interest to the attention of a small group of competent people. Mass education is likely to have only limited value and effect, and for only one special problem.

In the section on "Content Control" on page 2 it will be noted that almost all of the deficiencies noted were reflected in the reports.

On page 3 we again see systemic deficiencies of which the specific accident was only symptomatic. Specifically, a general lack of effective maintenance and inspection plans, and point-of-operation logs is suggested by this accident.

The role of the supervisor is inadequately examined in the reports -- this means the institution of supervision, not the man. To wit, it is suggested that training and time may be inadequate for assigned functions.

Most important -- in the absence of a JSA-JIT-SO sequence implemented organization wide, the effect of such platitudes as "reinstruct operator and give closer supervision" will have minimal, short term effect for this operation — and no effect whatsoever at the locus of the next serious accident.

Basically, the analysis suggests that the safety system is in need of improvement, whereas the conventional reports are so constructed as to focus on the specifics of the event.

The site complied with AEC reporting procedures. The reporting procedures are inadequate because they do not suggest or imply that the general safety system may be in question or doubt. The next failure of similar severity may be in an entirely different content or subject matter field.

A3 - A4 - A5 - A6

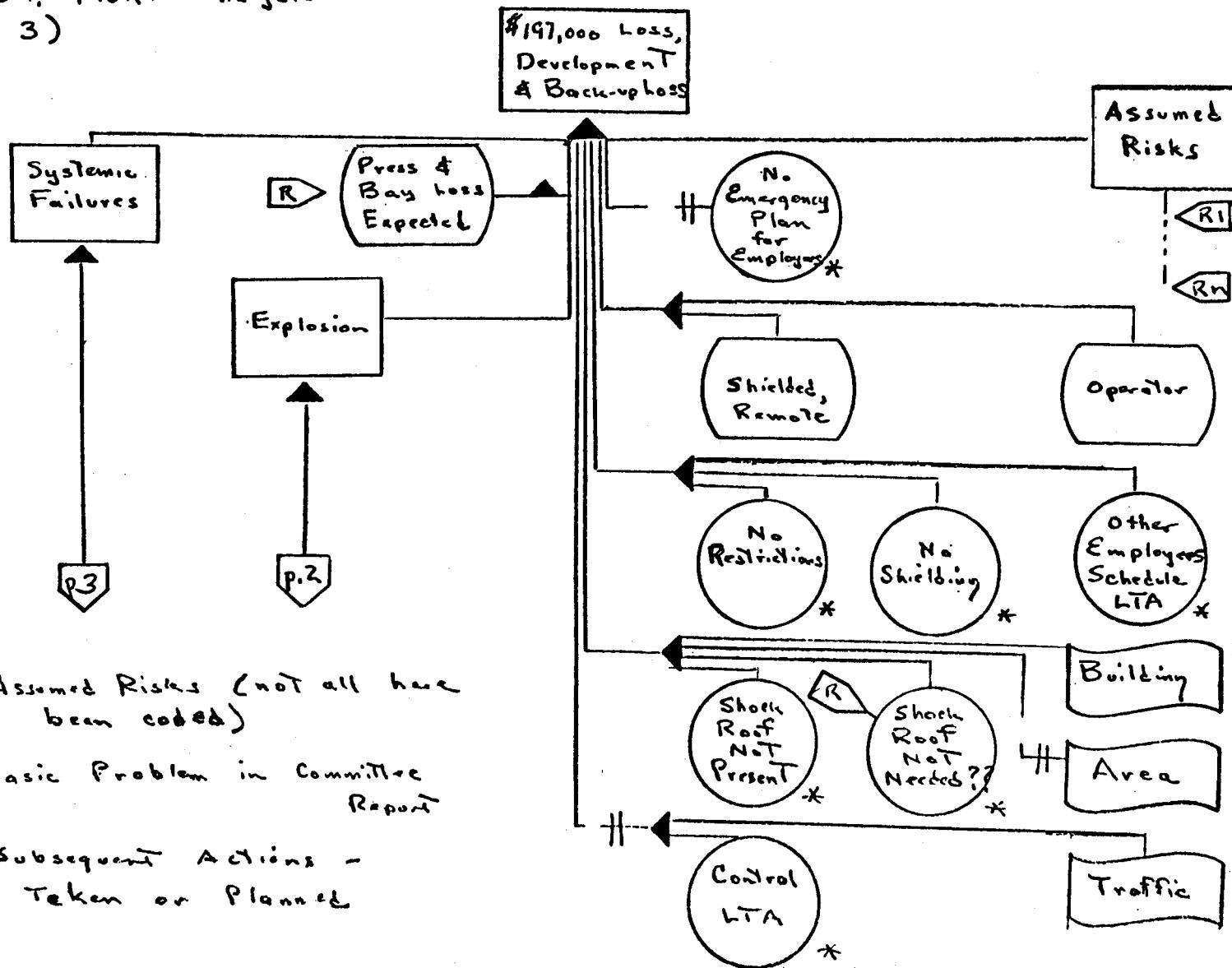
Brief Summaries of Four Cases

- A3 HE Press Press was used to compress high explosives. The mushroom plate seal was omitted by error by a previously reliable operator. Fluids extruded through threads and a hole, then the sac enclosure, extruded, then the HE extruded, was heated and exploded. The operator was in a remote, shielded area; other employees were not. Despite lack of control of adjacent traffic, no harm was done to traffic. The operator had a personal problem--wife seriously ill. The report shows a recommendation to reinstruct without any reasoning or analysis as to why such retraining might have effect. A common recommendation--enforce--is made even though failure was not detected!
- A4 MAPP Gas Liquid gas was being transferred from a supply to a cylinder by two experimenters.
- A5 Falls Two almost identical falls from sloping roofs.
- A6 Initiators Explosives initiators were being modified. Employee was the one who gave safety instruction for this kind of work. The static-free room had other use intermittently, and had been modified.

HE Press Explosion

on 12/26/69

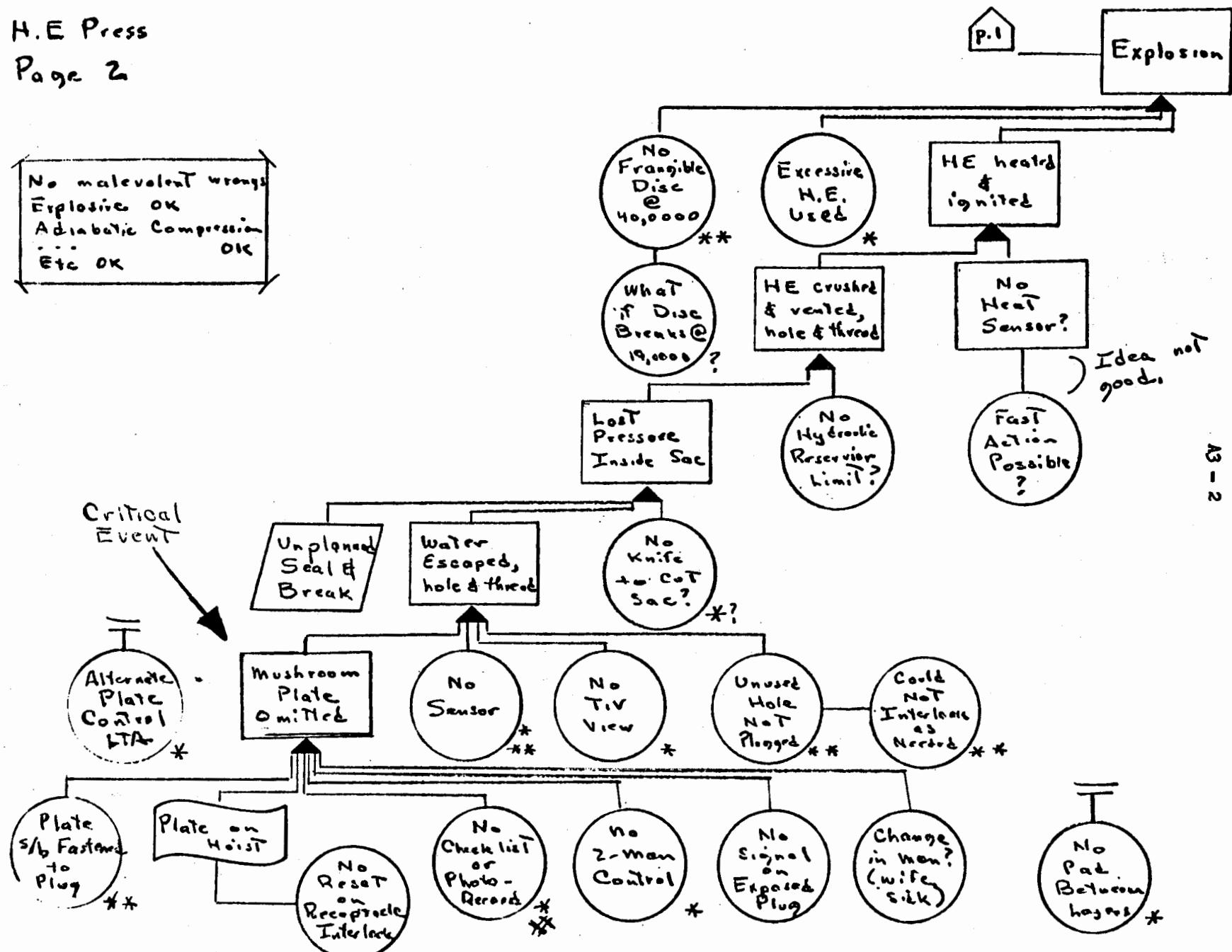
Page 1, MORT Analysis
(of 3)

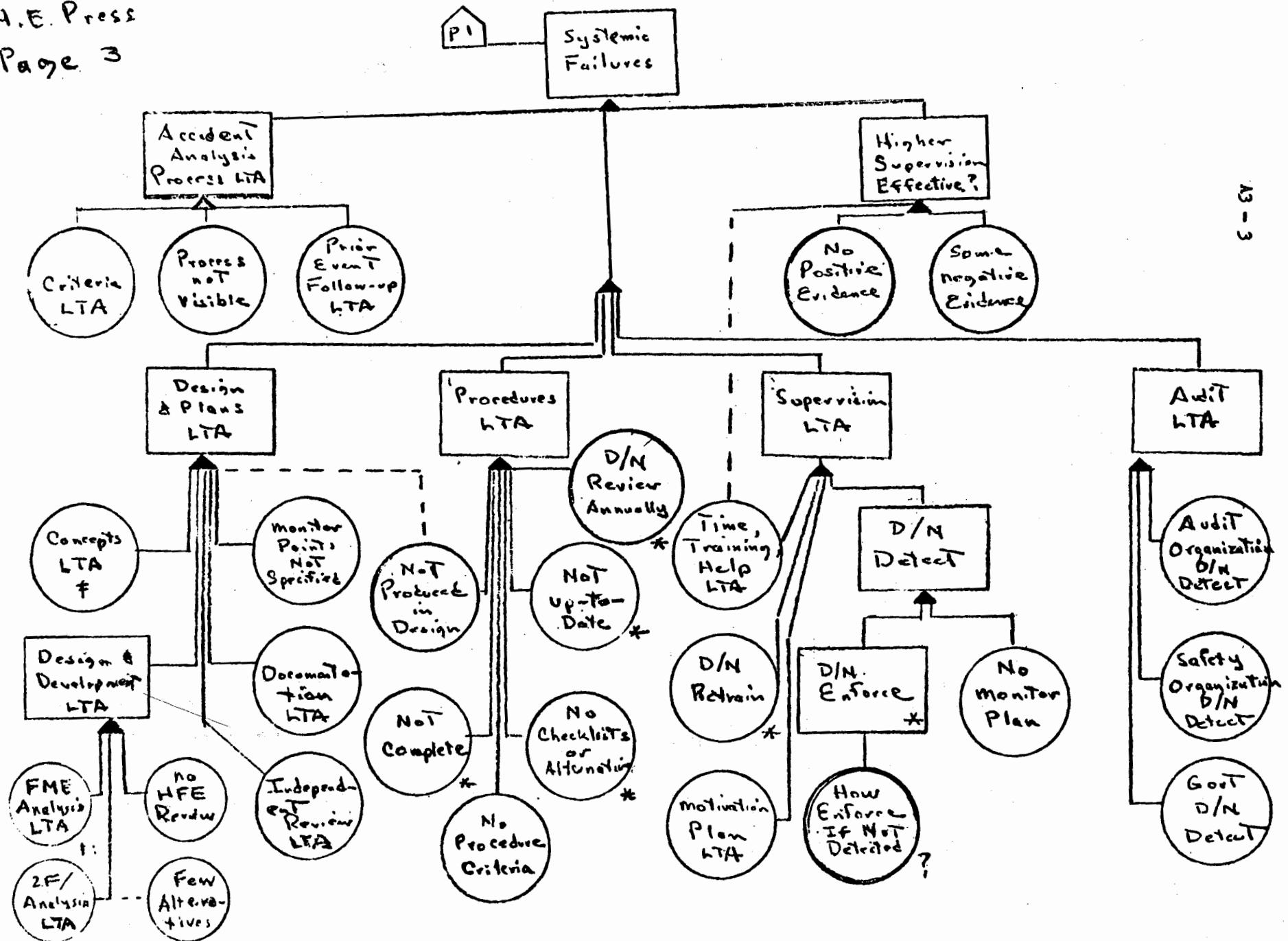


H.E Press

Page 2

No malvolent wrongs
Explosives OK
Adiabatic Compression
OK
Etc OK





Footnotes to Case A3

Why not a push-button checklist for catastrophic potentials which has time-lag interlocks to not permit further operations to be performed? (In other words, the computer won't let you proceed, so you have nothing to do while waiting except perform required step!) Then, for redundancy, interlock hardware and computer! We need more "black boxes" for really high potential failures.

D/N restrict press to one operation

Poor criteria for roof need

D/N estimate life cycle exposure

D/N estimate life cycle error rates

D/N estimate life cycle risk acceptance

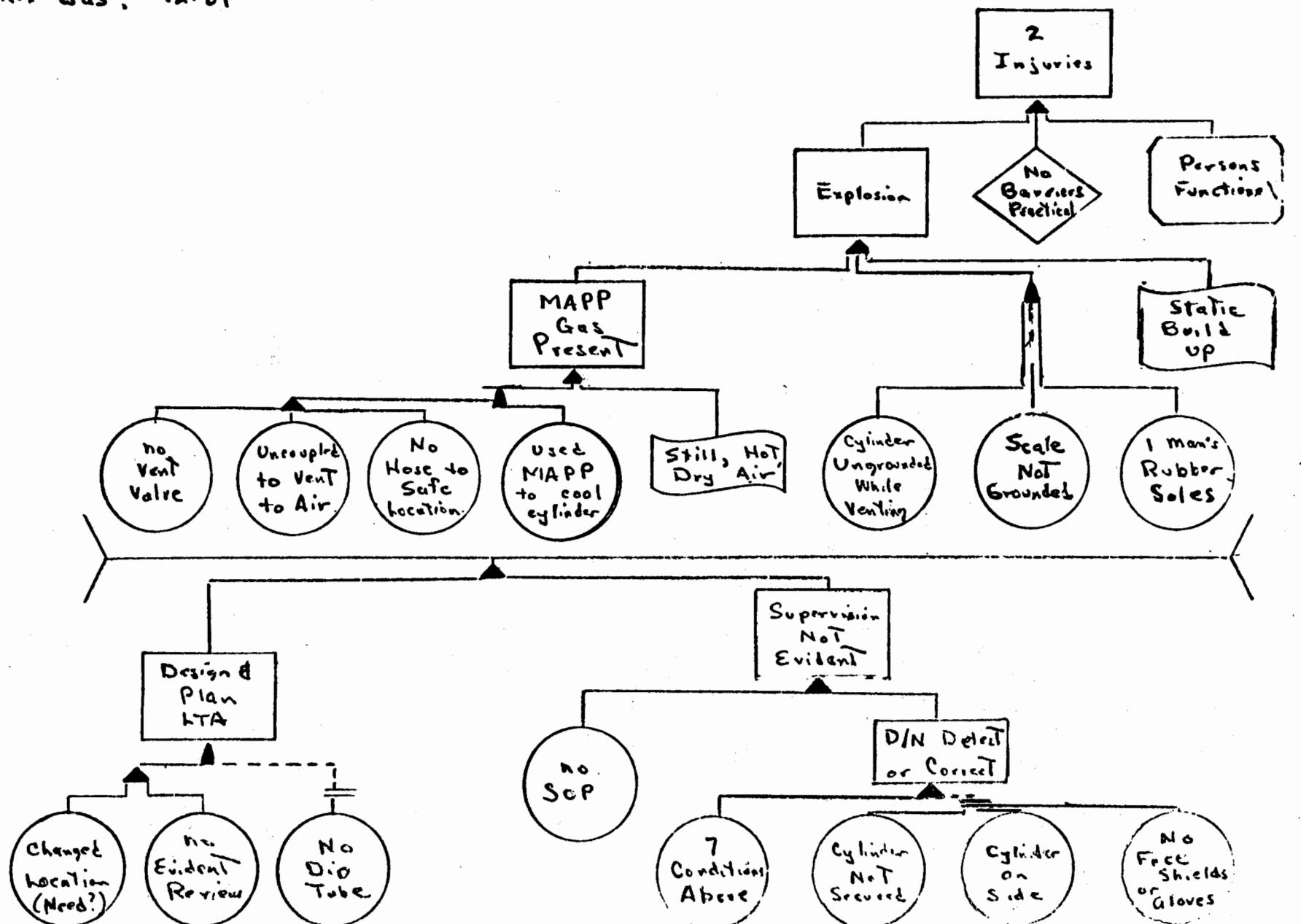
No Failure-Mode-and-Effect Analysis

No Two-Failure Analysis

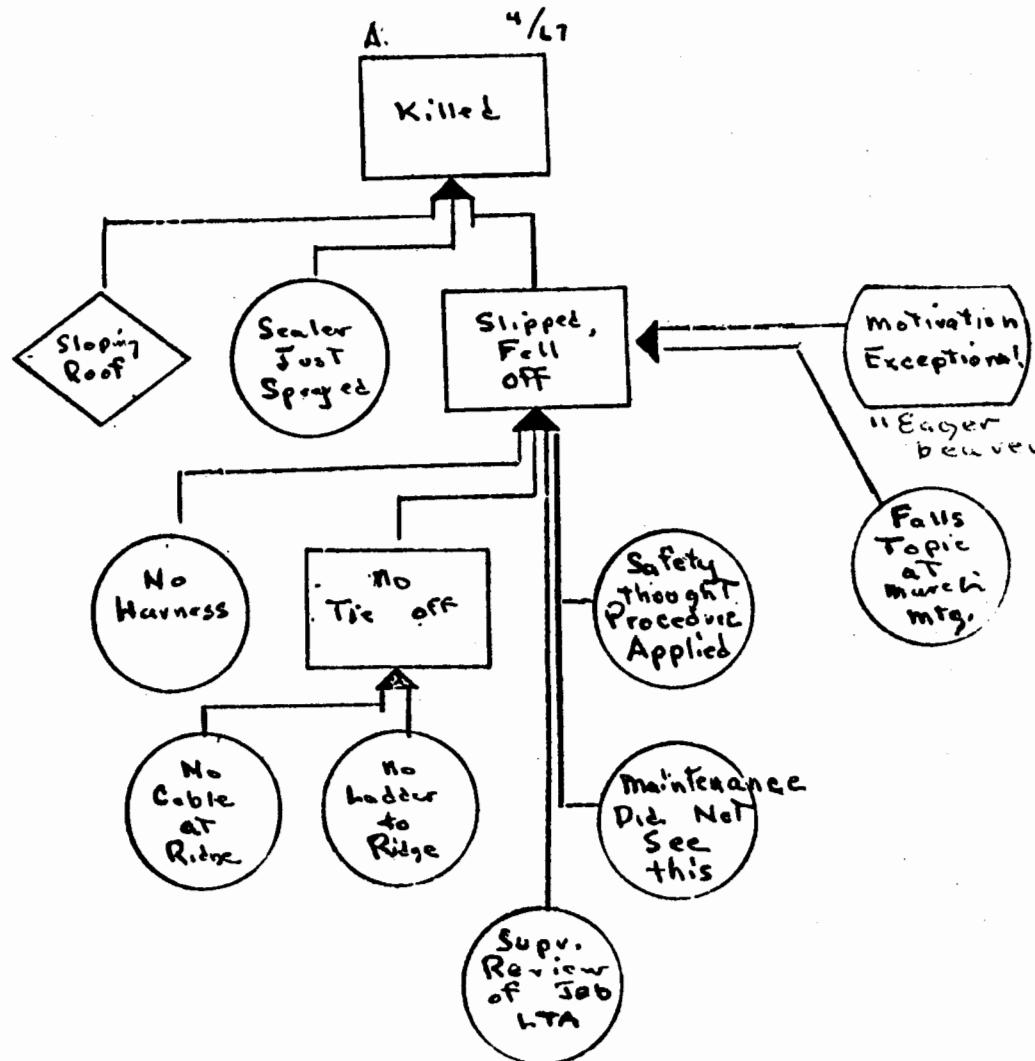
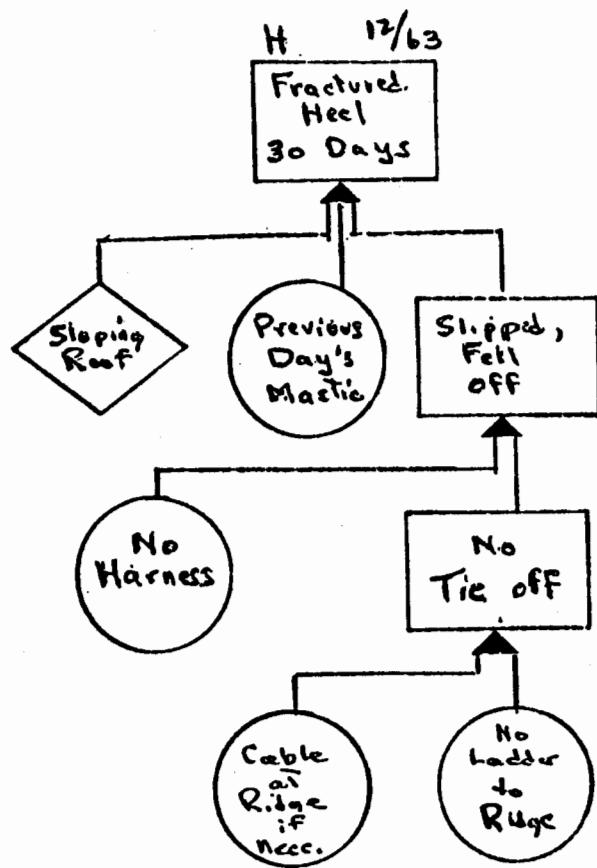
.:. Inadequate alternatives of controls and redundancy.

(On-the-right) No Human Factors Review of Error Potential.

MAPP Gas, 8/12/69



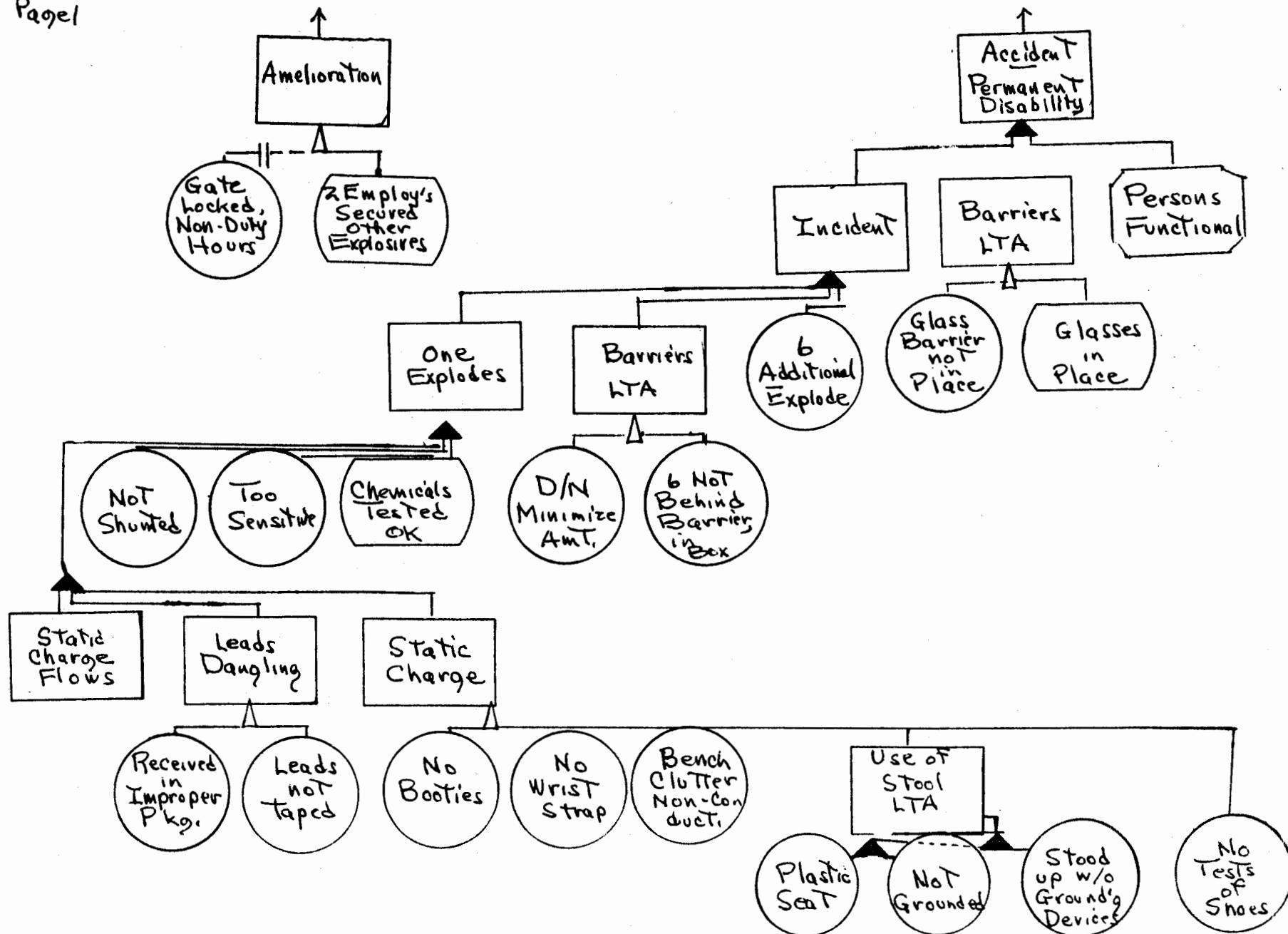
Sequence of Falls



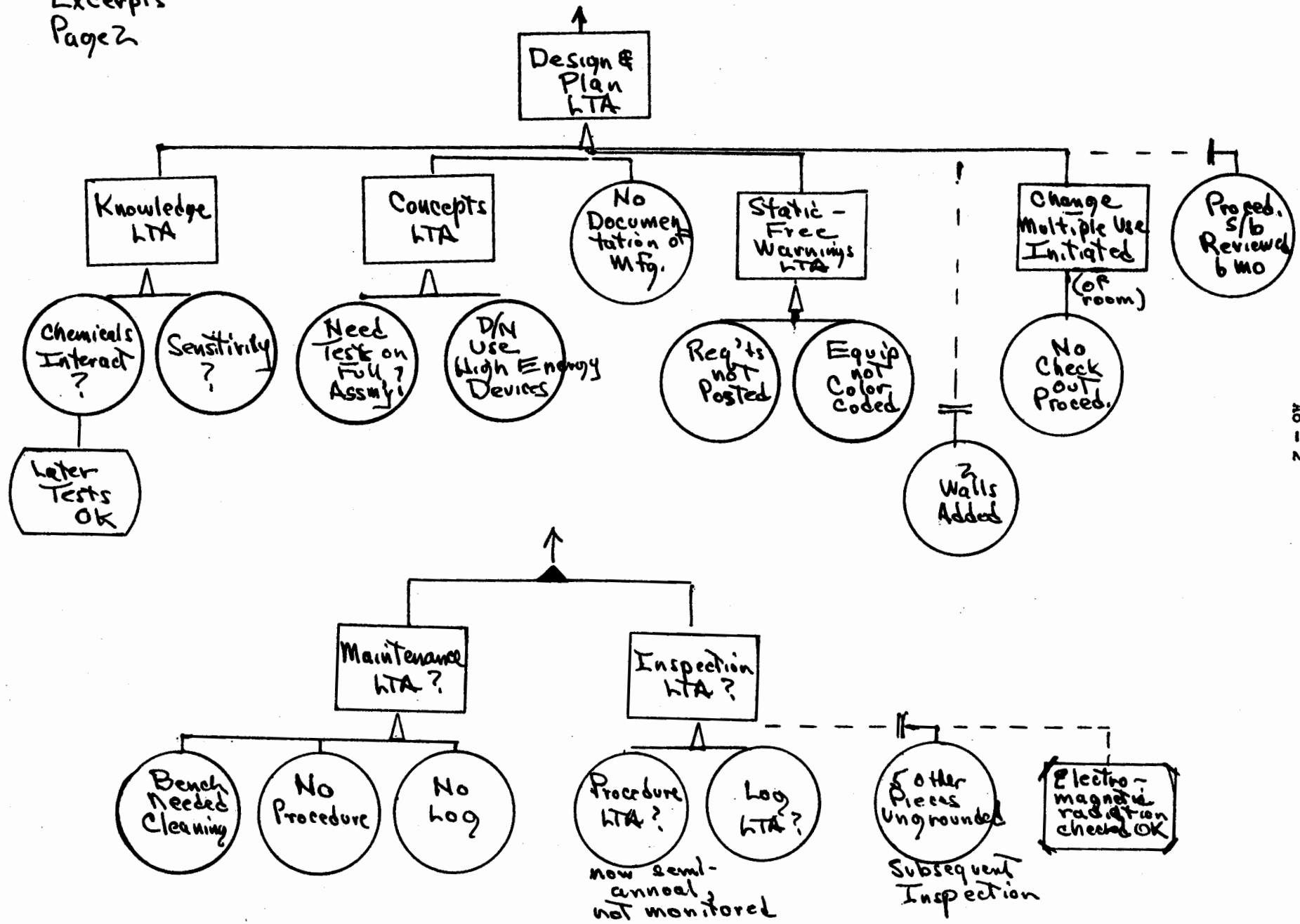
MC 1090 Initiator Explosion (1963)

Excerpts

Page 1

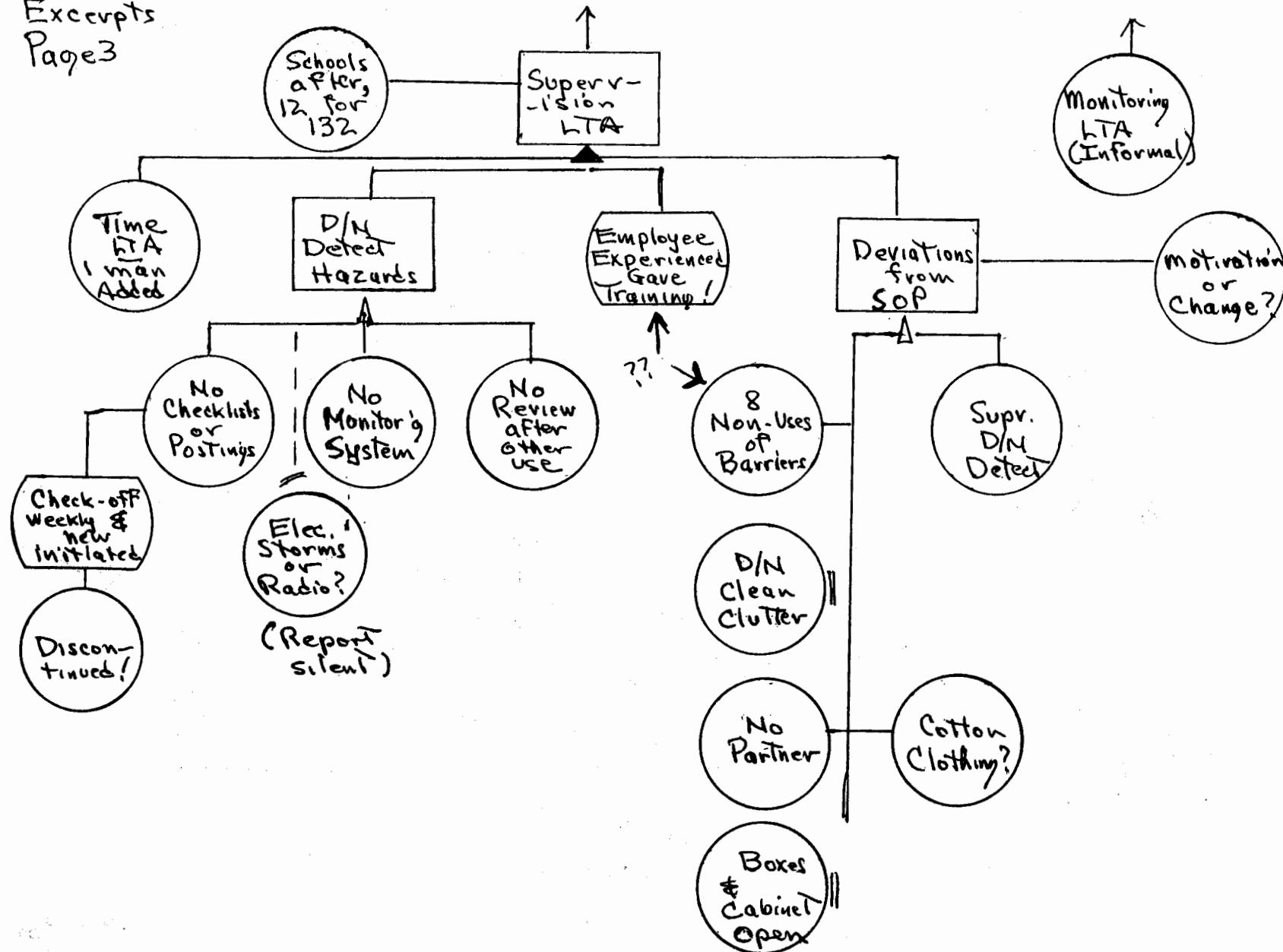


MC = Initiator Explosion
Excerpts
Page 2



MC = Initiator Explosion

Excerpts
Page 3



Appendix B. A Few Useful System Concepts

People often complain that they don't have a "feel" for what is meant by systems. On occasion, insight has seemed to come from thinking a little about various kinds of systems:

*A toaster with bread and a housewife-operator is a system.

*An unmanned satellite and a ground controller is a system.

These first two are rather limited, or "bounded."

*Traffic is a system, of which traffic lights and controls are a subsystem.

*A corporation (or a government department) is a system - perhaps imperfect and very likely imperfectly understood, but nevertheless a system.

*The U.S. Congress, or the Boy Scouts are systems.

Examine these systems against the definition at the beginning of Chapter 11.

Can you name the components of these systems? Can you state how they interact?

* * *

This is not a treatise on system development as such, but there are a few concepts fundamental to understanding and application of the text.

System Nomenclature. The usual subdivision of systems is:

The System as a whole

Subsystems

Components

Parts.

The difficulty begins when the carburetor designer sees the carburetor as a system, while the automotive engineer sees the car as the system. The National Highway Safety Administration in turn sees the car as a subsystem in an overall transportation system.

If we were more strict in our terminology (and we probably should be), we'd

have the following arrangement:

System

The organization as a whole

Subsystem

Safety as a functional entity.

Components

Program elements such as:

Information

Monitoring

Hazard Analysis

Upstream Process

Work Flow Processes

Parts, such as:

Accident Reports

RSO Studies

Worst Potential Lists

Information Search

Design

Independent Review

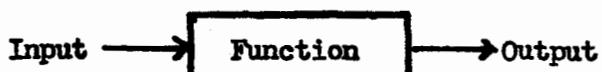
Construction

Supervision

Operating Procedures

Operating Personnel

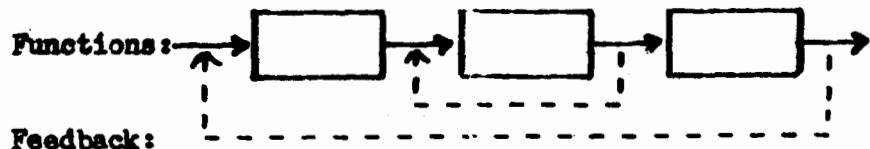
Input-Output Models. It is customary to develop system models in terms of:



Variation on the term function may include: processing, mediation, operation.

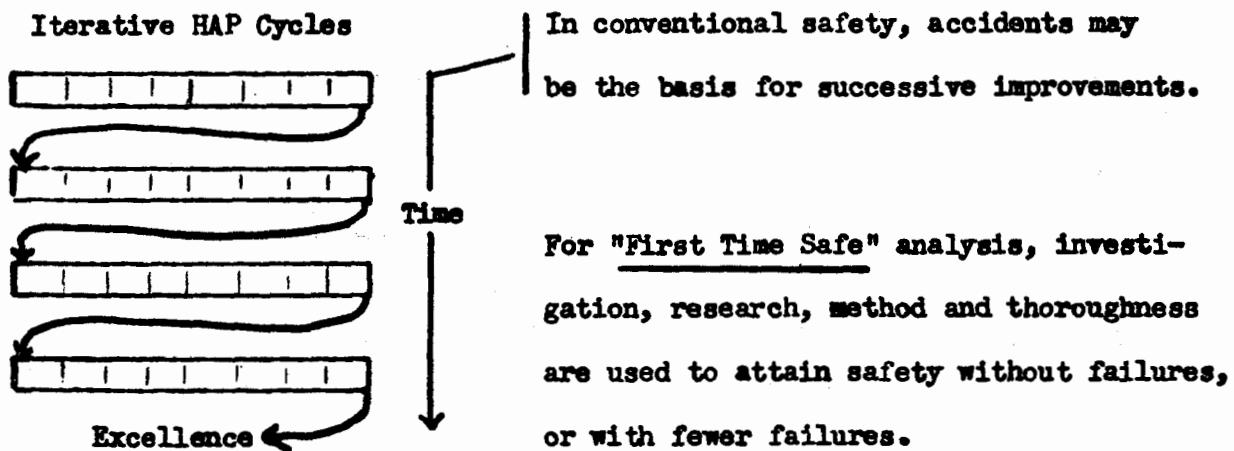
Naturally, there may be one or more inputs and outputs. In general the rectangle is used for a function, and input or output is shown cause → or cause data .

Feedback. Systems are dynamic and employ feedback to control themselves and restore balance (homeostatis). A system model must then, show feedbacks.



System Models. Actual systems are far more complex than the simple models which can be drawn or the more complex mathematical models which are increasingly used. The test of a model is whether it usefully explains specific aspects of how a system operates, and whether data can, therefore, be collected and used to improve system operations. Or, when data collection is not possible, the system element or function may be redesigned to operate according to a plan, and thereby become susceptible to measurement.

Iterative Cycles. Most systems employ successive iterative cycles to improve a function. Such cycles were shown for the general management systems discussed above. Design is in itself an iterative function. In safety, a series of uses of a Hazard Analysis Process can be seen as follows:



System Elements. One concept which has seemed to be useful in analyzing system problems has been that we deal with only three functional things:

Energy
Information
Time.

Energy is here seen as the energy forms which produce work or accidents, energy stored in machines or devices to produce work or contain and direct other energy, or stored in money, or as exemplified by persons doing things.

Information processing (collection, analysis, storage, retrieval, analysis) is a function of machine or man.

Time has aspects of change and probabilistic deviations over time, and time for energy-information processes to develop.

People are seen as information processing and energy devices. (Somewhat inhuman, but we can compensate with humanistic philosophies of error reduction, help and assistance, and building acceptance.)

Viability of a System. The viability of a system seems to be dependent on three characteristics:

1. Its ability to examine its own failures and make both specific and systemic corrections, but especially the latter.
2. Its ability to analyze and compare itself with other systems (perhaps because of indications of efficacy in other systems), and as appropriate, initiate corrective changes.
3. Its ability to deal with new information and changes.

A conscious effort has been made to use these three criteria in developing MORT, and results to date have seemed to be salutary.

Appendix C. Example of Analysis of Value Aspects of Alternatives

Most of MORT analysis is quantified in terms of energies, barriers, targets, and probabilities and consequences thereof. Quantification of values is also desirable.

The Kepner-Tregoe analysis of alternatives requires that you set down MUSTS - criteria which must be met. Then desired criteria are listed and given weights as to importance. The author has inserted a column to categorize Investments/Benefits/Values/Threats (as outlined on page 256).

In the example, four alternate plans, plus a supplementary plan to substantially improve safety are scored. The first number in each column is its score, and the second number is the product of weight times score.

The programs evaluated are:

- IA Present, same = continue present rate of improvement (a standard of comparison, but not usually a winner).
- IB Present, more = increase rate of improvement with present type safety programs.
- II Consensus, composite = an assembly of present best contractor programs.
- III MORT = inclusion of general management techniques and human factors and error reduction programs.

Supplemental - plus a funded safety research program.

To familiarize yourself with this technique:

1. Examine, modify and add to the author's criteria,
2. Examine and modify the weights assigned by the author,
3. Review scores assigned,
4. Re-compute aggregate scores.

Perhaps you have a candidate program which you want to enter and score.

Notes for figure:

*except for items proven on I/B/V/T evaluation.

**occupational plus nuclear, radiation, etc.

Problem: How Can We Substantially Improve Excellent Occupational Safety Programs in the Next Five Years?

Alternatives (see Notes on page 2)	I/B/ V/T	Weight	I. Present		II Consensus Composite	III MORT etc.	Plus Research					
			A. Same	B. More								
<u>Criteria</u>												
<u>REQUIREMENTS</u>												
1. Comply with all applicable laws			x	x	x	x						
2. Not impair present control			x	x	x	x						
<u>OBJECTIVES</u>												
1. Greatly improve hazard control:												
a. For safety reasons	B	10	1 10	5 50	5 50	10 100	+5 50					
b. For economic reasons	B	10	1 10	5 50	5 50	10 100	+5 50					
2. Not greatly increase program costs*	I	9	10 90	1 10	1 10	5 50	-5 -45					
3. Congruous with good management	V	8	1 8	1 8	3 24	10 80	+1 +8					
4. Tested and proven	B	7	2 14	2 14	2 14	5 35	+10 +70					
5. Enhance human values	V	5	1 5	2 10	5 25	10 50	+1 +5					
6. Assimilation:												
a. Easy	T	6	10 60	8 48	6 36	1 4	-1 -6					
b. Quick	T	6	10 60	8 48	6 36	1 4	-2 -6					
7. Applicable to all phases**	B	4	1 4	3 12	3 12	10 40	+1 +4					
8. Project good AEC image	V	3	1 3	5 15	5 15	10 30	+1 +3					
9. Flexible for adaptation by:												
a. Various companies	B	2	1 2	1 2	5 10	10 20	+1 +2					
b. large and small	B	2	3 6	3 7	5 10	2 4	+1 +2					
c. Various kinds of work	B	2	10 20	10 20	7 14	4 8	+1 +2					
<u>Summations</u>			292	293	306	525	+149					

- Q -

Appendix D

S 331

Discussion of Critical Incident or Incident Recall Techniques

Critical incident reporting has yet to be proven practical as a trend measurement technique. However, the reports collected have proven to be extremely helpful raw material for the hazard reduction mill. CIT was developed by John C. Flanagan (1954); also see Tarrants (1965) for a safety application.

The "critical incident technique" was summarized by O'Shell and Bird (1969) as follows (they used the term Incident Recall):

"The Critical Incident Technique (CIT), is one significant method of identifying errors and unsafe conditions that contribute to both potential and actual injurious accidents. A stratified random sample of participant-observers is asked to report all critical incidents recalled that produced or might have produced injury or property damage.

CIT grew out of the aviation psychology program of the Air Force. Many cases were discovered of pilots misreading instruments, failing to detect signals, and misunderstanding instructions. Analysis of these errors suggested some logical remedies, such as the improvement in readability of some instruments.

Several tests of the Critical Incident Technique in industry have been made. The results of a recent study at a Baltimore industrial site with participation by the Division of Accident Research of the Bureau of Labor Statistics revealed that:

- 1) The Critical Incident Technique dependably reveals causal factors in terms of error and unsafe conditions that lead to industrial accidents;
- 2) The technique is able to identify causal factors associated with both injurious and non-injurious accidents.
- 3) The technique provides more information about accident causes and a more sensitive measure of total accident performance than other available methods of accident study.
- 4) Causes of non-injurious accidents identified by CIT can be used to identify sources of potentially injurious accidents.
- 5) Use of CIT to identify accident causes is feasible.

Similar conclusions have come from other recent industrial studies using the technique. In addition, there are numerous modifications of CIT currently being applied in the aerospace and electronic industries, where it has been developed into a highly successful and sophisticated error-removal tool in quality control.

In spite of all this positive evidence of its value when applied under controlled circumstances, the Critical Incident Technique has not been widely applied in industry.

There are very practical reasons for this lag in moving to before-the-fact methodology via the Critical Incident route. The major studies that have been reported on CIT were organized by researchers and academicians, who "apparently did not have a full appreciation for the everyday problems and behavioral factors that influence the practical application and success of a safety technique with supervision in general industry."

O'Shell and Bird also provide suggested forms and procedures.

The emphasis which has been placed on CIT as a measurement tool, ie, for comparisons of units or periods, has probably misdirected attention away from the tremendous value of individual recall reports as triggers for the hazard analysis and reduction process.

Since large numbers of valuable reports can be obtained, a criterion for program evaluation is the use of CIT on at least a minimal basis as a method of collecting incident data individually useful (but not necessarily valid for comparing units).

A point could be made: No matter how small the safety budget, some allocated fraction of time should go into critical incident studies. Experience would then lead to a consensus as to optimal fractions of time.

Appendix E
Excerpts from Tables of Human Error Rates
HUMAN RELIABILITY IN OPERATION OF
CONTROLS AND DISPLAYS

<u>DEVICE AND PARAMETER</u>	<u>RELIABILITY*</u>
<u>Circular Scale</u>	
Scale Diameter, Inches:	
1	0.9996
1.6 to 1.75	0.9997
2.75	0.9993
Scale Style:	
Moving scale	0.9966
Moving pointer	0.9970
Color-coded	0.9999
Pointer Style:	
Horizontal bar, 0 at base	0.9990
Triangle or vertical bar at base	0.9987
Distance Between Marks, Inches:	
Less than 1/20	0.9975
More than 1/20 to 1/4	0.9986
Proportion of Scale Marks Numbered:	
1:1	0.9999
1:5	0.9991
1:10	0.9980
Number of Units on Scale:	
50 to 100	0.9996
200	0.9984
400	0.9962
600	0.9952

* Reliability is probability that device with given parameter will be read or operated correctly.

Source: Garrick (1967), which continues for two more pages.

Appendix E-2

HUMAN RELIABILITY IN THE PERFORMANCE
OF VARIOUS TASKS

<u>TASK ELEMENT</u>	<u>ERROR RATING*</u> <u>MEAN STD. DEV.</u>		<u>ESTIMATED RELIABILITY</u>
Read Technical Instructions	8.3	2.2	0.9918
Read Time (Brush Recorder)	8.2	2.1	0.9921
Read Electrical or Flow Meter	7.0	2.8	0.9945
Inspect for Loose Bolts and Clamps	6.4	1.9	0.9955
Position Multiple Position Electrical Switch	6.3	2.4	0.9957
Mark Position of Component	6.2	2.1	0.9958
Install Lockwire	6.0	2.3	0.9961
Inspect for Bellows Distortion	6.0	2.7	0.9961
Install Marmon Clamp	6.0	1.8	0.9961
Install Gasket	6.0	2.1	0.9962
Inspect for Rust and Corrosion	5.9	2.1	0.9963
Install "O" Ring	5.7	2.2	0.9965
Record Reading	5.7	2.3	0.9966
Inspect for Dents, Cracks, and Scratches	5.6	2.4	0.9967
Read Pressure Gauge	5.4	2.3	0.9969
Inspect for Frayed Shielding	5.4	2.3	0.9969
Inspect for QC Seals	5.3	2.6	0.9970

* Error rating is a numerical assigned value indicating degree of difficulty of task performance. The error rating is a measure of the error potential for the task accomplishment. The rating range is normally one to ten with the digit 1 corresponding to least error potential and the value 10 for most error potential.

Source: Garrick (1967), which continues for eleven additional pages.

Appendix F

Criteria for Preparation or Review of Procedures

Source: Originally based on Farish (1967), modified by an Aerojet Procedure Review Board, and further modified by the author for this text.

A. Correlation between Procedure and Hardware.

1. Does the procedure contain a statement as to the hardware configuration against which it is written?
2. Does the procedure contain background descriptive or explanatory information where needed?
3. Does the procedure reflect or reference the latest revision to drawings, manuals or other procedures?

B. Adequacy of the Procedure.

1. Is this the best way to do the job?
2. Is the procedure clear, concise and free from ambiguity which could lead to wrong decisions?
3. Have calibration requirements been clearly defined?
4. Have critical red-line parameters been identified and clearly defined, and have required values been specified?
5. Have corrective controls of these parameters been clearly defined?
6. Are all values, switches and other controlling components identified and defined?
7. Are such items as pressure limits, caution notes, safety distances, or hazards peculiar to this operation clearly defined?
8. Is the procedure easy to understand?
9. Are hard-to-locate components adequately defined and located?
10. Are job safety requirements defined - e.g., power off, pressure down, and tools checked for sufficiency?
11. Is system operative at end of job?
12. Is detail appropriate - not too much, not too little?
13. Has the hardware involved in the procedure been evaluated for human factors and behavioral stereotype problems? If not corrected, are any such clearly identified?
14. Are monitoring points and methods of verifying adherence specified?
15. Is maintenance and/or inspection to be verified? If so, is a log provided?
16. Is safe placement of other process personnel or of equipment specified?
17. Were errors in previous, similar processes studied for cause? Does this procedure correct such causes?
18. Have jigs and arrangements been provided to minimize error?

C. Accuracy of the Procedure

1. Has the capacity of this procedure to accomplish its specified purpose been verified by internal review?
2. Are all gauges, controls, valves, etc., which are called out in this procedure, described and labeled exactly as they are actually?

3. Are all setpoints or other critical controls, etc., compatible with values given in control documents and stated in the procedure?
4. Are the safety limitations in this procedure adequate for the job to be performed?
5. Are all steps in the proper sequence?

D. Adequacy and Accuracy of the Supporting Documentation

1. Are all adequate supporting drawings, manuals, data sheets, sketches, etc., either listed in this procedure or attached?
2. Are all interfacing procedures listed in this procedure?

E. Securing Provisions

1. Does the procedure contain adequate instructions to return the facility or hardware to a safe operating or standby condition?
2. Do these securing instructions contain step-by-step operations?

F. Backout Provisions

1. Can this procedure put any component or system in a condition which could be dangerous?
2. If so, does this procedure contain emergency shutdown or backout procedures either in an appendix to the procedure or as an integral part of the procedure?
3. Is the backout procedure or instructions for its use included at the proper place in the basic procedure?

G. Emergency Measures

1. Are there procedures for action in case of emergency conditions?
2. Does the procedure involve critical actions such that pre-performance briefing on possible hazards is required?
3. Are adequate instructions either included or available for action to be taken under emergency conditions? Are they in the right place?
4. Are adequate shutdown procedures available and do they cover all systems involved and are they available for emergency re-entry teams?
5. Does the procedure specify the requirements for an emergency team for accident recovery, troubleshooting, or investigative purposes where necessary, and describe the conditions under which the emergency team will be used and the hazards they may encounter or must avoid?
6. Does the procedure consider interfaces in shutdown procedures?
7. How will changes be handled? What are thresholds for changes requiring review?
8. Have emergency procedures been tested under the range of conditions which may be encountered - e.g., at night during power failure?

H. Caution and Warning Notes

1. Have caution and warning notes been included where appropriate?
2. Do caution and warning notes precede the operational steps containing potential hazards?
3. Are they adequate to describe the potential hazard?

4. Are they separate entries with distinctive bold type or other emphatic display?
5. Do they include supporting safety control (health physics, safety engineer, etc.) if needed at specific required steps in the procedure?
6. Are human-induced hazards identified and described by cautions and warnings?

I. Requirements for Communications and Instrumentation

1. Has an adequate means of communication been provided?
2. Will loss of communications create a hazard?
3. Is the course of action clearly defined in the event of loss of required communications?
4. Has verification of critical communication been included where required?
5. Will loss of control or monitoring capability of critical functions create a hazard to people or hardware?
6. Have alternate means or a course of action been clearly defined to regain control of monitoring functions?
7. Are the above situations flagged by cautions and warnings?

J. Sequence-of-Events Considerations

1. Can any operation in the procedure initiate an unscheduled or out-of-sequence event?
2. Could it induce a hazardous condition?
3. Is it identified by warnings or cautions?
4. Is it covered by emergency shutdown and backout procedures?
5. Are all sequence steps prescribed in the procedure sequenced properly and such that they will not contribute to or create a hazard to the hardware?
6. Have all steps which, if performed out-of-sequence, could cause a hazard been identified and flagged?
7. Have all non-compatible simultaneous operations been identified and suitably restricted?
8. Have these been prohibited by positive callout or separation in step-by-step inclusion within the text of the procedure?

K. Environmental Considerations (Natural or Induced)

1. Have environmental requirements been specified which constrain the initiative of the procedure or which would require shutdown of the action or evacuation, once in progress?
2. Have the induced environments (radioactive, toxic or explosive atmospheres, etc.) been considered?
3. Have all latent hazards (pressure, height, voltage, etc.) in adjacent environments been considered?
4. Are there induced hazards from simultaneous performance of more than one procedure by personnel within a given space?

L. Personnel Qualification Statements

1. Has a requirement for certified personnel been considered?
2. Is required frequency of re-check of personnel qualifications specified?

M. Interfacing Hardware and Procedures Noted

1. Have all interfaces been described by detailed callout?
2. Have interfacing operating procedures been identified or written to ready equipment?
3. Where more than one organizational element is involved in an operation, have proper liaison and areas of responsibility been established?

N. Procedure Sign-Off

1. Is procedure to be used as an in-hand, literal checklist?
2. Have step sign-off requirements been considered and identified and appropriate spaces in the procedure provided?
3. Have procedure completion sign-off requirements been indicated (signature, authority, date, etc.)?
4. Is supervisor verification of correct performance required?

O. General Requirements

1. Are the procedures set up such as to discourage a shift change during performance or in such a manner as to accommodate a shift change?
2. Where shift changes are necessary, does the procedure include or reference shift overlap and briefing requirements?
3. Is there mandatory inspection, verification and system validation required whenever the procedure requires breaking into and reconnecting a system?
4. Are safety prerequisites defined? Have all safety instructions been spelled out in detail to all personnel?
5. Do the procedures require pre-checks of supporting equipment to ensure its compatibility and availability?
6. Has consideration for unique operations been written into the procedures?
7. Do the procedures require walk-through or talk-through dry runs?
8. General supervision requirements - e.g., what is the protocol for transfer of supervisor responsibilities to a successor?
9. Are responsibilities of higher supervision specified?

P. Reference Considerations

1. Have applicable quality assurance and reliability standards been considered?
2. Have applicable codes, standards and regulations been considered?
3. Does the procedure comply with control documents?
4. Have hazards and system safety degradations been identified and considered against specific control standards and procedures?
5. Have specific prerequisite administrative and other management approvals been complied with?
6. Have comments been received from the people who will do the work?

Q. Special Considerations

1. Has a documented safety analysis been considered for safety-related deviations from normal practices or for unusual or unpracticed maneuvers?
2. Have new restrictions or controls become effective that affect the procedure in such a manner that new safety analyses may be required?

Appendix G

S 347

Participation and Motivation

(Excerpt from earlier report)

Participation and Social Forces

We have seen in innovation diffusion* the possibility of substantive effects from participation and inter-personal influences in acceptance of changes.

The management style of the organization, and its use of behavioral science principles, aside from how we design safety projects, will obviously have a predominant, or at least underlying, effect on safety. High morale has been shown to be associated with acceptance of personal responsibility for safety. Low promotion possibility has been shown to be associated with accidents.

* Appendix H

Seiler describes the strong influence of the social factor or social inputs on behavior in terms of establishment and maintenance of group norms. Obviously such norms can be favorable or unfavorable for safety, especially so if a constructive change is desired. Therefore, planned programs for safety should include identifiable elements which endeavor to enlist support from the social structure.

Performance of scientists in a research organization was shown to be related to group variables in variety of values and experience, and when supervisors provide stimulation and autonomy. Thus, a few possible guides for laboratory safety can be perceived.

Participation in development of safety measures can involve group leaders in such ways as to promote, first, individual and then, group acceptance.

Participation, especially by a group, may supply valuable on-the-job know-how, but has a limiting value where professional expertise is required.

We now see more clearly why participative activities are not just as option - they are necessary to success. The case histories of successful programs are replete with references to need for participation.

Participation can, obviously, take many forms. Committees are one of the forms very common - management committees to build acceptance and team spirit, and committees with employee participation (in some cases union-selected and in others otherwise selected). In those low-accident-rate companies which frown on committees, in general, or employee committees as such, there is most often great stress on other forms of participation.

There are four common forms of safety committees:

1. Corporate, or plant-wide - usually a management committee.
2. Departmental - usually a committee of foremen.
3. Area - a committee of workmen.
4. Ad Hoc, Special Problems.

However, there are wide variations from this pattern, including plant labor-management committees.

The functions of committees include:

1. Arouse and maintain interest.
2. Promote personal responsibility (management and employees)
3. Help integrate safety in operations
4. Provide for discussion
5. Help management evaluate suggestions
6. Develop team spirit.

Written terms of reference for committees are essential. Meetings should be well planned. Follow up to secure action or disposition on recommendations should be unfailing. A record of accomplishment should be built.

Specialized committees or special functions of existing committees may include inspection and accident investigation - however, committee work here is definitely no substitute for the primary line responsibility. Because committee inspection and investigation may impair line responsibility, such functions are frowned on by many.

In planning the participation aspect of a safety program, the safety director will want to take account of other pertinent activities - e.g., the presence of a suggestion system.

The duPont company stresses the value of discussion in problem solving (safety or other). They have an interesting pictogram, which says that a full discussion is the best way to get there first.

duPont	Discussion	Execution
Others	Disc.	Execution

Hughes emphasized participative and social influences in motivation, but first placed these aspects in a context of clear goals, job satisfaction, and mutual confidence of management and employee. Such conceptual or context considerations tremendously complicate safety program analysis or measurement, but it would be

foolish and dangerous to oversimplify the motivational problem.

Supportive Programs

Human relations programs, and mental health and alcoholism programs, are additional examples of basic programs to support and assist the individual, which can have an important relation to safety. Brody concluded they could contribute much and could profitably be expanded.

Presumably the role of safety is to provide data pertinent to support of such broad programs, and to utilize them to the fullest.

The Individual in a Sociotechnical Context

We shall shortly come to the fuzziest areas of human factors - attitudes, emotions, and personality - so we can profitably recapitulate the elements in his environment which the Hazard Reduction Precedence Sequence has ideally provided.

The organization has now maximized its contributions in the following areas:

1. Proven management concern - sincere and vigorous,
2. A safeguarded environment,
3. Tasks and equipment integrated and error preventive - tolerant of human limitations,
4. Good job safety procedures, job training and supervision,
5. Safety improvement programs which provide for participation and group reinforcement and support, and
6. High morale and productivity through sound human relations, backed up by mental health resources where needed.

Sounds like heaven! However, in an ideal system it makes sense to put preferential emphasis to those programs which have demonstrated some efficacy before trying to "change human nature."

The Individual

The individual person has been dealt with in terms of selection, adequate training, good supervision, opportunities for participation, group influences, morale and supportive services - all of which should be influential in producing safe behavior. It remains to consider whether some additional problem variables -

negative attitudes, emotions, and social maladjustment can be constructively affected.

Brody reports that the evidence for relationships of attitudes to safety is in some conflict, and that personality and psychological tests have not been sufficiently predictive to be of great use. Safety-related attitudes may be the result of the broader morale building situation.

Emotions, emotional cycles, and particularly emotions which disrupt tasks requiring thought and decision have been shown to be accident related.

The socially maladjusted, the deviates, and those in conflict with organization and authority produce more than their share of accidents, perhaps because group norms are less effective.

McGlade says:

"The list of psychological constructs in accident causation is long. Safety specialists are dog-eared from hearing the hackneyed phrases bandied about concerning the relationships of accidents and such psychological traits as "aggressiveness," "hostility," "insecurity," "emotional instability," and "resentment of authority."

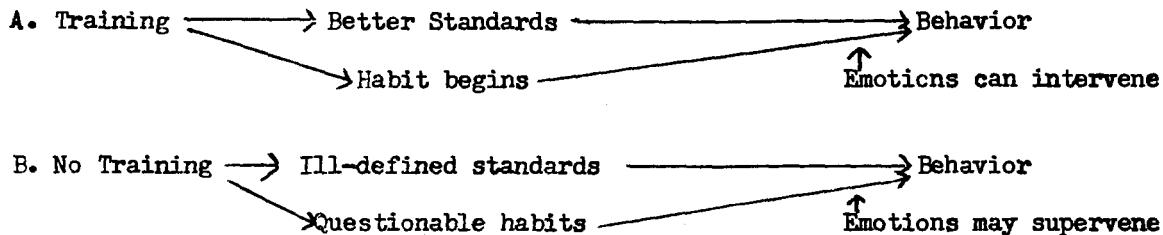
"Safety specialists are disillusioned as well as dog-eared. Unfortunately, none of these characteristics has been isolated in relation to accident incidence to a degree necessary to demonstrate its causative influence. It is more likely a configuration of these characteristics, as yet unidentified, which gives the clearest picture of the accident-susceptible individual. Even if such an identification were available, it might be meaningless in the long run. Most individuals possess these characteristics in varying degrees, and it is highly improbable that diagnostic or corrective measures could ever be developed which would be valid or practical in application."

The action potentials are far from clear. Certainly mass programs to change attitudes and improve social adjustment have not been forthcoming.

The person has a personality which gives him certain needs (worth, achievement, acceptability, etc.) and these in turn give him goals. Between needs and goals, we find emotions and frustrations. Our task then is to build in motivational programs which attempt to satisfy needs, and provide supervision to attempt to control adverse effects of emotions.

Attitude. There has been a lot of apparent nonsense on attitudes in safety work, e.g., "Good attitude is all important." Actually, a man could have a "wonderful attitude," and if he had poor standards of judgment or poor habits, kill someone in the next few hours.

We can use pictograms to trace two divergent sequences:



This conceptualization, if the scientists can bear with the simplifications, would provide us with some framework for planning and investigation, and obviously will place a heavy load on close personal supervision to detect relevant changes, and to avoid creating emotional problems.

Changes in People. Discussion with experienced accident investigators suggests that information on personal problems and changes, sometimes highly personal, is quite often revealed or hinted. Certainly personal privacy is a value to be protected. But if records are to remain silent on known variables, how shall we improve our work? How shall we assess the need for additional supportive programs for the individual? How shall we diagnose our accident problems? A real dilemma.

Motivation

In summing up motivation for safety, McGlade and Campbell have touched on specific aspects relevant to supervision, participation, social factors and human relations: opportunity to express oneself, job satisfactions which meet personal needs, understanding, acceptance, security, reasonable autonomy, and freedom to be skillful. Morale affects productivity and safety; and if attitudes are mutable it is through job-related satisfactions, rather than through propaganda.

Moser provides a less dissection, but equally persuasive philosophy which relates motivation for all aspects of performance to management's attitude on safety.

Mass Communication.

Propaganda such as slogans, posters, leaflets and magazines, and program

devices such as contests, constitute a highly visible part of many safety programs.

McGlade observes:

"...psychological research has demonstrated that reliance on typical publicity campaigns of an informational or admonitory nature which are intended to dispel ignorance, alter attitudes, create or change motives and consequent behavior, or make the population more Safety-minded, are of dubious value. For they are based on such dubious assumptions as: individuals themselves are largely responsible for their own fate; knowledge alone will automatically lead to appropriate and safe social behavior; propaganda will make unscrupulous men moral or unsafe men safe; and campaigns will confer foresight on those who lack it."

However, McGlade's guidelines for communication can be helpful in designing and evaluating programs.

"Psychological theory and research have evolved some general principles to guide us in developing safety mass communications: the lines of communication should be as direct and short as possible; communication should be complete and continuous; and communication must be based on confidence.

"There are also some specific principles relating to mass communications: (1) a person hears what he expects to hear; (2) a person will ignore information which conflicts with what he already knows; (3) the source of a message is a determinant of the individual's acceptance of it; (4) the parts of a message are usually linked together in a 'halo effect,' - if the individual rejects the first part of a message he will tend to reject all of it; (5) people interpret a given stimulus in different ways, and this interpretation is dependent to a large extent on their previous experiences; (6) words mean different things to different people; and (7) vague messages often act as emotional stimulants, prompting feelings of insecurity and consequent rejection.

"These principles are interwoven, and there are some basic lessons to be learned that are relevant to the development and implementation of safety communications. The most obvious statement that can be made is that successful communication does not take place automatically when a message is imparted. This statement appears self-evident and mundane, and yet it is an axiom as often ignored as not.

"There are several guidelines which can serve to place safety communications in the proper perspective relative to other safety management functions: (1) mass communications are most effective in a supporting role, when used to enhance and support operational aspects of the safety program; (2) safety mass communications should be presented in a planned sequence to support specific aspects of the safety program and specific safety promotional campaigns, rather than haphazardly presented in a "shot-gun" fashion; (3) repetition leads to retention, therefore safety mass communications should be repeated on a planned periodic basis in support of specific safety program features; (4) immediate benefits attract more attention and positive reaction than remote or long-range ones, therefore safety mass communications should be activated concurrently with safety program procedures and activities; (5) the familiar is grasped and supported more readily than the unfamiliar, therefore, safety mass communications should link new ideas to accepted safety procedures or activities; and (6) the objectives of a safety mass communication or series of communications should be limited in number so that the recipient can readily absorb them."

Planek's program planning model is valuable for any program plan, but particularly for mass communications. (See figure next page.)

Some forms of one-way communication (e.g., supervisor materials or general rule books) would be evaluated as part of the supervisor or job analysis programs.

The injunction to consider propaganda as supportive for the basic program, rather than a primary influence, is wise advice.

A limited number of studies have indicated that posters, if relevant and placed at an action point, produce changes in behavior. Psychologists have urged that posters not be anxiety-producing.

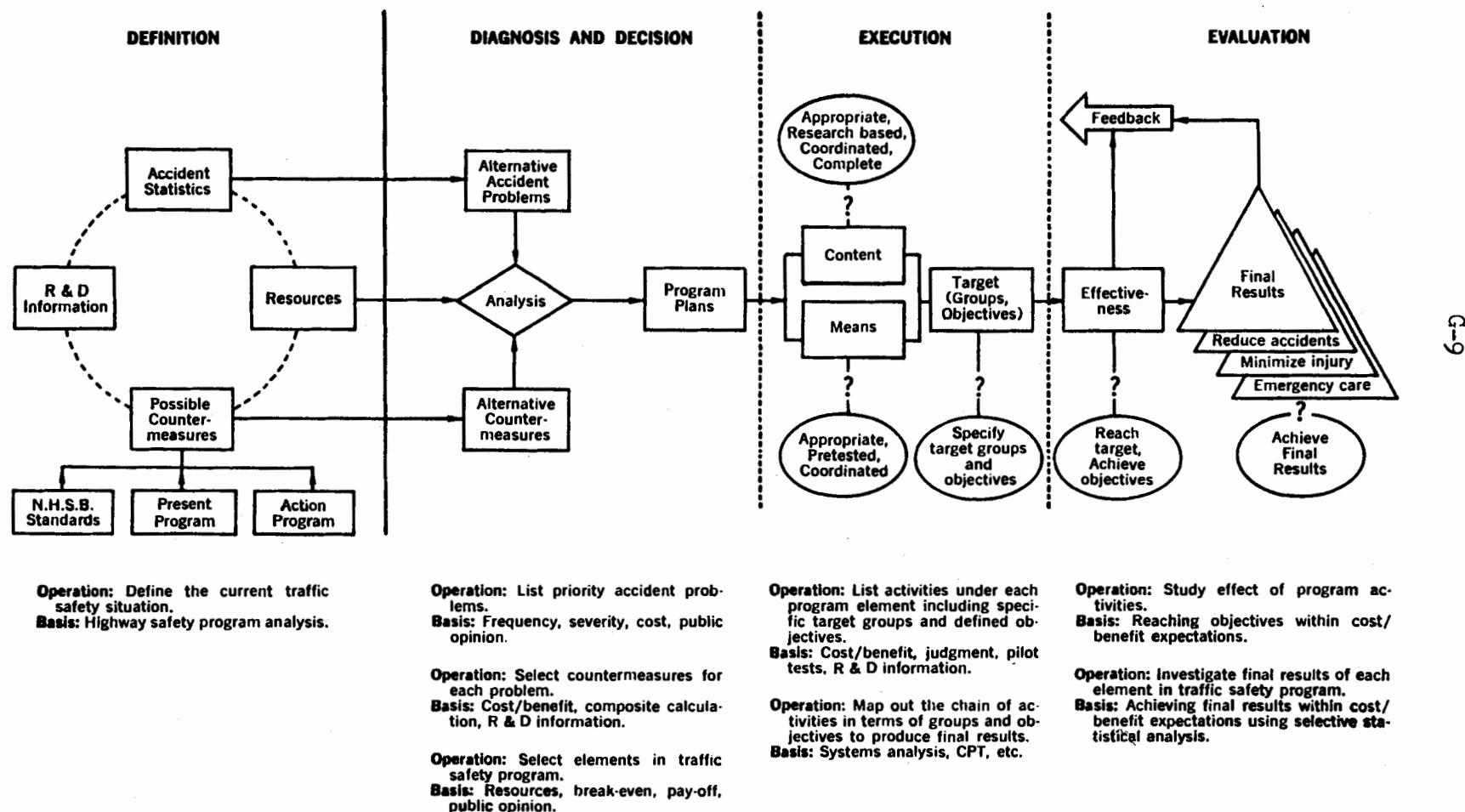
Certainly recognition of achievements, such as award ceremonies, are a proper and merited recognition of efforts and help build morale.

Criteria for designing programs to maintain interest and obtain helpful publicity are provided in the NSC manual and other references.

In recent years, off-the-job safety has been promoted by many organizations because of the company's concern for costs as well as employee welfare. Initially such campaigns appeared highly productive - latter evidence of effectiveness is not persuasive.

Family involvement, for example by material in off-the-job safety sent to homes, has seemed helpful in stimulating personal discussion and involvement.

It does not seem at all likely that mass communications will have identifiable effects on mass behavior. Therefore, the intermediate evaluations of message, target, etc., suggested by Planek should be emphasized, while the safety program as a whole is evaluated by behavior and accident indices.



Appendix H. INNOVATION DIFFUSION

Acceptance of safety-related changes is a goal of the safety program. Indeed, it could be argued that a primary activity of the safety professional is changing behavior.

The existence of a set of research-based concepts on methods of behavior change, plus strong indications of proven effectiveness in the field of safety, seems reason enough to select this topic for special treatment as an example of availability and use of guiding principles from the behavioral sciences.

The concepts of the process of diffusion and acceptance of innovations provides a very useful framework for program design and measurement. The concepts also help define and inter-relate the functions of group or interpersonal influence and mass communications, and thereby provide some guides for separate evaluation of social and propaganda forces.

The process was described in NSC's Community Support Report (1968) as follows:

"Research studies in the agriculture community have produced findings which can be useful to safety program planners faced with the problem of diffusing new ideas and practices. Known as innovation diffusion the process is based on two generalizations revealed by the research. The first is that the process by which people accept new ideas is not a unit act but rather a series of complex unit acts. This mental process consists of at least five stages. The second generalization is that individuals can distinguish one stage from the other and can designate points in time when they went through each stage. The five stages are:

1. Awareness. At this stage the individual becomes aware of the proposed program. He knows about it but doesn't have the details concerning it. He may know what it is called but not how it will work.
2. Interest. Here the individual wants more information about the program. He wants to know what it is, how it will work and what results are expected. Also he may want to know how the program will effect him personally or his group.
3. Evaluation. At this stage the individual begins to make a mental trial of the program. He applies the knowledge obtained from the previous stages and begins to ask questions as to what the effects of the program will be on himself, his family and associates. He weighs the plus and minus factors.
4. Test. If he decides the program will work, has value and appears to be the thing to do, he will test it, maybe on a small scale at first. He may discuss it with colleagues or others who have tried it. He sees that it has worked elsewhere and learns that the idea or concept of the program works.
5. Acceptance. This is the final stage in the mental process, the program is accepted and the individual is satisfied with the program and will act in support of it.

"If the program planner knows the process he can use it to better identify what stage the target person or group has reached.

"The rate of this process may be different for each target depending upon the complexity of the program and the quality of the information obtained and evaluated at the various stages. For certain targets the process for a given program and time may be shortened by his previous experience. He may already be aware or past the evaluation stage and need only to go through the test and acceptance stages.

"The program planner can design the material for use by various targets and community groups to help them through the above process. Publicity for mass communication can be purposely made to start the target through this process. The first two stages especially are adaptable to one-way communications. However, two-way communication, questions and answers, is needed in the last three stages. This can be done by interpersonal techniques, correspondence, meetings, personal contact, etc.

"Up to the present the average safety program planner has not consciously used step by step techniques such as innovation diffusion in program development and execution. Generally speaking, he has made people aware of their programs and has created some interest, but most targets are left at this point to go through the two-way communication stages on their own initiative and at their own pace."

One-way communications include posters, leaflets, written instructions, magazines, newspapers, radio, television and meetings exclusively with speeches or films.

Two-way communications include committees, meetings with participation, job analysis with participation, job training (if the supervisor uses two-way discussion, as he should), day-to-day contacts with management and fellow-workers, family life (a value in off-the-job safety activities), bull sessions and gripe sessions.

Acceptance is defined as a change in behavior. "Innovators" (perhaps 3% of a general population) and "Early Accepters" (perhaps 15%) can usually be identified by name for personal attention.

These, and related concepts, provide the safety professional with a sequential framework for building acceptance - both in management and in the work force. If somewhat mechanistic and perhaps over-simplified, the procedure more than makes up for its shortcomings by providing a unifying plan.

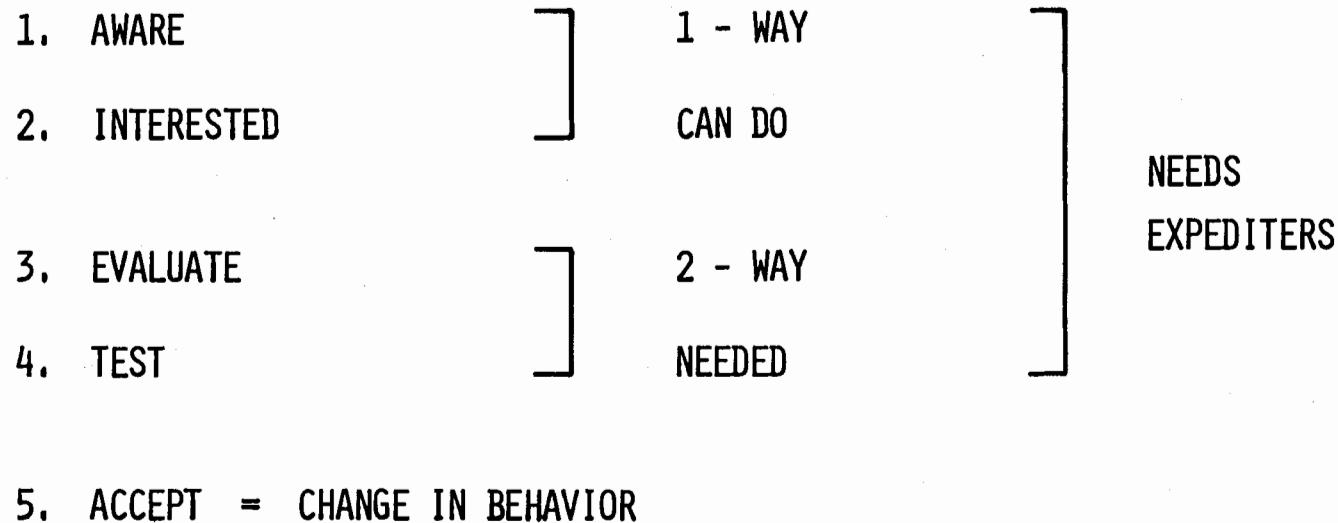
If we use the 5-step yardstick of the Innovation Diffusion process, we have a way of measuring where a person or group is in the process.

More important, we have a way of planning subsequent activities so that the nature of the material and the form of communication will be effective in attaining the next stage toward acceptance. In short, a planned program for behavior change, without careful planning for two-way communications, is likely to fail. A visual used in presenting the program is shown as Figure H-1.

The studies have also shown the need for expediters - the process is likely to slow or stall unless someone, usually the safety professional, finds

Figure H-1

'INNOVATION DIFFUSION'



PERSONS HAVE INFLUENCE

PERSONS HAVE NAMES!

IDENTIFY TARGETS

* * *

USE S-CURVE TO KNOW WHERE YOU ARE!

E.G. LOOKING FOR INNOVATORS

out where the hang-up occurs and gets this moving.

Additional reference material includes Juran (1964) (who has chapters on "Breakthrough in Attitudes" and "Resistance to Change ' Cultural Patterns") and Currie (1968) (Thirteen Steps for Innovation).

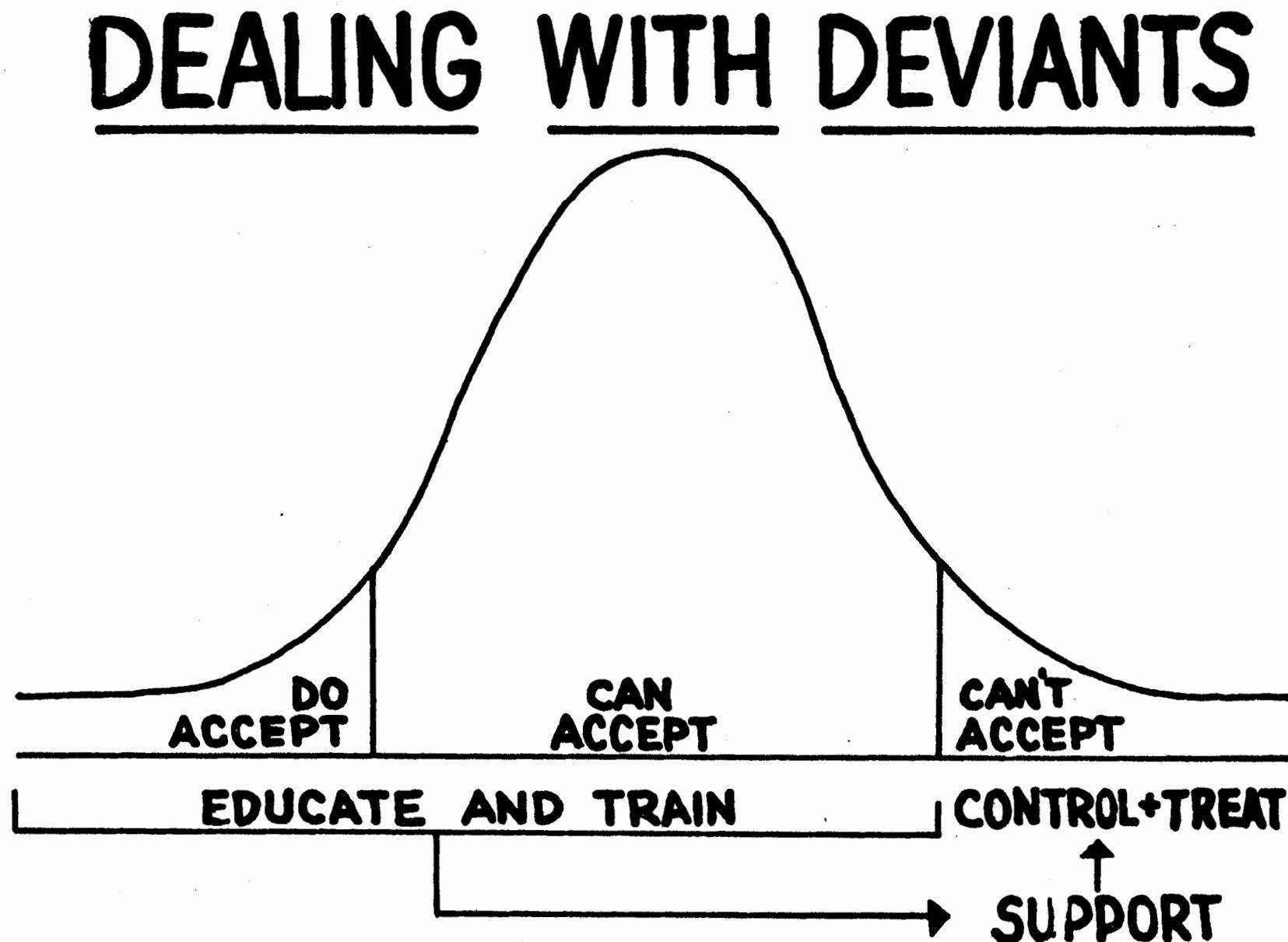
A report on worker acceptance of occupational safety measures reflected factors associated with innovation diffusion (Suchman and Munoz).

The innovation diffusion process has been shown to follow a cumulative S-curve, and there is evidence that the program which gets an idea to the 15% breakpoint, if continued, can over time move acceptance to 85%.

As we come closer and closer to full acceptance we begin to see a logical, proper and useful role for enforcement. (See Figure H-2, which presents the cumulative S-curve as a normal distribution.) The clear implication is that enforcement is a last step in programming rather than an introductory or primary step.

During the Aerojet trials, a number of program innovations have been introduced in a manner consistent with the above principles. These include: project engineers' use of national information sources , the same engineers' use of local information and change analysis, job safety analysis, a field safety engineers' audit plan, criteria for procedures review and other review boards, and MORT analysis of accidents. In all of these kinds of programs, acceptance of a new idea (and perhaps some adjustment of the idea) preceded the issuance of directives establishing the process. Handled in this fashion, the common resistance to directives and procedures can be largely overcome.

Figure H-2.



Appendix I.

ACCEPTANCE OF PROCEDURALIZED SYSTEMS AT AEROJET

The Problem

1. The acceptance of proceduralized systems can be seen as a candidate for the "number one present problem" of Aerojet, despite current audit records of 99.4% compliance, a very high compliance rate.
"Hardware" was, and always can be, the basic problem; but, hardware problems seem to be generally well handled (with the exception of some human-related or human factors hardware problems).
2. Acceptance of procedures often means acceptance of change - change in a task-method, or the broad problem of Aerojet's change to a proceduralized system. There are relevant social science findings.
3. Acceptance involves all the complexities of human variables, and is, therefore, a difficult problem.
4. Unplanned variability, over-simplification, and spottiness, as well as questionable effectiveness, characterize many programs and approaches to human variables.
5. There is no considered, explicit and practical basis for planning behavioral programs - no firm basis for designing a program modification-test-evaluation-application cycle of behavior change.
6. In consequence, a "state of the art" paper (modifiable always) seems to be a first requirement, and is the objective of this memorandum.

The Approach

This discussion treats the following aspects of acceptance:

1. Defined systems goals - i.e., systems that work!
2. Present Aerojet systems - not working well enough.
3. Personal variables - other than 4 and 5 below.
4. The "psychology and sociology of acceptance" - participation, group norms, and the spirit of the group.
5. Deviant personalities, and a possible role for enforcement.
6. A framework based on the social sciences is outlined.

The consideration thus stated lead into specific problems:

7. Training requirements.
8. Supervisory requirements.
9. Monitoring requirements.
10. Participatory and other humanizing requirements.

These in turn, suggest two requirements:

11. An experimental approach to specific methods of gaining acceptance, and suggestions of areas to be explored.
12. Need for an internal group with the broadest available competence to maintain an advisory overview of programs to gain acceptance.

Defined Systems Goals

The hardware should be adequate to the task before we can expect acceptance. MORT suggests a sequence of aspects and procedures. The Hazard Analysis Process should be well defined and operative. A Safety Precedence Sequence which places first emphasis on hardware and operability should be clearly stated and carried over into practice. This SPS sequence includes human factors engineering to reduce error-provocative aspects of tasks.

Procedures that work well can then be developed by use of adequate criteria, including checks with the people who do the work, adequate Job Safety Analysis for repetitive craft assignments, corrections for faults revealed by past inci-

dent data, and provisions for prompt fixes of deficiencies in hardware, procedures or personnel.

Supervision based on the Job Safety Analysis-Job Instruction Training-Safety Observation sequence can then be effective. Direct "Safety Observation" monitoring by supervisors can be augmented by other, adequate monitoring schemes which provide usable feedback on work well done, as well as failures.

Such a monitoring system provides indispensable bases for design of motivational programs likely to be effective, including rewarding experiences for work well done. The monitoring system should provide larger numbers of experiences deserving reward, as contrasted with smaller numbers of experiences meriting penalties. It seems that a monitoring system producing only penalties is likely to be ineffective, capricious, and variable.

Present Aerojet Systems.

The present Aerojet systems, while excellent by comparison with general industrial norms, do not fully meet systems safety goals. The present ROD and NOS efforts to develop schematics and auditable criteria are first steps in improvement. This, of course, must be followed by substantive corrections based on audit findings.

Aerojet attempts to document in ANPP's-SP's-DOP's the systems by which the company operates. This documentation seems well conceived, but has certain limitations which should be understood:

1. The legalistic language is difficult to understand and subject to variable interpretation. This suggests several supplementary approaches:
 - a. Simple schematics and plain language flow diagrams which expose basic systems. (Plain language editing of basic documents might also pay off.)
 - b. Appropriate interface and internal discussions to develop understanding and implementation.
2. Complex systems always operate in ways different from manuals, procedures, etc. This axiom has several significant implications:
 - a. Monitoring to determine actuals is needed.
 - b. An organizational imperative to know that the problems are not solved by issuing directives must be a basis, conscious and explicit, for aggressive implementation of the substance behind the directives. Failure to observe this imperative leads to at least two problems:
 - (1) The fallacy of believing that things are changed or cured by issuing directives,
 - (2) "Covering your number" to show outward compliance with directives, but perhaps without substance.
 - c. Management and supervisors, technical personnel, and employees are commonly using many sound practices (as well as some potentially unsound practices) not explicitly covered in manuals, etc. Thus the sound practices should be identified, and must be considered for translation into directives, training, etc. However, the absence of items in directives, etc., is not all bad; it may provide good practices and freedom for the humans to use their capabilities.

It could be well argued that Aerojet does not, today, have the basis for full acceptance of proceduralized systems. In addition to the comments above, there

seems to be a deficiency in the purely human and personal aspects of acceptance, and as a corollary, perhaps some assumption that acceptance will come about because AEC (the customer) demands it. All of these aspects, if present and important, need examination, a guiding doctrine, and a program for progress.

Personal Variables in Behavior.

Individual behavior will be affected by psychological-sociological variables, and for a few persons will stem from deviant personalities (both discussed below). Here we are first concerned with those system aspects of the problem which foster or inhibit safe behavior in the individual.

The individual is a rational, goal-seeking, thinking element in the full system. He is also emotional, and his emotions may contribute strong motivation toward making the system work, or may derail the system.

Perhaps the most useful place to launch dissection of human variables is from a focus on safe habit formation. This gives us a tie to the training and supervising functions in the so-called tight system. Safe habits in thinking and action are probably the keystone in acceptable behavior. This suggests needs for, not just step-by-step training in actual tasks, but also training in how to analyze situations for risk, risk standards, and an environment which is controlled (or disciplined) - that is, an environment in which deviations are promptly detected and corrected. Rewards and penalties will reinforce or extinguish safe habits.

Within a general population which has safe habits, and for an individual within such a population, there will be variances in behavior which are to be expected and therefore can be said to be "normal." From this, error rates (rather than perfect performance) will be expected. A lowering of normal human error rates is possible, but modifiable situational factors (error provocative aspects) are more likely to be productive than purely motivational factors.

Temporary emotional or physical factors can affect performance, and should, where possible, be detected and corrected by supervisors, fellow employees, and medical and counseling staffs.

Sociology and Psychology of Acceptance.

More than a little is known about the sociology and related psychology of behavior formation. The roles of group norms and of participation in fostering acceptance are defined with usable, practical precision. Some protocols for behavior change, such as "innovation diffusion" are relatively simple and have been tested in practice.

Thus, the forms of safe procedure development (e.g., Job Safety Analysis and checking with people who do the work), and monitoring (e.g., RSO studies) have sociologic virtues over and above the tangible products of such programs.

All programs should be examined for collateral qualities which enhance or inhibit safe behavior development.

There seems to be such a thing as "spirit" evidenced by hard work seeming easy, difficult tasks well done, and potential hazards safely circumvented. Spirit would seem to have at least the following aspects or dimensions:

1. Performance goals - either of the person or the organization.

If it be true that long-term stability and growth in Aerojet's role is contingent on its reputation for precise, error-free operation of advanced systems, the articulation of such goals to the work force may be most helpful in both of these first two dimensions.

2. From these, benefits to the person or group.
3. Teamwork, and group identification.
4. Morale - which may have many non-safety aspects, some of which may not be modifiable within the safety program.
5. Leadership - especially of management and supervision, but not excluding formal and informal leadership roles among operating employees.

Deviant Personalities.

There is limited evidence that persons not well adjusted to groups or to society, as measured by on-job relations or a biography showing evidences of credit, family, court and other conflicts, or alcoholism, have more than their share of accidents.

However, the group is not usually found to have such significance that its complete removal would materially alter overall accident rates.

However, the historic, common-law role of enforcement is directed at a deviant minority who do not voluntarily accept a code of conduct. This seems to provide a basis for the role of safety enforcement - namely penalties for willful or repeated violations of clear and workable procedures accepted by the majority. However, acceptance does not begin with enforcement penalties - rather, is a terminal aspect.

This is not to say that enforcement does not affect the general population. It does. However, voluntary acceptance of change or rules still seems to be basic to high levels of acceptance (or public support for enforcement).

The S-shaped innovation acceptance curve (alluded to in Chapter 36) also carries the implication that a fraction of the population, perhaps one to three percent cannot be brought to acceptance.

Menninger and Dunbar have written of the fraction of accidents seemingly attributable to purposive accident-producing behavior. Their findings are difficult to digest into a positive preventive process. A recent review of the literature concluded (Nygren, 1971):

"Two practical suggestions are advanced by Hirschfeld and Behan: (1) plant medical personnel should watch for a sudden increase in the number of sick calls an individual makes, and (2) line supervisors should listen closely to the worker who may, in his own fashion, be pleading for help."

A Social Science Framework for Acceptance

MORT.

In MORT will be found an analytic method reflecting some social science findings in Motivation. Also provided is an Appendix (taken from earlier Phase II work). These should be reviewed.

The MORT Trial at Aerojet has, in some degree, endeavored to use innovation diffusion techniques. An illustration may be helpful:

1. A project engineer, after hearing an explanation of the resources, used the Nuclear Safety Information Center and received helpful information. Two other engineers then sought information on where and how NSIC services could be obtained.
2. This should set the stage for broader acceptance in the project engineering group for information search protocols to be tested and evaluated.
3. Based on such experience, a directive will likely be developed based on trial and acceptance.

Such an evolvement is not the usual organizational approach to directives and procedures.

Note further in this case that, if a work site error occurred for lack of information search, the problem's causes could be seen in successive error layers: 1st layer, a work site error; 2nd layer, a less than ideal hardware situation; 3rd layer, a project engineer's oversight; 4th layer, deficiency in information search requirements; and 5th layer, a deficiency in promoting (or requiring) use of NSIC. Acceptance of procedures at any level may, therefore, be contingent on a higher order of procedure acceptance and use.

Thus the proceduralization and improvement of "upstream processes" - the engineering and scientific development of elements of a work situation - will likely have effects on operator acceptance of procedures. If errors in hardware or procedures are seen by operators as proceeding from vague, unproceduralized requirements in the development process, operators will probably be less likely to accept their obligations.

The alacrity with which technical and professional personnel have accepted improved hazard analysis procedures has been encouraging. When a review board described criteria for an information search and the presentation thereof as part of supporting analytics, an engineer was able to produce an excellent exhibit to support a modification within 24 hours - a short time for turn around from work open to criticism to work deserving praise.

The above two cases suggest that engineering personnel may be eager to accept proceduralization of their work if values are clear.

"Human Behavior - An Inventory of Scientific Findings"

This is the title of a text (Berelson and Steiner, 1964) believed to be useful in constructing a cogent and coherent basis for programs intended to develop acceptance. Topics covered include:

1. Habit formation (roles of rewards and punishments, varieties of rewards, and instrumental conditioning by acts as simple as a nod, a smile or expressed agreement, or programmed learning, reinforcement schedules, learning rates, transfer of training).
2. Thinking (concept formation, problem solving and creative thinking, individual differences).
3. Motivation (goal formation, striving for stimulation or knowledge, attention getting stimuli, striving for variability, interest in problems, affiliation needs, social hierarchies).
4. Face-to-Face Relations, in Small Groups. These were believed to be so important to safe or unsafe behavior that examples of findings were cited in the memo.
5. Organizations (again specific examples of findings were cited).

The Human Behavior Inventory, as well as Altman (1970), present observations on transfer of training, for example:

"If the new skill presents stimuli that are similar or identical to those in a previous learning situation, and the stimuli demand similar or identical responses, high positive transfer usually results: i.e., learning of the new skill progresses more rapidly than it would if the situation were totally new (e.g., learning motorcycling after bicycling). However, if the new stimuli are identical with the old but require similar but not identical responses, then there is only slight positive transfer: the learning situation is so close to the old one that the previous response tends to persist."

"If the new situation presents stimuli that are similar or identical to those in a previous learning situation but demands dissimilar or opposite responses, negative transfer results: the previous response persists and retards acquisition of the new one."

As Aerojet procedures reflect successive changes in a task or succession of tasks, these principles have obvious relevance to acceptance or error.

Local Data.

Dr. R. J. Nertney of Aerojet analyzed problems inherent in developing acceptance of a formal, rigid management system on a population which has essentially rural and small town background. Many excellent suggestions for improving communications were developed. What is here proposed is that the recommendations be reexamined in the context of this paper, and that attention be given to improved communications as they will particularly relate to acceptance of the formal system.

Further, Nertney also used local data to illustrate the applicability of general principles. For example: Human Factors Note #8, November 18, 1966, dealt with non-accessibility of supervisors; Note #9, November 22, 1966, dealt with changing behavior; and Note #13, January 17, 1967, dealt with tailoring instructions to the receivers' characteristics.

All of this type of material should be incorporated in a general guideline or series of references. The amount of time necessary to assemble and apply such guidelines is likely to be less than the time spent straightening out problems resulting from unguided or unstructured acceptance efforts.

Suggested Aerojet Approaches.

The findings cited above suggest that maximum acceptance of a proceduralized system is more likely to be attained if programs and day-to-day relations are based on a well-considered, cogent and coherent statement of organizational beliefs and principles. Without such a statement or guideline, management actions at various levels are more likely to be variable, ineffective, or even counter-productive. For example, the role of penalties may be capricious, emotionally biased, and even unfair. Or the recognition of rewards, intra-group relations, participation and discussion may be inadequate.

Aerojet should consider the formation of a qualified internal task force to develop an appropriate guideline.

Relation to Aerojet Programs.

Monitoring. Several new monitoring programs have been installed. If these are seen as "too much" surveillance, the programs could even be counter-productive. To what extent can the monitoring programs be cast as "a good thing because they help tell us how we are doing?"

Adequate monitoring is a factor in habit formation. Are good reports typically followed by commendation or favorable recognition to reinforce safe habits. Also, the monitoring system itself, by reinforcement of observing tasks, becomes self-reinforcing.

Monitoring reports which provide rapid, useful feedback (e.g., Shewhart Control Charts for supervisors) enable all normal administrative techniques to be used, and these can be based on sound concepts, for example, as to the role of informal groups in building acceptance.

Monitoring schemes thus far installed tend to emphasize participation or discussion. Such factors should foster acceptance.

Procedure Development.

Improved criteria, including a requirement for review with those who will do the work should help build acceptance. (Note - Aerojet has done a superlative job in this area.)

Job Safety Analysis, now being tried experimentally, should be especially helpful since discussion, involvement of leaders, and use of past experience will foster acceptance.

Safety meeting plans should be revised. The MORT text cites clues as to questionable effectiveness of meetings of the usual type. Perhaps the group which drafts the guidelines could recommend better use of meetings to work on priority problems utilizing group participatory methods.

Neither a MORT format for the hazard analysis process, nor a DOP for work performance need be seen as inflexible or immutable. If both are presented as bases for development and improvement by the personnel involved and real opportunities for participation in improvement are provided, the procedural programs themselves can help fulfill the psychological needs for growth.

Appendix J

Modified Air Force Accident Investigation Checklist

'Accident investigation is spoken of as both a science and an art. Certainly, it contains elements of both ... a controlled method/system is essential, and a clear understanding of the techniques to be used allows investigators to develop a 'feel' for what needs to be done and how far to pursue each course of action. ...

Be knowledgeable about board conduct prior to performing board duties.

Decide what organization and procedures to be used and follow plan unless you see a definite need for rearrangement. Have specific tasks assigned to individuals and insure that each is accomplished.

Explore every possible cause of the accident until it is proved to be an actual cause or ruled out.

Recognize both the extent and limitations on your own knowledge about technical subjects and call on specialists if necessary.

Not be discouraged if the cause is not immediately apparent and avoid jumping to what appears to be an obvious conclusion.

Record all evidence accurately; corroborate when possible and evaluate all statements and testimony.

Base your conclusions only on factual evidence. Be familiar with reporting requirements to effectively communicate facts, findings and recommendations to people who must take corrective action."

A section on functional responsibilities follows. The essence is that each member of the team works, and diligently, (a) as a specialty or discipline, and (b) as a group member. Also included are responsibilities for Board Chairman, Recorder, Technical Advisor, Board Member, etc.

"How is an Accident Investigation Conducted" is described as follows (slightly modified):

Initial Actions--getting started properly. Evidence can be lost while the board is trying to organize itself. Assemble and assign specific initial tasks to board members while enroute to the scene. (If board members travel by different means, do this as soon as possible).

Get a short briefing from the man who controlled the scene.

Assign additional tasks or revise instructions based on the briefing.

Go to the accident scene.

Perform a general survey of the scene to get a "feel" for the accident.

Prevent unnecessary handling or moving of wreckage.

List witnesses for questioning. Conduct a brief interview to find out what each witness might contribute. Alert him to a follow-up visit.

Photograph wreckage and the wreckage area.

Then follows a description of duties of various Board personnel in language appropriate to the Air Force. Pertinent excerpts seem to be:

1. Release of information: "Reports...are used only within the organization for the sole purpose of accident prevention. Reports are considered privileged documents, and distribution is limited. News releases should be made only by the (local) information officer."

2. Daily Meetings: "Should hold meetings of the entire investigating board at the close of every working day. These meetings should include individual board members and specialized group leader reports, instructions for the following day, administrative announcements, decisions about requirements for additional personnel/equipment."
3. Board Proceedings: "Before questioning a witness, the board must advise him of the purpose of the investigation and that the evidence may not be used in disciplinary actions, establishing pecuniary liability or line of duty status, etc.

It is important that the Chairman exercise control over the questions asked. . . Collect a list of questions to be asked each witness in advance so that needless repetition and non-pertinent questions can be avoided. Once pre-arranged questions are answered, the board can follow up with additional questions raised as a result of the testimony, but caution must be exercised to prevent wandering." (The NTSB has a pre-hearing conference to arrange orderly, relevant, non-duplicative testimony. Nothing in this procedure should inhibit a witness, but it could!)

"Eye witness testimony should be corroborated. Try to find witnesses that were located at different points so that observations can be verified or eliminated as inaccurate.

Be cautious about accepting nonexpert witness statements at face value. For example, most people will describe an inflight structural failure when parts fall off the aircraft as an 'explosion.'

Witnesses should not be interrupted while giving evidence except to prevent discussion of irrelevant topics."

Specific Checklists.

What follows is the "General Check List for Investigations" (AF-MAC, 1966) heavily edited to delete air-related items, but retaining general headings of a checklist which another type of activity should develop:

1. a. Was there an alarm system?
b. Did it function?
c. Is it adequate?
d. Pre-accident planning functional in use?
2. Guards posted, cognizant of their duties?
3. a. Rescue and fire procedures functional for this specific accident?
b. Hazards and dangers of cargo (or other factors) established?
4. Medical aid and evacuations rendered promptly and efficiently?
5. All personnel concerned fully aware of responsibilities and joint purpose?
6. Official photographer arrived promptly and began photographic responsibilities without delay?
7. a. Newsmen handled efficiently, courteously?
b. Premature news releases avoided?

ON SCENE:

8. a. Witnesses present on the scene?
b. All questioned fully (names, addresses)?
c. Check made for missing witnesses?
9. Master sketch begun?
10. Search crew required?
11. Special assistance obviously necessary?
12. Any obvious signs of structural failure?
13. Diagnostic distances (between obstacles, pieces, etc.) measured and recorded?
14. Occupants identified, evacuated promptly, possessions preserved?
15. Claims officer notified of external damage?
16. Responsibilities defined in interorganization involvements?
17. Civil authorities notified?

INITIAL SPECIFICS:

18. All parts, pieces, equipment accounted for?
19. Any obvious oddities or anomalies?
20. Means of energy transfer determined in meticulous trace of evidence as to path, speed or force, etc?
21. Secondary impacts, if any, determined in relation to force? Effects?
22. Distance of travel (of energy involved) and structural displacement from initial impact measured?
23. Gouge marks measured (length, width, depth, shape, etc.) and distance between marks?
24. Manner of travel after impact taken into consideration and verified?
25. Any objects hit during post-impact travel?
26. Added all necessary data to master sketch?
27. Checked control position as necessary?
28. Recorded all pertinent environmental conditions?
29. Photo coverage checked with photographer?

DETAILED SPECIFICS:

30. Instruments: a. Photographed?
b. Sketched?
c. Readings recorded and compared?
d. Analysis given, if significant?
e. Damage described?
f. Other?
31. Operator: a. Photographed?
b. Condition described?
c. Safety device use noted?
d. Condition of items in c noted?
e. Causes of injuries described?
f. Special equipment noted?
g. Operational records, etc., checked?
h. Condition of floor, walls, ceiling, fire exits, etc., checked?
i. Lighting equipment checked?
j. Other?
32. Operator controls and setting:
a. Control positions noted, related, etc?
b. Radio settings, conditions, use, etc.?
c. Automatic controls used?
d. Position of controls noted?
e. Other?
33. Structural failure:
a. Determined operational (not impact)?
b. Causes of structural failure?
c. Impact failures excessive in terms of occupant safety?
34. Other safety features and equipment:
a. Structures allowed reasonable safety for personnel without excessive breakage? With reasonable absorption of impact forces?
b. Redesign of feature or equipment for safety considered essential?
c. Operator vision clearance adequate?
d. Respiratory equipment satisfactory?
e. Safety design of seats, height, cushions, injury potentials thereon, etc.?
f. Safety design of instrument controls for ease of use and delethalization: appropriateness of locations, materials used, strength, elasticity, and absorption qualities, etc.?

35. Malfunctioning or failure of equipment:
- Determined as preimpact?
 - Cause discovered?
 - Maintenance record and history checked?
 - Maintenance personnel questioned?
 - System failure checked throughout? Relation to failure in other systems?
 - Help of specialist(s) needed? Obtained?
 - Tech reps called on (chemist, metallurgist, etc.)?
 - Cause factors of malfunctioning and/or failure of equipment ascertained?
 - Other?
36. Structural damage:
- Preimpact and impact distinctions?
 - Any parts or pieces missing?
 - Extraneous articles involved?
 - Examined metal, wood, joints, etc.?
 - Other?
37. Energy Source:
- Damage checked, structural and operational?
 - Faults checked, structural and operational?
 - Evidence in relation to statements considered?
 - Linkage, connections, breakage, etc.?
 - Energy transfer mechanisms described?
 - Other?
38. Communication system checked?
39. Lighting system(s) involvement?
40. Sequence of accident events:
- Determined?
 - Exhibited (photography, sketch, etc.)?
 - Proved?
41. Damage (repair or replacement cost) noted?
42. Injury:
- Medical reports completed?
 - Causes of each injury determined?
 - Autopsy report for deceased?
 - Preaccident human factors checked?
 - Other?
43. Operators, Supervisors and all other personnel:
- Experience record? This type of operation? Last month? Last 24 hours? Etc.?
 - Mission capability analyzed?
 - Training history checked?
 - Mental aptitude, attitude, emotional tone, and other human factors checked? (Personal, family)
 - Other?

44. Witness information:
- Complete?
 - Testimony related to events and evidence?
 - Useless testimony omitted?
 - Other?
45. Operations:
- Personnel questioned, if appropriate?
 - Planning checked?
 - Operator attitude, conduct, etc.?
 - Messages sent, received, attempted?
 - Communications indications, technique?
 - Other?
46. Other supervision:
- Medical supervision adequate?
 - Management supervision adequate?
 - Other?
47. Photography:
- Wholly adequate, clear, orderly, captioned?
 - Emphasis techniques used as essential to clarity?
 - Other?
48. Samples:
- Suspense-date time, person or agency handling?
 - Sample reports included?
 - Other?
49. Charts and sketches:
- Adequate?
 - Appropriate? (Best media choice)
 - Master sketch details completed?
 - Nonstandard facilities, illusion producing conditions defined?
 - Other?
50. Wreckage released to salvage crew?
51. Finalized report:
- Well organized?
 - Excess wordage, statements, photographs deleted?
 - Supplementary details filed? (For example, Board Minutes.)
 - Report complete, or explanation and date additional data will be submitted?
 - Medical reports, every person injured? Autopsy for deceased?
 - All required signatures?
 - Other?

The AF-MAC (1966) document also contains appendices on processing tapes, recommending reading assignments, and a report status schematic (item, responsible person, draft, approved, reproduced).

In response to requests, the following questions were prepared as a possible improvement in routine reports:

Supplemental Questions for Accident Investigations

1. Does a written procedure or job safety analysis exist for this job?
Is it complete and correct?
2. Did the injured (and others in the work crew) have job instruction training for this job?
3. Was there a pre-job briefing?
4. What were the changes in the material, equipment, job procedure or people?

5. When did the changes (above) occur?
6. When did the supervisor last see the employee doing the task correctly?
7. When did the supervisor last see the employee before the accident?
Any special contact or observation at that time?
8. Where was the supervisor at the time of the accident?
9. If there was unsafe equipment involved, when was it last inspected?
What was its condition then?
10. When was the next inspection scheduled?
11. What countermeasures should be introduced into the system to counter the undesired change that occurred?

This page intentionally blank

Office Use

Non-Disabling

Supervisor Accident Report

Disabling (lost-time)

Name of Injured _____ Check No. _____ Date of Injury _____

Age _____ Length of Service: With Company _____ on Present Job _____

Occupation _____

Nature of Injury _____

Description of Accident

(This information is for use in preventing similar accidents. Answer questions specifically, as indicated by example.)

1. What Job Was Employee Doing Including Tools, Machine and Materials Used? (Example: Lifting a heavy casting onto a four wheel truck.)
-
-

2. How Was Employee Injured? (Example: The casting slipped from his grasp and fell on his toes.)
-
-

3. What Did Employee Do Unsafely? (Example: Tried to lift too heavy load.)
-
-

4. What Was Defective, In Unsafe Condition, or Wrong with Method? (Example: Should have had help.)
-
-

5. What Safeguards Should Be Used? (Example: Wear Safety Shoes.)
-
-

6. What Steps Were Taken to Prevent Similar Injuries? (Example: Instructed men to assist each other in lifting heavy loads.)
-
-

7. What Other Steps Should Be Taken to Prevent a Recurrence? (Example: Provide mechanical handling equipment for this work.)
-
-

Signed _____

Department _____

(Over)

- J-8 -

For Office Use Only

(Enter as Facts become available)

8. Temporary Total

Started losing time _____

Returned to work _____

Time charge _____

Permanent Partial

Part of Body _____

Per cent loss or
loss of use _____

Time charge _____

Death or Permanent Total

Time charge _____

9. Compensation \$ _____ Medical \$ _____ Other \$ _____

Issued by National Safety Council, Inc., 425 North Michigan Avenue, Chicago, Illinois 60611.

- J-9 -



ACCIDENT REPORT
2533 (Rev.G 11-66) Printed in U.S.A.

INSTRUCTIONS: STRIKE OUT WITH A DASH THE NUMBERS OF ITEMS THAT DO NOT APPLY AND THE ANSWER SPACES OF ITEMS FOR WHICH THERE ARE NO ANSWERS

BACKGROUND INFORMATION (1—19)

1. Name (last name first)	Social Security No.			1-9	2. Symbol No.	3. Age	10 1 <input type="checkbox"/> Death 2 <input type="checkbox"/> P. T. 3 <input type="checkbox"/> P. P. 4 <input type="checkbox"/> T. T. 5 <input type="checkbox"/> Other	
4. Facility	11-12	5. Division	13	6. Department	14-16	7. Section/Unit		17-18
8. Date injury was reported	9. Date of accident	19-23	10. Time of accident (Use 24 hour clock)	24-27	11. Position title at time of accident	28-31		
			Month	Day	Year			
			13. Length of service in position worked at time of injury			14. Length of company service		
			32-33					
			15. Date last time began	16. Date released to				
						a. Reg. work	b. Other work	
			17. Date of death	18. Time of death				
						<input type="checkbox"/> A.M.	<input type="checkbox"/> P.M.	
19. Exact location of accident								

ACCIDENT DESCRIPTION (20—22)

20. What job was the man doing?	J. S. A. No.	36-39
21. What basic job step was he doing?	J. S. A. Step No.	40-41

22. What happened? Describe in order (1) the man's exact physical position, (2) how he was doing the job, (3) what happened that caused the accident, and (4) the type and agent of contact. Give additional facts if necessary. [For example: The injured was standing $\frac{3}{4}$ way up a 12' ladder, positioned so the top rung rested against a 12" vertical steam pipe. He had his left arm around the steam pipe for support. He used a sledge hammer in his right hand to bang on the frozen air line. As he did so the ladder pivoted on the vertical pipe causing him to fall to the floor below. The ladder was not tied on, nor was it held secure from below, although a helper was present. Job done frequently in freezing weather because of frequent air line freezing.]

Accident Type
42-43

Accident source
code 44-46

ACCIDENT CAUSE ANALYSIS (23—26)

23. What did the injured or other persons do or fail to do that directly contributed to the accident? Don't use words like "carelessness." Be specific; for example: "He failed to shutdown machine before beginning adjustment."

Man cause code 1
47-48

Man cause code 2
49-50

24. Check those items (below) that in your opinion were responsible for what was done or not done and which contributed to the accident. More than one item may apply. Write in Information
81-82, 83-84, 85-86 when necessary. Omit if No. 23 does not apply.

INJURED OR OTHER PERSONS:

- | | | |
|--|---|---|
| 01 <input type="checkbox"/> Did not know of hazard | 08 <input type="checkbox"/> Was emotional | 14 <input type="checkbox"/> Was not wearing personal protective equipment |
| 02 <input type="checkbox"/> Did not know safe way | 09 <input type="checkbox"/> Was fatigued | 15 <input type="checkbox"/> Other underlying causes..... |
| 03 <input type="checkbox"/> Had low level job skill | 10 <input type="checkbox"/> Was ill at time | |
| 04 <input type="checkbox"/> Tried to gain or save time | 11 <input type="checkbox"/> Had temp. injury handicap | |
| 05 <input type="checkbox"/> Tried to avoid effort | 12 <input type="checkbox"/> Had perm. physical handicap | |
| 06 <input type="checkbox"/> Tried to avoid discomfort | 13 <input type="checkbox"/> Had poor vision, hearing | |
| 07 <input type="checkbox"/> Failed to pre-plan job | | 16 <input type="checkbox"/> Unable to form opinion of underlying causes |

(OVER)

ACCIDENT CAUSE ANALYSIS (23—26) Continued

25. What in the man's surroundings contributed to the accident? Consider condition or design of tools, equipment, structures, work area, personal protective equipment, etc. Be specific. (Examples: Sparks from grinding; lack of a machine guard; inadequate clearance between two specific objects; oily floor.)

Environmental cause code 1 57-58

Environmental cause code 2 59-60

26. Check those items below that in your opinion were responsible for the conditions which contributed to the accident. More than one item may apply. Write in information when necessary. Omit if No. 25 does not apply.

- | | | | |
|---|---|--|--|
| 01 <input type="checkbox"/> Wear out through normal use | 05 <input type="checkbox"/> Unsafe basic design | 09 <input type="checkbox"/> Congestion; lack of storage space | 13 <input type="checkbox"/> Inadequate illumination |
| 02 <input type="checkbox"/> Abuse or misuse by user(s) | 06 <input type="checkbox"/> Unsafe construction | 10 <input type="checkbox"/> Exposure to corrosion | 14 <input type="checkbox"/> Exposure to vibration, etc. |
| 03 <input type="checkbox"/> Required inspection not carried out | 07 <input type="checkbox"/> Required clean-up not carried out | 11 <input type="checkbox"/> Weather conditions; natural causes | 15 <input type="checkbox"/> Exposure to temperature extremes |
| 04 <input type="checkbox"/> No inspection required heretofore | 08 <input type="checkbox"/> No clean-up required heretofore | 12 <input type="checkbox"/> Inadequate ventilation | 16 <input type="checkbox"/> Failure to check before using |
| | | | 17 <input type="checkbox"/> Other than above as follows: (Be specific) |

ACTIONS TO PREVENT RECURRANCE OF ACCIDENT (27—30)

27. Check corrective actions already taken to prevent recurrence at time of this report. Mark "P" those actions that are planned, but remain to be taken. More than one item may apply. More than one level of supervision may take or plan corrective actions listed.

- | | | | |
|--|---|--|---|
| 01 <input type="checkbox"/> Reinstatement of man involved | 06 <input type="checkbox"/> Permanent reassignment of man | 11 <input type="checkbox"/> Revision of JSA ordered | 16 <input type="checkbox"/> Personal protective equipment required |
| 02 <input type="checkbox"/> Reminder instruction of others | 07 <input type="checkbox"/> Check of how others do the job | 12 <input type="checkbox"/> Repair of tool, equipment, structure, etc. | 17 <input type="checkbox"/> Written pre-job plan required |
| 03 <input type="checkbox"/> Warning or formal reprimand | 08 <input type="checkbox"/> Improved inspection requirement | 13 <input type="checkbox"/> Improved design or construction | 18 <input type="checkbox"/> Pre-job safety instruction required |
| 04 <input type="checkbox"/> Formal disciplinary correction | 09 <input type="checkbox"/> Improved housekeeping requirement | 14 <input type="checkbox"/> Clean-up of hazardous condition | 19 <input type="checkbox"/> Substitute tool, equipment, material required |
| 05 <input type="checkbox"/> Temporary reassignment of man | 10 <input type="checkbox"/> Job Safety Analysis ordered | 15 <input type="checkbox"/> Installation of guard or safety device | 20 <input type="checkbox"/> Other departments to be contacted |
| | | | 21 <input type="checkbox"/> Other than above |

Describe details of primary corrective action:

28. Describe further recommendations to prevent recurrence. Use this space to make recommendations that are beyond your authority to undertake and require the prior approval of higher supervision.

29. Person(s) responsible for actions indicated in Items 27 and 28.

30. Date to be accomplished.

30a. Date accomplished.

MISCELLANEOUS INFORMATION (31—35)

31. Witness names and symbol numbers.

32. Was there a J. S. A. on the job? 73 33. If Yes, was it adequate? 74 34. If answer to 33 is No, was it revised? 74 35. Serious injury category (Circle proper number) 75

1 Yes 2 No

1 Yes 2 No

1 Yes 2 No

1 2 3 4 5 6 7 8 9

2 sorted by? (Name and Title)

Symbol Number

76-79

37. Reviewed by? (Name and Title)

Man Cause Code:

- 01 "Operating or using without authority.
- 02 Failure to secure against unexpected movement.
- 03 Operating or working at unsafe speed
- 04 Failure to warn or signal as required
- 05 Removing or making safety devices inoperative
- 06 Using unsafe tools and equipment
- 07 Using safe tools and equipment unsafely
- 08 Assuming an unsafe position or unsafe posture
- 09 Repairing, servicing or riding hazardous equipment
- 10 Engaging in horseplay, distracting, teasing, etc.
- 11 Failure to wear prescribed personal protective equipment
- 12 Wearing unsafe personal attire
- 13 Use of hands and feet instead of tools
- 14 Deviation from recommended job procedure of J. S. A.
- 15 Failure to keep out of danger zones
- 16 Manually lifting or handling materials improperly
- 17 Creating dangerous combinations of objects or materials"

Environmental Cause Code:

- 01 "Lack of safety devices; inadequate safety devices
- 02 Lack of warning system; inadequate warning system
- 03 Flammability or explosibility
- 04 Susceptibility to unexpected movement
- 05 Poor housekeeping
- 06 Protruding objects
- 07 Congestion and insufficient clearance
- 08 Hazardous atmospheric conditions
- 09 Poor arrangement, placement or storage
- 10 Defect of tools, equipment, etc
- 11 Inadequate illumination; excessive noise
- 12 Hazardous personal clothing
- 14 Lack of proper tools and equipment for job
- 15 Weather conditions
- 16 Animals, insects and poisonous plants
- 17 Heat or cold exposure"

It will be noted that there are many items in the Bethlehem codes which can be keyed to systems analysis. For example:

- Deviation from recommended job procedure of JSA
- Worn out through normal use
- Abuse or misuse by user(s)
- Required inspection not carried out
- No inspection heretofore required
- Unsafe basic design
- Unsafe construction
- Job Safety Analysis ordered
- Revision of JSA ordered
- Written pre-job plan required
- Pre-job safety instruction required
- Substitute tool, equipment, material required

National Safety Council Symposium on Measurement of Industrial Safety Performance
Excerpts from Report of Group III - September 17, 1970

In order to design effective measurement programs it is necessary that:

First, Goals must be clearly defined, including conflicting or potentially conflicting goals of the system or organization. We need these statements in order to judge trade-offs.

Second, the information required for a decision must be known, or at least defined. It is at least helpful, and perhaps necessary, to know what information decision-makers are likely to use when decisions are made.

Measures of effectiveness should not be separated from program. We probably cannot effectively measure program independent of program design. That is, the specific features of what it is we are trying to measure must be defined with precision, or the measures will be lacking in relevant precision.

This implies, or even urges, that measures of effectiveness be built into programs, so that data relevant to assessing effectiveness are collected before, during and after the program.

We also said that, when we collect data, we should collect data to improve program -- that is, if measurement becomes controversial, it is at least as likely that program is suspect as that measurement techniques are suspect.

We found, or thought we found, that the safety professionals as a group are apparently not aware of, or not sufficiently aware to explore, the measurement technologies which are emerging and seeming to be useful in other, not dissimilar fields -- for example, reliability, medicine, or aerospace accidents.

We felt that, for the purposes of these few days, measures had several objectives, such as:

1. Comparisons
 - a. Cross-context -- i.e., compare industries, companies, plants or departments.
 - b. Trend
2. Diagnosis (what is happening and what should we do?)
3. Effectiveness of program (Did what we did work?)
4. Parenthetically, a further purpose, that is, to describe the magnitude of a problem, national, state, or local, is important -- but definitions, rather than uniform, universally used standards will suffice for this, and gross measures are probably adequate.

Current Measures.

For current measures in widespread, general use -- this is, the frequency and severity rates defined in ANSI Z.16.1 (and two special kinds of frequency rates also therein defined) we said:

1. The ANSI standard reflects many assumptions which are (a) stated and open to serious questions, and (b) unstated (and so far as the text of the standard reveals, unexamined) but probably important.

2. These assumptions qualify and limit the usefulness of the ANSI standard.
3. If the assumptions are imperfectly understood, or imperfect, the usefulness of the standard rates will be proportionally imperfect.
4. The stated assumptions, for example, man-hours as the denominator of the ratio, can be analyzed: Is a man-hour an adequate definition of an "error opportunity" for the purpose of comparing two situations? Probably not.
5. The unstated assumptions reflected in the standard would have to be, first, identified, before they can be analyzed, and before the analysis could be examined. A standard which is silent on its major trade-off assumptions is not likely to be a good measurement tool.
6. The rates based on expanded definitions of "serious" or "disabling" injuries are essentially minor improvements on a measure that is only useful for gross comparisons.
7. When discussion turned to the current considerations of a measure based on two visits to a doctor (and which "double doctor visits" would not have to be counted) we can only report that the scientists were unimpressed and even amused. This should not be construed as meaning that the "double-doctor" rate is worse than the ANSI standard rates -- they were reflecting the inadequacy of both measurement concepts.
8. Rates or ratios are just that -- they have numerators and denominators. Much time and thought has been given to discussion of the numerator in ANSI and other rates. "Equal time" should be given to consideration of the denominator. The human factors people told us they saw their first task in useful rate construction as a careful identification of "error opportunities." Without such careful consideration, rates may have limited usefulness and may be misleading.
9. Safety performance should be reported both with and without a weighting for hazardousness in the denominator. The value of such weighting could then be ascertained.
10. The widely used rates are useful for only gross (that is, "rough" or "first try") comparisons. They probably cannot be "tinkered" into substantially greater usefulness.

Cross-Context Comparisons.

We strongly challenged the validity of present rates for cross-context comparisons -- that is comparisons of companies or other organizations, comparisons of plants within organizations, departments within establishments, or indeed functions within groups.

Having said, in using rates, give equal attention to the numerator and denominator, we then said, give equal attention to context before interpreting, ascribing meaning, to such rates.

When we told the scientists that present widely used rates resulted in a plant with a rate of 2.43 being designated as "first" or "better" than a plant with a rate of 2.58, we can again only report that they were amused.

Having said, "Give equal thought to numerator and denominator," they said,

"Give equal thought to context." The usefulness of measures for comparisons will depend on the adequacy of definitions and data on events, on exposure, and on comparability of context: low comparability of context, little usefulness; no knowledge of comparability, little meaning to comparisons.

Present rates are useful for only gross comparisons.

Trend.

When rates are used to measure trend in a unit, we do not completely escape the need to consider context — we simply, and perhaps quite usefully, limit context to changes in that unit, which are easier to judge or measure.

Statistical Significance.

A major question was raised: "Are any statistical tests of significance commonly applied in the reporting and interpretation of present measures of performance?" Unfortunately the answer had to be, "Largely, no." (Such tests are a routine part of the NSC and some other award plans, but not the usual contests or ratings.)

Thus rates as presently used often cast improper doubt on a performance, or praise a performance which was of dubious significance. Does it make sense to continuously provide management with tables of rates whose significance is unassessed and dubious?

When there are stochastic or random variations in the time, place or circumstances of accidents, this type of variation does not mean accidents are not caused. It means, in a situation where multiple causal factors are present, random variations will play a part in determining the timing of interaction of the underlying variables.

A "rash" of accidents may be essentially a random interaction of underlying factors, or it may have a special, new factor. Which is it?

We were asked whether there had been many special studies of inter-accident intervals and had to answer there had seemingly been extremely few.

Diagnosis.

There are technologies of measurement for diagnosis which are emerging and being found useful in comparable fields. They should be tried in occupational safety. Examples were:

Human Factors Engineering*

Reliability Engineering - for example, the methods of the Fault Tree, perhaps simplified, can be applied to analysis of potentials or to accidents.

Medical Science -- for example, a matrix of conditional probabilities.

(We were asked whether such matrices had been used experimentally in occupational safety and had to say we thought not.)

It was emphasized that sound diagnostic measurement requires, not only data on the accident cases, but also data on the non-accident cases (the population at risk and the control groups).

Effectiveness of program. The techniques for measures of program effectiveness also constitute an emerging, nascent technology.

* A memorandum "Description of Human Factors Reports by Sandia Laboratories" was submitted by our member, Alan Swain.

We saw a few examples of such techniques being experimentally applied in other fields. It was urged that initial trials of advanced techniques for occupational safety be made by those who know the techniques.

The requirements for application of modern measurement technology were said to be two — trials and education. Trials require (1) guts, and (2) willingness to pay the relatively high cost of innovation.

If trials are successful, education is required for dissemination of the technology. It is not reasonable to expect to be able to "read an article" on advanced technology and then apply it.

Measures Plural. A variety of measures will be useful to decision-makers in knowing the dimensions of accident propensity, predicting the future, and lowering risk.

Useful measures are numerous, changing and dynamic, and should be self-renewing, that is, they should collect the data to improve the measures themselves.

Most of the measures need not be uniform nationally. As with medical data, many of the variables are local. Therefore collect local data on local (i.e. plant, department or function) problems — they are likely to be more reliable, more variables will be known.

Our challenge is not to develop or reform some simple, nationally applicable measurement, with simple numerical indices. It is rather to develop promising measurements which can be used in specific situations and for relevant time periods for purposes of accident study and reduction.

Measures should include records on (1) accident experience, (2) errors which indicate unsafe behavior conditions, and (3) changes which could be predictive of unsafe behavior or conditions.

Performance measures should enable judgment of (1) the individual operator or user, (2) the manager or maintainer of the accident context, and (3) the conceiver and designer of the accident context; and should go to behavior, to the tool, vehicle or machine, and to the system which controls the interactions.

We should measure and compare specific, alternate machines, personal protective equipment, methods and processes, using brand names and highly specific models and types as necessary.

Decision-Making Potential. The decision-making potentials of data and measurements should be emphasized. Current, commonly used rates are weak in decision potential. Such rates may indicate a performance is excellent when, if context were known, it is mediocre. Random variations are largely unassessed.

Measures will have greater value if they are sufficiently descriptive to suggest what should be done.

During the discussions a variety of suggestions were offered as to how decision-making potential might be enhanced.

1. The apparent general lack of cross-tabulation of data was noted many times. It was said that one-variable data tabulations indicate a rather simplistic notion of the events we are trying to measure and control.

2. Among the variables suggested for tabulation and cross-tabulation were:
 - a. Industry plus "function" — e.g., transportation, material handling, maintenance.
 - b. Energy type and energy barriers (Gibson-Haddon concept)
 - c. Types of management intervention potential
 - d. Part of body as related to the above, and adequacy of medical care.
 - e. More use of cost data. Cost data holds a potential for showing relations with non-injury events and with non-accident criteria of performance. Its use is not to be construed, ipso facto, as reflecting unconcern with human values.
 - f. Data which would show how the accident control system failed.

It was pointed out that many of these types of data are commonly sought and found in accident investigation, but that they are not commonly seen in published summaries of data.

The earlier injunction to break program into parts to effectively measure performance, was reemphasized -- that is, decision-making potential will reflect the program specificity of data.

Bi-Level Reporting. A concept of a minimum routine report plus temporary sample reports of a large number of topical concerns was explained. The human factors specialists say, for their discipline, it is possible to design questionnaires for use by non-specialists to obtain objective data. They would, however, set up two requirements for a useful supplemental report -- expert knowledge of the subject matter area, plus knowledge of questionnaire technology.

Seriousness Sequence. Early in the discussions, a concept of sequence in seriousness of events was established and proved useful during the meeting. The sequence used was:

Disaster
Multi-death
Death
Permanent Injury (can be scaled)
Temporary Total Disability (can be scaled)
Lesser Injury
 Temporary Partial (variously defined)
 Medical Attention
 First-aid Attention
No Injury Accidents
Unsafe Conditions and Unsafe Acts
Errors
 Planning
 Operational

Some of the points made apropos of such a sequence were:

1. Disasters, and fatality and permanent injuries are not proper topics for "statistical management"; but for very broad samples there may be relevant statistical data.
2. The more serious events are even more rare than the less serious events. We therefore may need to go to the less serious events to get sufficiently large numbers for more reliable statistics.
3. The non-accidents are constructively "before-the-fact."

4. However, if the less serious events are used to predict the more serious events, the limitations and validity of their predictive value must be analyzed and tested.

The obvious point was made — when an event reveals hazard, don't wait for numbers or measures to take action. On the other hand, don't go forever without numbers and measures.

Alternate Strategies. There was considerable discussion of alternate safety management strategies:

1. Emphasize the prevention of the "vital few" which account for the bulk of human and economic costs, OR

Emphasize the prevention of the "lesser many" which may also reduce the "vital few;"

and a set of alternatives of a different sort:

2. Emphasize that the greatest reductions can be achieved by correcting "accident prone work situations," OR

Emphasize "accident prone behavior."

It was probably not the function of this group to recommend alternate strategies, but it certainly was our function to point out that the strategies selected (your assumptions) may very well color the data collected.

Although the discussion seemed to favor the "vital few" approach, coupled with the "accident prone work situation approach" as management techniques, we backed off from this type of recommendation to a strong recommendation that the data collection methods and measures be such as to give a valid basis for choosing emphases and strategies.

A Few Specific Suggestions.

One member suggested that measurement of individual reactions to risk in various situations, that is, accident propensity, be not measured by verbal symbols, but by behavior measurement. However, others did not agree that we should, at this time, preclude any types of measurement.

Another member suggested that deviant behavior which was accident-producing (dysfunctional risk taking) be related to other forms of deviant behavior. Also that the aspect of out-of-plant accidents as an aspect of deviant behavior not be neglected, particularly where strong in-plant programs limit deviant behavior in-plant. There was no apparent disagreement.

Mechanisms for Progress. In a short meeting such as a symposium there is the opportunity to glimpse the potentials of a few new technologies and to infer that there are likely many more potentially useful technologies. Therefore, the need for ongoing mechanisms is evident to:

1. Help launch trials of promising technologies.
2. Identify other potentially useful technologies. (If you don't know a thing exists, it is hard to ask for it.)

Three types of mechanisms were suggested:

1. Safety institutes in universities.
2. Special purpose committees within safety organizations (e.g., NSC and ASSE) fully representative of relevant disciplines (as was NSC's alcohol committee).
3. Safety committees within relevant professional and scientific societies.

Without such mechanisms there is not likely to be adequate transfer of technology. Nor can transfer be expected without both courage and funding of a research-demonstration-trial-evaluation-application cycle.

Practicality. The first consideration of a measurement of safety performance must be to define and test its useful limits and validity. Then the measure must be made practical, administratively feasible. This latter process may involve simplified methods as well as translation into user language.

Do Something. In our closing discussions, the advice was tendered, "Don't just do research, do something!" A set of specifics was discussed and is offered:

1. We should as rapidly as possible minimize the misuse of the disabling injury frequency rate because it has the following limitations:
 - a. It does not correlate with professional judgement of plant safety program.
 - b. It does not correlate with accident costs.
 - c. It deters management safety action if rates are "average" or better. Management has been oversold on the significance of frequency rates.
 - d. It degrades safety when awards are given despite the above facts.
 - e. It degrades safety when so many people know that the classification of accidents is distorted by award motivations.
 - f. The rate is not understandable.
2. We should immediately begin to test modifications of rates to correct apparent faults:
 - a. Change the events to be counted (expand the definitions).
 - b. Change the measures of exposure.
 - c. Where man-hours are used, translate into meaningful terms, e.g., man-years, rather than an abstraction.
 - d. Test differences for statistical significance.
 - e. Explore methods of analysis of rates to increase their predictive value.
3. In recognition of the problems, we should define what we eventually want measures to accomplish.

Sweeping Change. If major improvement is to be sought, it cannot be achieved solely by "tinkering" changes, helpful as they may be. Major changes usually require more knowledge, extensive staff study, and demonstrations and evaluation.

Exhibits from the MORT Trials at Aerojet

1. Recent Crane Safety Activities at Aerojet Show the General Safety System in Operation.
2. Experimental Scaling Method.
3. Configuration Control Analytic Tree.
4. Review Criteria Used by a Reliability and Quality Assurance Representative. [REDACTED]
5. Modification and Experiment Review Board Criteria
6. Review Criteria of Nuclear and Operational Safety Representative.
7. Safety Review--Redundancy and Independence Scale.
8. Safety Review--Analytic Tree.
9. NOS Division Review Routing Sheet.
10. Fire Rating Sheet.
11. Fire Reviewer's Criteria.
12. Inspection Chart.
13. "Systems Analysis"--the RSO Forms Used at Aerojet.
14. Sample Schematics for Upstream Audit.
15. The Safety Monitoring Function--A Step-By-Step Guide.
16. Field Safety Engineer's Role.
17. Safety Program Improvement Projects.
18. Injury Control Chart prepared by computer.

EX

Exhibit 1. Recent Crane Safety Activities at Aerojet Show the General Safety System in Operation

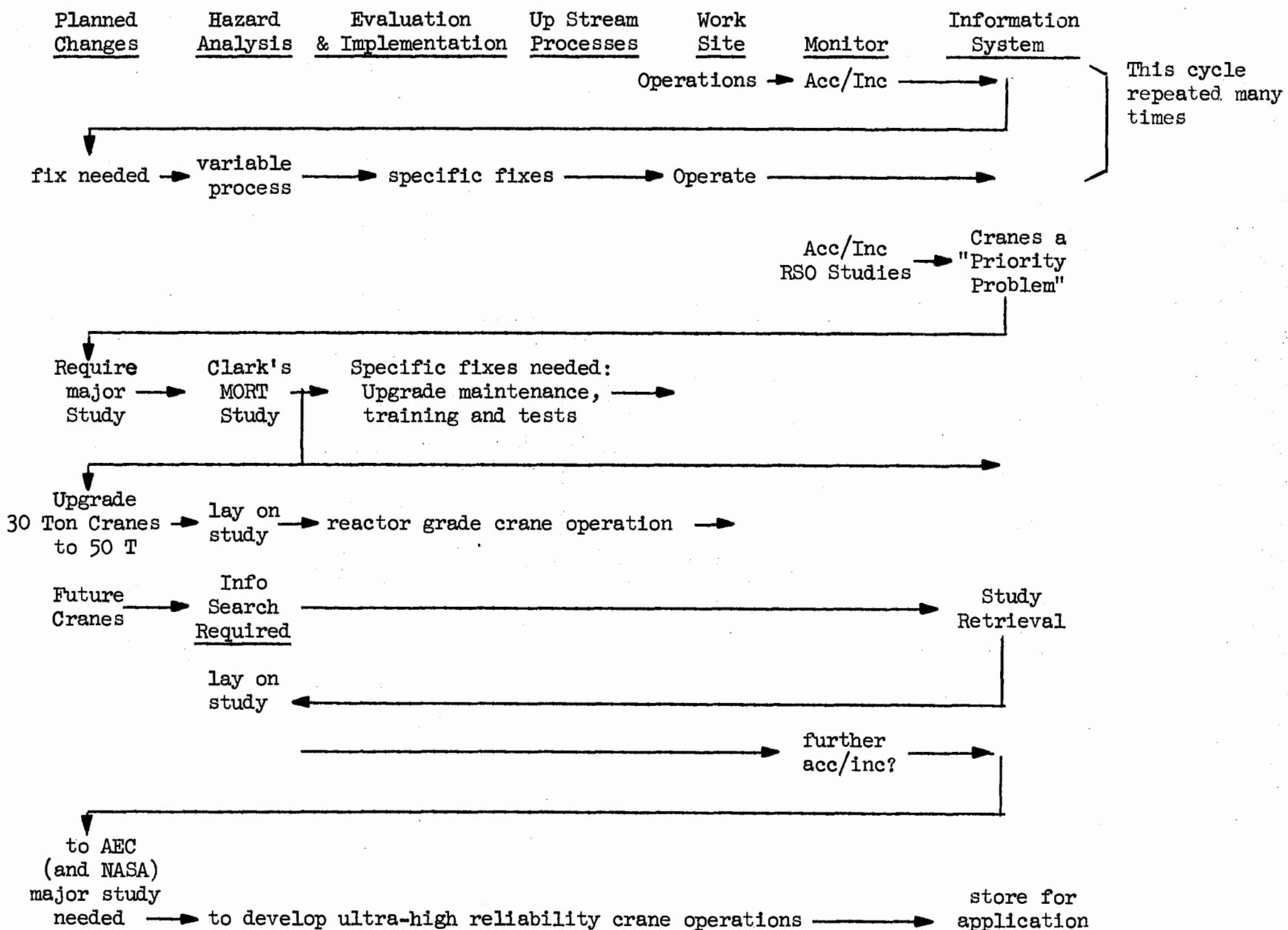


Exhibit 1.

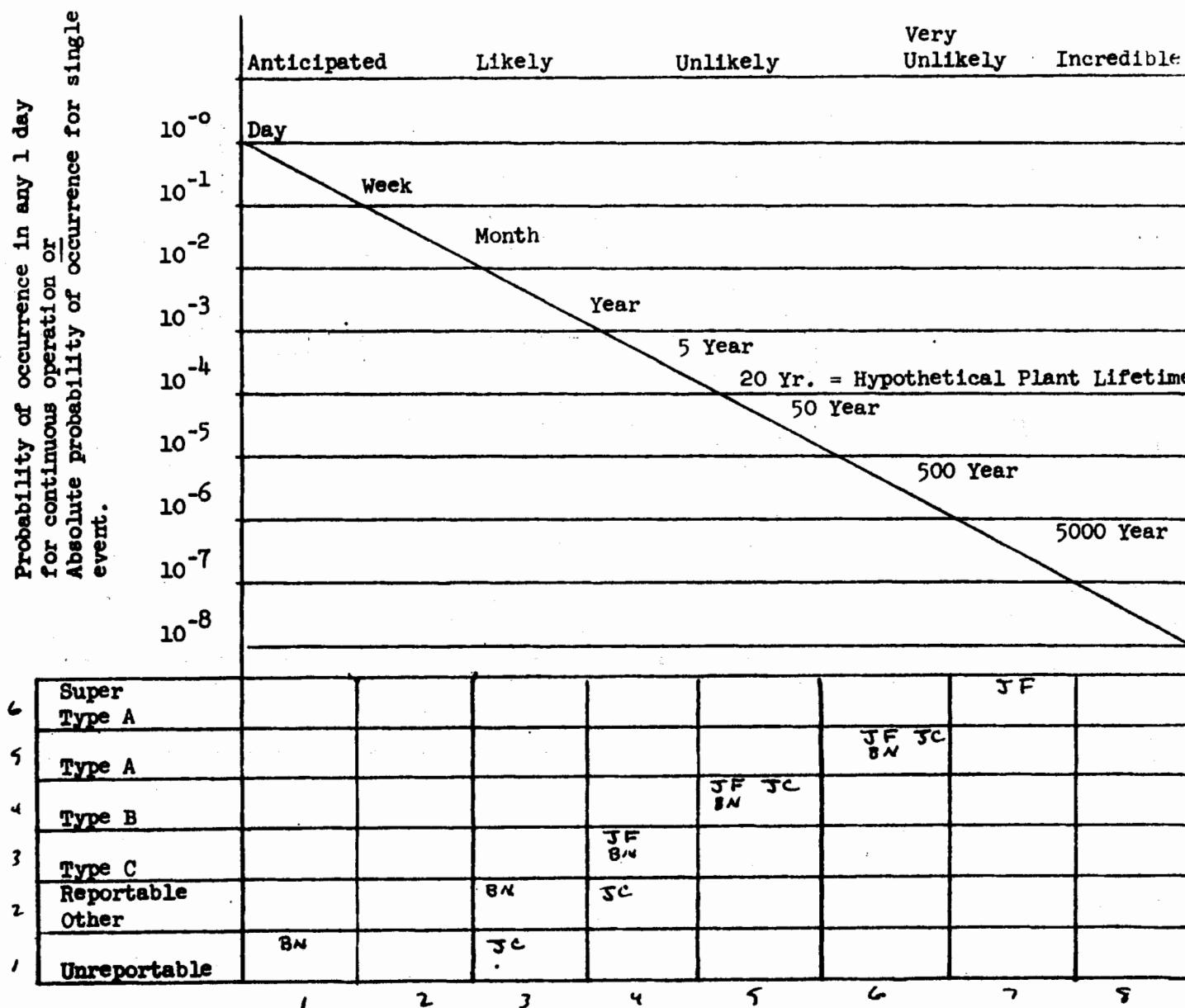
Exhibit 2.

Experimental Scaling Method

An experiment in scaling was conducted by two safety professionals and a manager. Each independently rated 36 tasks on a matrix of probability and consequences, shown on the next page. The ratings were then combined as shown by the initials in the figure. There was close correspondence between raters.

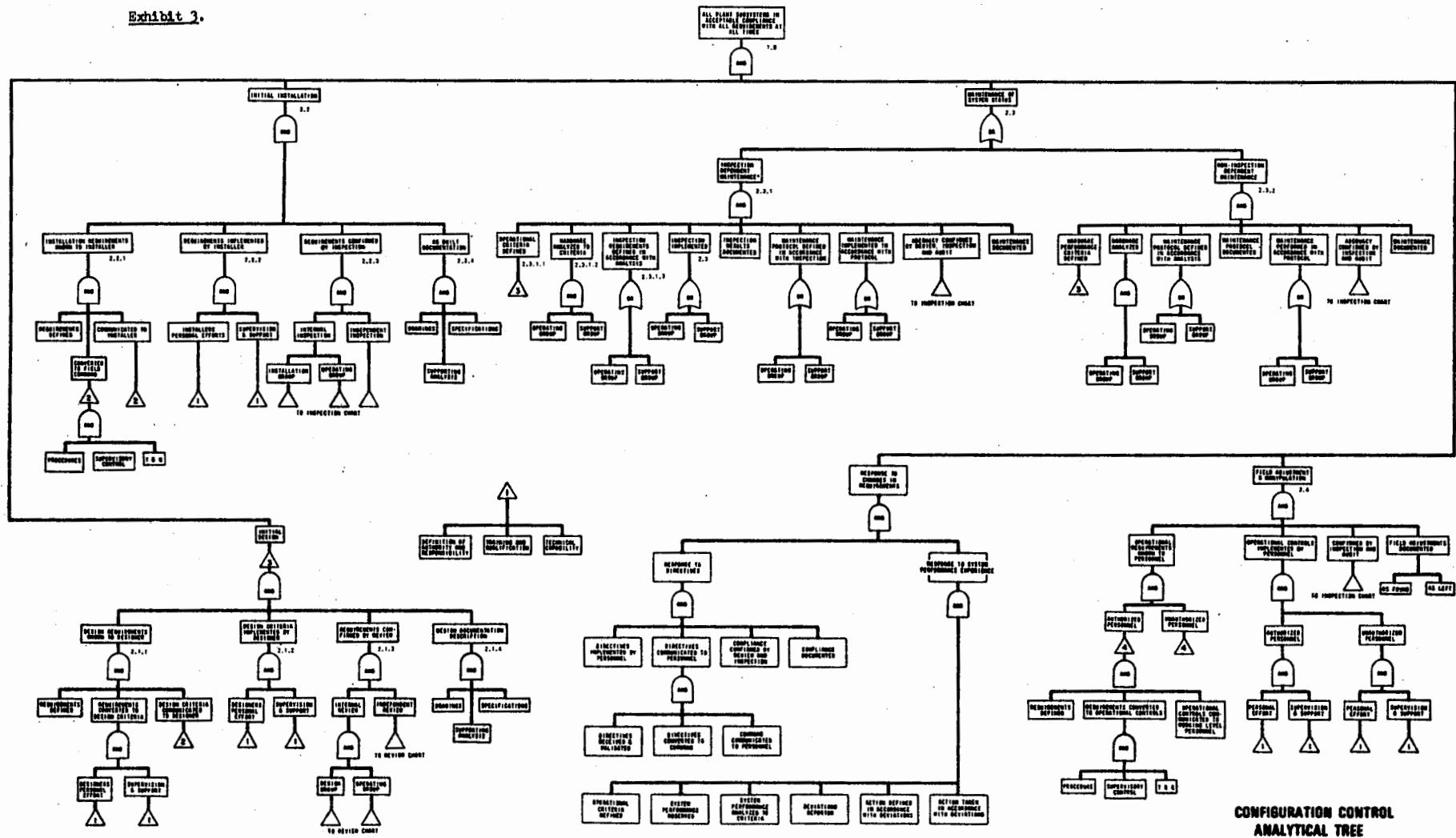
The farther the trend line is to the left, and the steeper the line, the more urgent is the process audit and review. From the ratings, the 36 potential problem areas were arranged in rank order for in-depth review by the surveillance unit in the safety division.

Exhibit 2, Crane transfer of heavy cask (> 10T). Highly radioactive material involved.



Exh.2 - 2

Exhibit 3.



CONFIGURATION CONTROL
ANALYTICAL TREE

Exhibit 4.

Design Review Criteria Used by a Reliability and Quality Assurance Representative

Conceptual Review

1. Have the operational performance criteria been established and documented?
2. Have the operational environmental criteria been established and documented?
3. Do the established performance and environmental criteria meet customer requirements?
4. Have the operational reliability requirements been established?
5. Does the predicted reliability meet the reliability requirements?
6. Have alternate designs been investigated and an optimum selection made?

Preliminary Design Review

1. Have the check list items for the conceptual review been answered satisfactorily?
2. Has a failure modes and effects analysis been completed?
3. Have all preventive/corrective actions been initiated to eliminate or minimize all modes of failure?
4. Does the current reliability assessment and prediction indicate that the reliability requirements will be met?
5. Have reliability analyses been made for alternate designs?
6. Have trade-off relationships of reliability vs. weight, volume, maintainability, cost, schedule and producibility been maximized?
7. Are safety margins for the design adequate to compensate for uncertainties in material properties, loads, environments and analytical methods?
8. Do the design specification performance limits represent values which can be attained within the development program?
9. Will the development test program as planned evaluate the performance capability of the assembly or component in all critical modes of operation to be met in qualification testing?
10. Will development tests permit evaluation of critical modes-of-failure and the ability of the assembly or component to meet specified performance limits?
11. Has a test program which includes peripheral testing been planned to investigate the achievement of specified characteristics and pertinent modes of failure?
12. Have all doubtful areas of material applications in the assembly or component relative to fatigue, creep, corrosion, etc., been investigated by the Materials Engineering Division?
13. Has a final stress analysis of the assembly or component been completed?
14. Has a complete dynamic analysis been accomplished?
15. Does the assembly or component design provide for efficiency in inspection and replacability for restoration to operational effectiveness?

16. Will manufacturing and inspection variability in dimensions and processing degrade reliability below an acceptable level?
17. Have process control procedures and inspection procedures been prepared for all assembly or component fabrication operations requiring high accuracy of adjustment, special equipment, special tools, and techniques; or where inaccessability creates special problems?
18. Does the design incorporate positive features that prohibit incorrect installations?
19. Have adequate protective equipment and procedures been provided to prevent damage to the assembly or component during fabrication handling, test, cleaning and shipping to prevent degradation of reliability?
20. Is the design conductive to the maintenance of cleanliness and corrosion resistance?
21. Have all items requiring identification and traceability been identified?
22. Have all reliability sensitive components been identified?
23. Has a parts application review been conducted for all purchased parts?

Final Design Review

1. Have the check list items for the preliminary design review been answered satisfactorily?
2. Do the design specifications conform to customer requirements?
3. Have the drawings met all checking requirements?
4. Are the process and material specifications released?
5. Do the design specifications, drawings and process and material specifications contain all necessary reliability assurance provisions?
6. Does the current reliability assessment and prediction indicate that the reliability requirements will be met?
7. Has a reliability demonstration plan been established?
8. Have all action items from previous reviews been completed?
9. Have all reliability problems been resolved?
10. Has an integrated test program been defined including incorporation of statistical techniques and reliability testing provisions?
11. If the design contains subcontractor or vendor supplied parts, have subcontractor and vendor reliability assurance provisions been required?

Exhibit 5.

Modification and Experiment Review Board Criteria

1. For Reactor Operations discipline:

- a. Design is such that the reactor and experiment systems can be safely and efficiently operated.
- b. Design permits operation within applicable specific reactor Operating Limits document.
- c. Design is compatible with other operating features of the plant and experiments.
- d. Sufficient operational information is included to develop operating procedures and designate experiment setpoints.
- e. Maintenance and service provisions have been defined and set forth.

2. For Nuclear Engineering discipline:

- a. Design work is adequate and meets necessary safety considerations.
- b. Complies with requirements of applicable specific reactor Technical Specifications and other applicable codes and standards.
- c. Sufficient installation instructions are provided to assure a proper and correct installation.
- d. Quality Control and inspection requirements are defined.
- e. Complies with the requirements of R & QA and configuration control.
- f. Effects on the ... characteristics of the reactor are such that the plant integrity is not jeopardized or the operational safety margin is not reduced below that evaluated in the safety analysis associated with the particular reactor.
- g. Conformance with existing instrumentation and control capabilities.

3. For Nuclear and Operational Safety discipline:

- a. Nuclear criticality hazards are minimized.
- b. Safety evaluation has been performed and is commensurate in scope and depth with proposed modification or experiment.
- c. Safety evaluation shows that the risk level of reactor operations is not increased beyond that evaluated in the safety analysis associated with the particular reactor.
- d. Conforms to health physics standards practices and other nuclear and operational safety requirements.
- e. Conforms with industrial safety standards and practices.

4. For Nuclear Physics and Technology discipline:

- a. Conforms to the appropriate specific reactor Technical Specifications and Operational Control documents.
- b. There is no adverse effect from the standpoint of reactor physics.
- c. Consistent with existing instrumentation and control capabilities.
- d. Required reactor physics data have been obtained and evaluated, including criticality calculations as needed.

Exh.5 - 2

5. For Reliability and Quality Assurance discipline:

- a. Quality control and inspection requirements are defined.
- b. Complies with the requirements for R & QA and configuration control.

6. For all Board Members:

- a. Conclusions stated in proposal package are clearly supported by appropriate analyses.
- b. Risks and system degradations are clearly identified.

Exhibit 6. Review Criteria of Nuclear and Operational Safety Representative

Proposal: _____

Basic Request Letter Reference: _____

Date: _____

Score	Item
	That nuclear criticality hazards are minimized.
	A safety evaluation has been performed and is commensurate in scope and depth with the proposed modification or experiment.
	The safety evaluation shows that the risk level of reactor operations is not increased beyond that evaluated in the safety analysis associated with the particular reactor.
	Conformance to Health Physics Standard Practices and the requirements contained in Reference 4.4.
	Conformance with Industrial Safety Standards and Practices.
	Conclusions stated in the proposal package are clearly supported by appropriate analyses.
	Risks and system degradations are clearly identified.
	Scoring System: 3. Criterion exceptionally well satisfied 2. Criterion well satisfied 1. Criterion adequately satisfied 0. Criterion inadequately satisfied (negative vote)

Exhibit 7. Safety Review
Redundancy and Independence Scale

Minimal redundancy
and Independence

Complete Redundancy
and Independence

Role of Safety Review Agent		
Performs primary safety analysis to operational proposals		Not involved in performance of primary safety analysis
Specifies proper codes, standards and regulations		Validates codes, standards and regulations selected by others
High degree of personal interest in operational impact of review decisions		No personal interest in operational impact of review decisions
Dependent on operating group for funding		Financially independent of operating group
Common management or supervision with operating groups or groups performing primary safety analyses		Organizationally independent of operating group and groups performing primary safety analyses
Rewrites proposals to meet review criteria or participates directly in rewrite		Rejects proposals with cause. Does not participate in rewrite
Automatically utilizes same analytical methodology as group performing primary safety analysis		Utilizes different analytical methodology and/or challenges analytical methodology used by group performing primary safety analysis

Exhibit 8.
Independent Safety Review System Analytical Tree

Introduction:

This analytical tree is designed for evaluation of independent safety review systems. It is designed to indicate those factors which must be considered in evaluating an independent safety review system and its individual subsystems and elements.

The tree does not itself result in value judgements in the areas defined. For example, the tree leads to a conclusion that "objectivity and independence" must be considered in system evaluation and goes on to define those things that must be considered in evaluating degree of objectivity and independence. It does not define the degree of objectivity required. This must be determined on a case basis depending on the nature of the material being reviewed and specific constraints imposed on the system (AECM, internal ANC requirements, etc.).

The tree is designed to be used as a part of an evaluative process which in its entirety consists of the following steps:

1. Analyze the work being conducted and identify and scale the job hazards on a probability-consequence basis.
2. Identify the independent safety review agencies and elements.
3. Relate the safety review agencies to the job hazards i.e., what review agency reviews each hazardous job or class of jobs?
4. Use the analytical tree as an outline in establishing the system requirements for each job or class of jobs, e.g., how much objectivity and independence is required, what technical skills are required, etc.
5. Evaluate the related review agency against all requirements so defined.

Key to Symbols:



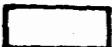
"and" gate. All subordinate items must be considered.



"or" gate. One or the other of the subordinate items may be considered. Note that in system evaluation, the basis for making the "or" choice must be clearly defined unless the option is of no concern. For example, in the case of operating reactors the "or" choice for type of review agency must be a review board (AECM 8401 requirement).



"ditto." If one reaches a ditto terminal, he must transfer to the triangle with the same number in another branch of the tree to continue downward.



Criteria to be considered.



Terminal criteria.

Independent Safety Review System Analytical Tree

Begin at the top of chart:

- 1.0 The objective of the process under analysis is to perform independent safety review in an effective manner.

1st "and" gate

- 2.0 The independent safety review process must provide for:

- 2.1 Review of Projects and Proposals
- 2.2 Review of accidents and incidents in the broad sense (evidences of the system's own failure).
- 2.3 Review of the safety review system itself (against general organizational and customer requirements and specifications).

1st "or" gate

- 3.0 Independent review may be provided by:

- 3.1 An independent review agency
- 3.2 An internal working group review process which has, itself, been reviewed by an independent review agency.

2nd "or" gate

- 4.0 The review agency (3.1 or 3.2) may consist of:

- 4.1 A review board
- 4.2 Individual review by one or more review agents functioning independently of one another.

2nd "and" gate

- 5.0 The review agency (4.1 or 4.2) must be evaluated in terms of the following characteristics:

- 5.1 Technical, Managerial and Analytical capability of the review agents.
- 5.2 The level of review effort applied.
- 5.3 The objectivity and independence built into the system.
- 5.4 The review and reporting criteria utilized.
- 5.5 The control (action) effectiveness of the Review Agency.
- 5.6 The quality of information input to the Review Agency.

Each of the basic characteristics listed above (5.1 through 5.6) will be discussed in turn. It should be noted that specific requirements which must be met by the various safety review system elements are determined by considerations external to the tree itself. These considerations involve the nature of the material to be reviewed and its associated review requirements.

Requirements are of two types:

- (a) Those requirements set external to the company, e.g., AECM-8401 requirements as clarified and interpreted by AEC sources.
- (b) Those requirements which are determined internally to ANC and which are generally based on probability-consequence considerations.

Branch 5.1 The review agents must possess:

- 5.1.1 Engineering and scientific capability appropriate to the review task.
- 5.1.2 Managerial capability appropriate to the review task.
- 5.1.3 Analytical review capability relative to the review task.

This, in turn, requires that one consider the following characteristics of the review agents as related to 5.1.1, 5.1.2 and 5.1.3 above.

- 5.1.x.1 Educational background
- 5.1.x.2 Special Training
- 5.1.x.3 Present work assignment
- 5.1.x.4 Total experience
- 5.1.x.5 Continuing processes which exist and are utilized to upgrade the review agent's techniques and skills.

Branch 5.2 The level of effort must be appropriate to the review tasks. This includes two system characteristics:

- 5.2.1 Appropriate funding and allocation of resources to each review task.
- 5.2.2 Program and schedule arrangements which permit application of resources to the review tasks in an appropriate manner.

Branch 5.3 The system must provide a level of independence and objectivity appropriate to each review task. This includes three types of personnel objectivity and independence:

- 5.3.1 The manager who has responsibility for converting the review agency's activities to control action must be sufficiently independent and objective.
- 5.3.2 The parent manager(s) to whom the individual review agents report must provide a climate which permits the review agents to function in a sufficiently independent and objective manner.
NOTE: The parent manager to an individual review agent is not necessarily the individual to whom the review agency reports.
- 5.3.3 The review agents themselves must function in an objective and independent manner.

In the case of each of the above (5.3.1 through 5.3.3) the individuals involved must have:

- 5.3.x.1 The proper personal traits to permit functioning in an effective, objective and independent manner.
- 5.3.x.2 An appropriate vertical organizational position in the working, supervision, managerial hierarchy.
- 5.3.x.3 An appropriate functional organizational position and assignments.

Branch 5.4 The review criteria used by the review agency (and individual agents) must be properly defined in such a manner as to result in appropriate review action. This requires that:

- 5.4.1 The criteria are defined in appropriate detail.
- 5.4.2 The criteria are available and known.
- 5.4.3 The criteria are appropriate to the subject under review.

There are three aspects to this definition of criteria for 5.4.1, 5.4.2 and 5.4.3 above:

- 5.4.x.1 The criteria must be communicated to the review agency by their parent manager in appropriate management control language.
- 5.4.x.2 The 5.4.x.1 criteria must be converted to a proper working language at the interface between the review agency and the reviewee groups.
- 5.4.x.3 The 5.4.x.1 and 5.4.x.2 criteria must be converted to an appropriate working language for use by the review agents themselves (for handoff to alternates and to provide consistency in the review agents day-to-day activities).

These expressions of review criteria (5.4.x.1, 5.4.x.2 and 5.4.x.3) may not be identical statements and must, therefore, be validated against one another for consistency in basic content.

Branch 5.5 The system must possess a sufficiently high degree of action effectiveness. The review activity must result in appropriate organizational response. Implementation of review agency action depends basically on three factors:

- 5.5.1 The characteristics of the review agency's parent manager already defined in 5.3.x.1, 5.3.x.2 and 5.3.x.3.
- 5.5.2 The nature of the review agency's action which includes:
 - 5.5.2.1 Go-no-go opinions based on the agencies' assigned review

criteria (approval-disapproval).

- 5.5.2.2 Conclusions and/or recommendations based on the agency's assigned review criteria.

In the case of both 5.5.2.1 and 5.5.2.2 action is dependent on:

- 5.5.2.x.1 Existence of review and reporting criteria which are relevant, sufficient and are properly interpreted and applied.
- 5.5.2.x.2 A responsive reviewee line managerial position having appropriate characteristics (5.3.x.1, 5.3.x.2 and 5.3.x.3).
- 5.5.2.x.3 A management control system which defines appropriate direct control and which provides appropriate system performance information through individual item audit and followup.

- 5.5.3 A protocol which results in appropriate submission of items to proper review agencies for review. Effectiveness of this portion of the system is dependent on three factors:

- 5.5.3.1 Characteristics of the line (reviewee) managerial position which is responsible for submitting items for review (5.3.x.1, 5.3.x.2 and 5.3.x.3).
- 5.5.3.2 The criteria which define those items which must be submitted for review. These criteria are subject to the same branch of the analytical tree as the review criteria themselves, transfer point 8 in Branch 5.4.
- 5.5.3.3 Existence of audit information which indicates performance and provides a basis for remedial action in the event of misinterpretations or other definitive or action inadequacies.

- Branch 5.6 The review agency must have appropriate information inputs. These consist of five basic sorts of information:

- 5.6.1 Proposals presented to the review agency must contain complete information relevant to the review criteria utilized by the agency.
- 5.6.2 The review agency must possess appropriate systems information relevant to personnel, plant and hardware, and procedural and management control subsystems.
- 5.6.3 The review agency must possess appropriate information regarding restraints, policies, procedures, codes, standards and regulations. This includes such material generated by ANC, by AEC and by other sources.
- 5.6.4 The review agency must have information relating to appropriate analytical methodology (both technical methodology and review methodology). This includes both:
 - 5.6.4.1 State of the art
 - 5.6.4.2 Requirements relative to prescribed methodology (e.g., requirements for formal single failure analysis, etc.)

Exhibit 8 - page 5.

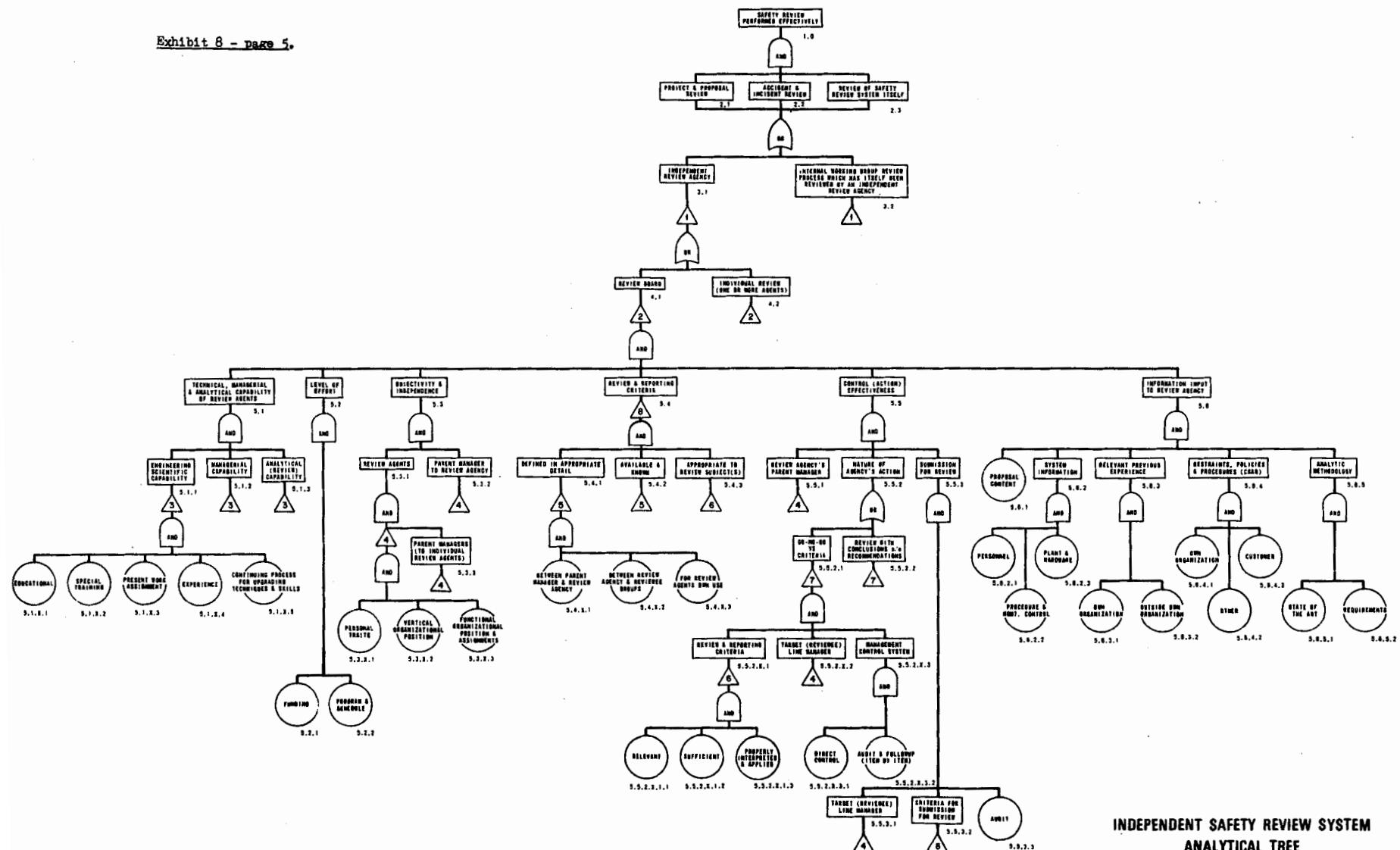


Exhibit 9.

NOS DIVISION REVIEW ROUTING SHEET

Date Out _____

Date Due _____

TITLE:

REVIEW ITEMS	Industrial Safety CRS	Health Physics JFS	Industrial Hygiene DDC	Nuc Sfty Analysis OLC	Fire Safety REC	Shipping HRO
Related Capital Equip. Proc.	X	X	X	X	X	X
General Plant Projects Proc	X	X	X	X	X	X
Internal Review System	X	X	X	X	X	X
Consequence Analysis				X		
Construction & Occupancy	X	X	X		X	
Criticality (ANPP 6.53)				X		
Emergency Preparedness	X	X				
Environmental Impact Statement				X		
Fire					X	
Health Physics		X				X
Heat Transfer				X	X	
Industrial Hygiene			X			
Industrial Safety	X					
Medical & First Aid	X					
Monitoring	X	X	X			X
Operational Suitability	X	X	X	X	X	X
OSHA Requirements	X	X	X	X	X	X
Radiation & Shielding		X		X		X
Radioactive Shipping						X
Reactor Safety				X		
SAR				X	X	
Sanitation			X			
Stress Analysis	X			X	X	
Traffic Flow & Parking	X					
Training Programs	X	X	X	X	X	X
Vehicular	X			X*		X
Waste Management		X	X	X		

* Accidents only

COMMENTS:

Comments Only Approved CA NA Letter & Date _____ Division Repres. _____

Exhibit 10.

Reviewer

Fire Rating Sheet (Ref: REC-21-72, for criteria details)

Review Subject _____

Date _____

Rating of Proposal	General Criterion	Rating of depth of Review
	Fire hazards are adequately described (qualitative).	
	Fire hazards are adequately analyzed (quantitative).	
	Adequate steps have been taken to minimize and control Fire hazards (design, monitoring emergency action, protective equipment, etc.)	
	Proposed actions and facilities are in compliance with all applicable codes, standards and regulations	

Scoring System:

- 3. Criterion exceptionally well satisfied
- 3. Reviewed carefully and conclusion is highly valid.
- 2. Criterion well satisfied
- 2. Reviewed in adequate depth to feel comfortable with conclusion.
- 1. Criterion adequately satisfied
- 1. Review marginal, but adequate.
- 0. Criterion inadequately satisfied.

Detailed explanation for "1" ratings.

Exhibit 11. Fire Reviewer's Criteria

NOS Representative:

- A. Construction and Occupancy Review
 - 1. Uniform Building Code compliance
 - 2. Exposure hazards
 - 3. Build exits requirements
 - 4. Process hazards
 - 5. Alarm and special extinguishing system requirements
 - 6. Compliance with AEC IDO Manual 12044 "Design Criteria Manual"
 - 7. General AEC "improve risk" requirements

- B. Fire
 - 1. Special Process Hazards
 - a. Flammable liquid use and storage
 - b. Pyrophoric metals
 - c. Electrical ignition sources
 - d. Heat ignition sources
 - e. What is being exposed and what is exposing the process from a fire risk
 - f. Use of approved equipment (UL and/or FM approved)
 - g. Gases
 - h. Ventilation
 - i. Special risk reduction equipment available (example: extinguishing and detection system)

 - 2. Trade Offs on the Fire Risk
 - a. Example: cost versus loss potential
 - b. Automatic extinguishing system available and in service
 - c. Availability of the fire department and trained fire brigade

- C. Operational Suitability
 - 1. Try to determine if the operation is suitable for the proposed location from a fire hazard and exposure standpoint.

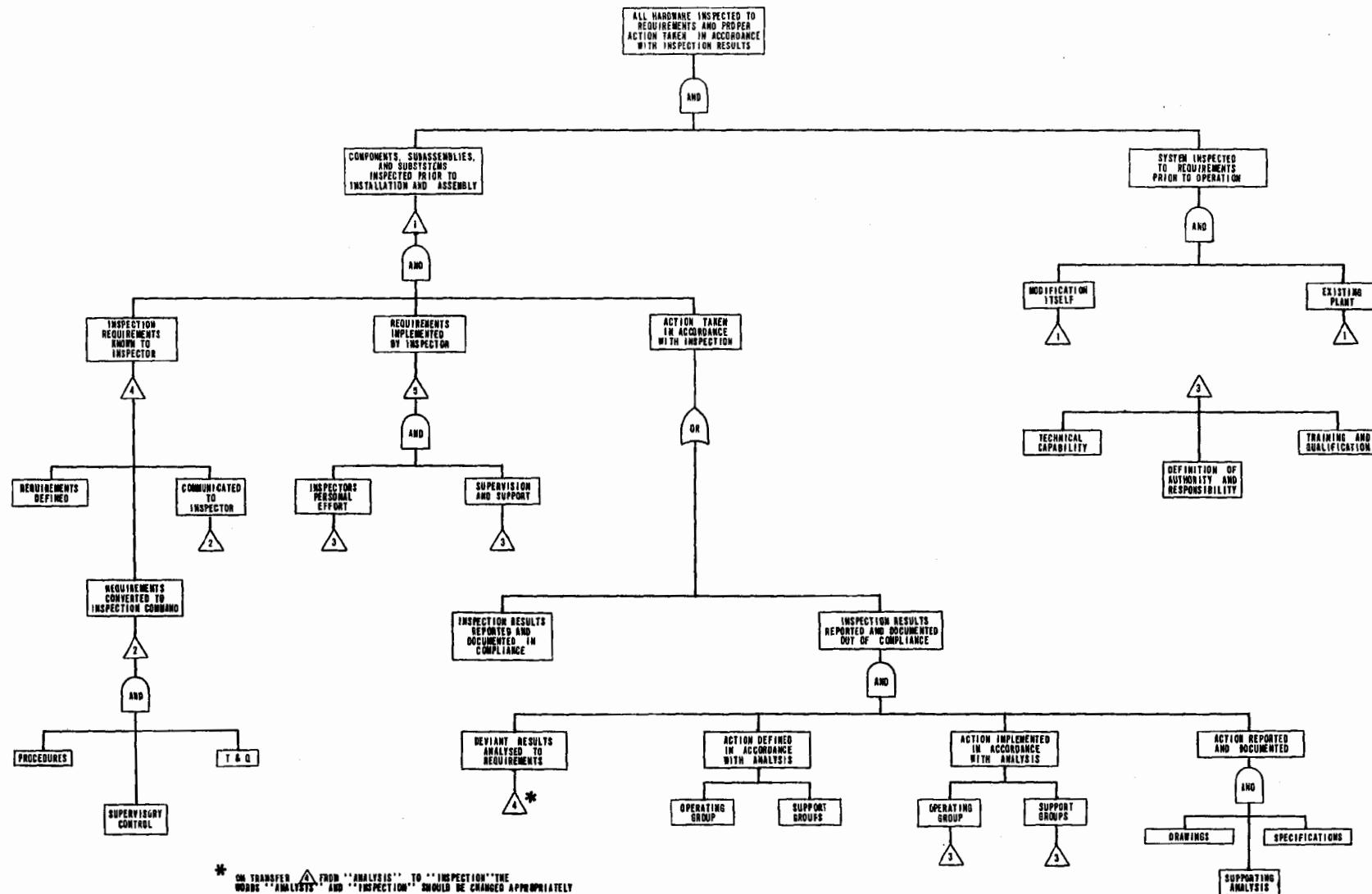
- D. OSHA Requirements
 - 1. Review proposal for compliance with OSHA requirements only for the following sections of OSHA.
 - a. Subpart E - means of egress
 - b. Subpart H - hazardous materials
 - c. Subpart L - Fire protection
 - d. Subpart N - Materials handling and storage
 - e. Subpart S - electrical

- E. SAR
 - 1. Try to determine if potential fire hazards have been evaluated for risk and if any fire potential situations have been overlooked.

- F. Training Programs
 - 1. The fire brigade is the only training program I review.

INSPECTION CHART

Exhibit 12.



* ON TRANSFER FROM "ANALYSIS" TO "INSPECTION" THE WORDS "ANALYSTS" AND "INSPECTION" SHOULD BE CHANGED APPROPRIATELY

Exhibit 13.

361
S302

"Systems Analysis" - the RSO Forms Used at Aerojet

SYSTEMS ANALYSIS
Operational Safety

1. I am in: _____ Branch, at _____ Area.
2. My job title is: _____
3. Date: _____.

As part of our continuing effort to upgrade operational safety, we would like to obtain some information from each of you.

On the following pages we will ask you for examples of jobs performed by your branch which you personally observed and in which you feel exceptionally high operational safety standards were maintained.

We will, also, ask for examples of jobs and operating situations in which operational safety standards were not so high.

Each of your examples should be a brief, factual account of something that:

1. Happened on a particular job at a specific time that you personally observed.
2. Involved handling of a job (or situation) that you judged to be especially good from the point of view of operational safety standards (or especially bad from the point of view of operational safety standards).

The examples needn't be spectacular or dramatic. Rather, they should apply to day-to-day handling of jobs and operating situations.

There need not have been an "incident" associated with your example. We're especially interested in situations which might have had serious consequences or which might result in future safety problems (under different conditions).

We, also, have a special interest in deficiencies in plant equipment and in basic plant design.

The examples should not include the names of the people involved. These reports are to be used only for research in methods and facilities improvement. We are, therefore, only interested in what happened (or might have happened); not who did it!

We've tried to anticipate some of the questions you might have regarding this study:

- Q. Why are you asking us?
- A. The answer to that is very simple. You're the experts. You're professional people and you are doing the work. It's been demonstrated time and again that the people who are doing the job are the ones who know what's going on.
- Q. Does this have anything to do with checking up on individual people in the Branch?
- A. Absolutely not! You'll note that we don't ask you to put your names on the reports and we ask you not to put anybody else's name in your examples. We're interested only in how the system works and what Branch and Division Management can do to help you in your professional goal of conducting the safest possible operation.
- Q. I've never seen anything like this before. Is this something new and experimental?
- A. This is not an experimental method. It's been used a great deal both locally and in other places.

Applications range from aircraft piloting to teaching methods at Colleges and Universities.

The method has been used in other R & D establishments including Oak Ridge engineering design shops.

Q. I've noticed that two of the questionnaire sheets are white and two are colored. Why is that?

A. We're asking you for four examples.

- (1) Most recent example of a job or operating situation in which you feel especially high standards of operational safety were maintained.
- (2) Another example of a job or operating situation in which you feel especially high standards of operational safety were maintained.
- (3) Most recent example of a job or operating situation in which you feel higher standards of operational safety should have been maintained.
- (4) Another example of a job or operating situation in which you feel higher standards of operational safety should have been maintained.

If you look at the top of the sheets you'll see that the white sheets are for good jobs (just like "white hats" are for "good guys"). The colored sheets apply to jobs or operating situations in which highest standards of operational safety were not maintained.

Q. Are you interested in any special sorts of things?

A. As we stated earlier, we're especially interested in design and equipment problems in the basic plants and supporting facilities.

We, also, have a special interest in things which are likely to cause operating incidents, especially in the older plants.

Q. What do I do when I've completed the sheets?

A. Give them to your supervisor. The results will be studied by an analyst who is not a member of your Branch.

Q. Then what?

A. Recommendations will be made to Branch and Division Management regarding changes designed to assist you in your objective of doing your job in the most safe and effective manner.

From your experience, think of the most recent situation where a job or operating situation involving your branch went especially well from the point of view of operational safety standards.

1. When and where did this happen? (Approximate date and place)
2. What equipment and/or what type of job was involved?
3. Briefly describe the situation at the time (process or reactor running, process or reactor shut down, abnormal operating conditions, etc.).

N.B. As indicated on the previous page, four forms are used. The paragraph at the top is modified appropriately. Good incidents are on white, and bad incidents on blue paper.

4. Exactly what happened? (Use other side, if necessary).
5. Why do you classify this as an example of particularly high safety standards?
6. What might have been expected from conducting the job less safely in this situation (e.g.. personnel exposure, plant contamination, gaseous or liquid effluent release, etc.)?

Exhibit 14

Project Engineering Flow Sheet

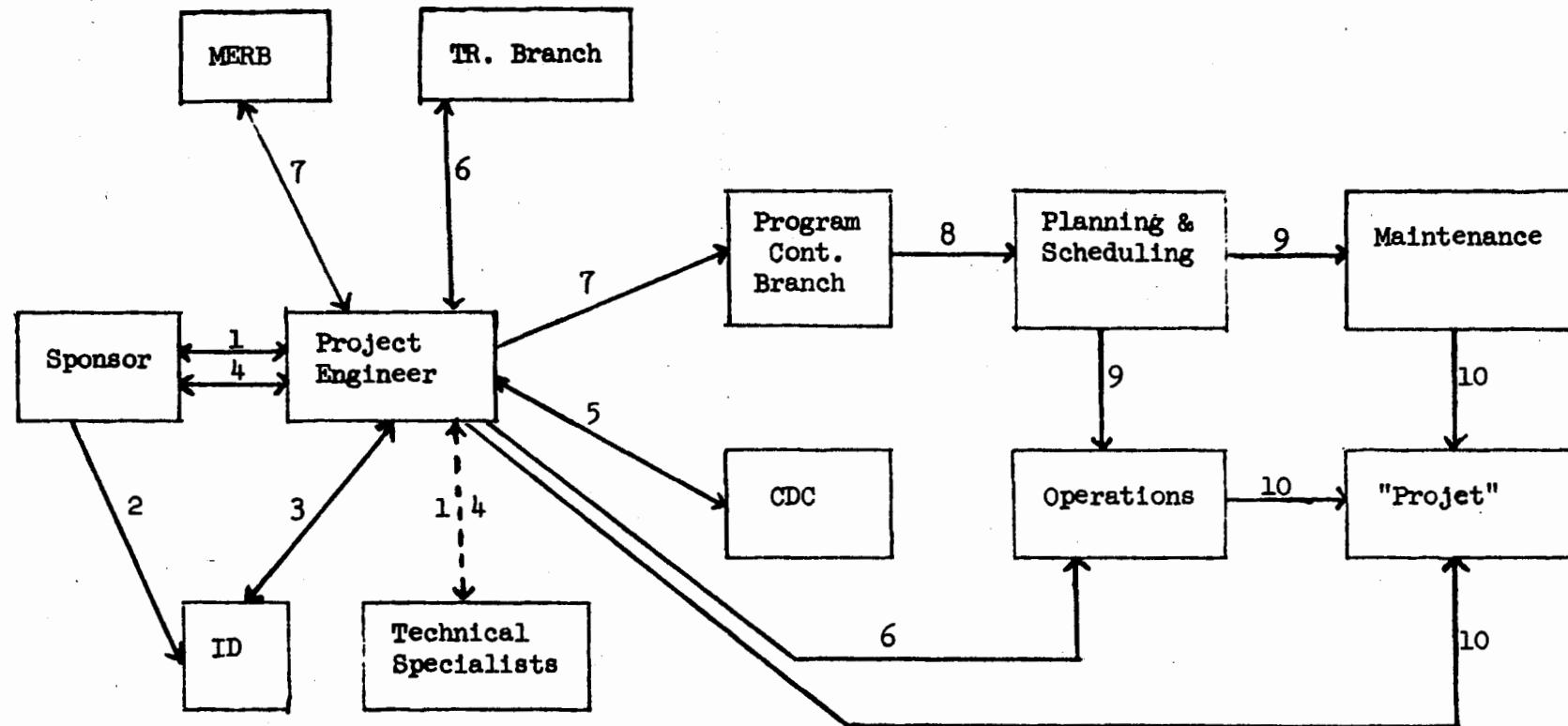


Exhibit 14 - 2

Project Engineering (Hardware Flow Sheet)



1. Sponsor ships hardware to mockup area along with radiographs.
2. Program Control representative opens shipment.
3. PE inspects the shipment (verification of right materials only).
4. PE has QA inspect the radiographs - if they are unsatisfactory, new ones are taken by QA.
5. PE writes GWA's to have equipment installed.
6. Maintenance people perform a casual inspection when installing equipment.
7. There is no real codes, standards inspection.
8. PE verifies that the installations are correct (process not formally auditable).
9. GWA's written for equipment removal.
10. GWA's written for equipment disposal (burial ground, etc.).

Exhibit 14 - 3. Project Engineering Flow Sheet

1. Sponsor and PE discuss informally the proposed project.

Safety considerations are discussed and QA standards.

Sponsor is furnished with data package requirements (FMc-126-68).

PE conducts liaison with other group specialists.

PE attempts to assure compliance with Tech. Specs. and Operating Limits.

PE furnishes Sponsor with drawings, Engineering requirements, etc.

2. Sponsor submits proposal to ID for approval.

3. PE completes an engineering study.

PE sends letter(FIM letter) to ID stating whether the job can be done or what changes are necessary.

PE assures compliance with engineering standards.

PE assures that Sponsor has complied with QA, etc.

ID approval returned to PE.

4. Sponsor and PE collaborate on formal design of project - by this time most of design is already completed.

PE obtains assistance from other Tech. Specialists.

PE has no method for recall of previous experience.

Very little contact with safety people.

5. PE generates drafts of the following documents and sends them to CDC:

1) Preinsertion procedure

2) Insertion DOP

3) Removal DOP (this must be an approved document before insertion is made).

4) Handling and shipping DOP (procedure to dispose of the experiment may already be in existence).

PE receives approved documents back from CDC (seeDRR flow sheet) but does not sign final documents (Sponsor does, however).

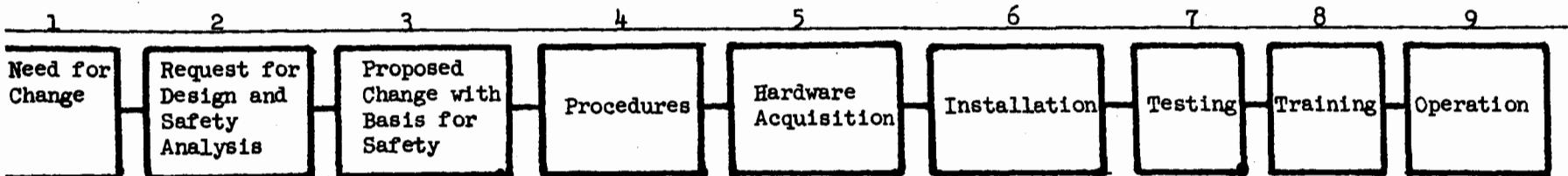
6. PE asks training branch to set up session for operation personnel.

PE has no training input to maintenance.

PE conducts training session for operations.

Exhibit 14-4. Project Engineering Flow Sheet

7. PE submits package to MERRB (must have completed a hazards analysis).
PE generates GWA's to Program Control Branch.
8. Work is scheduled.
9. Operations and Maintenance receive assignments
10. PE follows job to completion.

ATR REACTOR MODIFICATION CYCLE

1. Operations determines need for change.

2. Operations requests design and safety analysis from Engineering.

Operations not receiving adequate SAR all of the time.

Engineering-NOS interface unclear.

No evidence of literature search.

Responsibility for codes, standards, etc., rests with Engineering.

3. Completed package submitted for necessary approvals (MERB, etc.).

Operations usually must obtain additional support work from NOS-NT or others.

4. Operations writes draft of necessary procedures and submits to CDC.

Procedures routed through CDC chain including PRB.

Operations accepts responsibility for safety of procedures and compatibility with other documentation - How they assure this is not clear.

No formal "Basis for Safety" submitted for PRB review.

Formal procedures returned for Operations signatures and publication.

5. Engineering initiates hardware acquisition

Engineering assures compliance with both QA and Safety CS&R.

Not clear how this is done.

Operations and Engineering collaborate on establishing essentiality levels.

Operations and Engineering sometimes establish factory testing requirements.

Receiving inspections are performed by QA to Engineering established standards.

5. Con't.

Exhibit 14 - 6

Operations relies on QA for record retention.

No evidence of literature search for precedent hardware problems.

6. Instructions for installation originated by Engineering reviewed by Operations.

Planning and Scheduling transforms Engineering package into a smooth Maintenance package.

SWP may be required - no other safety review of actual installation.

No evidence of craft training (specific to job).

7. Operations originates "In Place Testing" requirements and Engineering writes the actual test procedures.

No visible safety review of test procedures.

Amount of testing done often limited to available "Shutdown Time" - Operations does feel that if they insisted shutdown could be extended.

8. Operations determines which modifications will require additional crew training.

Training requests then coordinated through Training Branch.

9. Reactor is operated.

Exhibit 15. THE SAFETY MONITORING FUNCTION
A Step-by-step Guide

Action	To or On	How	Who Does
A. Study	Basic plant safety analysis material	Assemble and catalogue basic safety analysis material. This includes Technical Specifications, Operating Limits, SAR material, Control documents, Procedural material, etc.	
B. Define	Key plant safety processes	<p>Extract the key processes from the material assembled in A. This will always include as a minimum:</p> <ul style="list-style-type: none"> (1) The basic personnel training & qualification process. (2) The basic hardware control processes. (3) The basic methodology for generation and control of procedural systems. <p>These will be augmented by the specific processes which protect safety endpoints.</p>	
C. Chart	Key plant safety processes	<p>Processes selected in B will be charted according to a two level charting system:</p> <ul style="list-style-type: none"> (a) A basic block diagram which indicates the essential functions which must be performed in reaching the required end-point or product (Figure I). (b) A two dimensional chart associated with each block which indicates in simple basic language "who" does "what" to implement the block (Figure II). 	
D. Analyze	Processes for oversights, omissions and lack of definition	The process of performing C will automatically make oversights, omissions and lack of definition clearly visible.	
E. Catalogue and report	Process oversights, omissions and lack of definition	Oversights and omissions are catalogued for followup and reported to appropriate management.	
F. Analyze	Processes for failure points having serious potential consequences of failure	The processes selected and charted are analyzed for steps which have serious failure consequences.	
G. Establish	Monitoring checkpoints based on consequences of failure	Monitoring checkpoints are established based on consequences of failure.	
H. Design	Monitoring systems	<p>Monitoring systems are designed and established using state of the art technology regarding:</p> <ul style="list-style-type: none"> (a) Sampling technology (b) Reduction and normalization technology (c) Validation technology 	

THE SAFETY MONITORING FUNCTION

Action	To or On	How	Who Does
I. Coordinate	Monitoring Program with: (a) Other monitoring capability in other corporate groups. (b) Technical experts.	Programs are coordinated through liaison with other corporate groups: (a) Performing monitoring functions (b) Having special skills related to state-of-the-art monitoring technology. (c) Having general responsibility for management information systems	
J. Observe	System Performance	Sample specified data at the monitor checkpoints. Observe other concurrent activities.	
K. Interrogate	Personnel in general terms	Input is obtained from field personnel relative to: (a) Acute current safety problems (b) Chronic safety problems according to a structured protocol.	
L. Analyze	Data obtained from monitoring	Data obtained from surveillance is analyzed - this includes: (a) Current data (b) Relevant historical file cabinet data	
M. Validate	Data obtained from monitoring	Data are validated as appropriate.	
N. Report	Significant findings	Significant findings are reduced and reported. This includes: (a) Negative findings (unsafe conditions and situations) (b) Positive findings (system adequate and functioning as advertised)	
O. Develop	"Fix" recommendations	Recommendations are developed in terms of two sorts of "fixes": (a) Item fixes associated with specific oversights and omissions. (b) System fixes associated with revising basic processes and systems.	

Field Safety Engineer's Role

When the monitoring plan was being developed, the role of the safety engineer was of the greatest importance in everyone's mind, but we could not scale or describe the function in the way we could other monitoring functions.

The judgements of the field engineer function at that time, and using criteria listed in Chapter 37, were: S 358-360

<u>Desired Qualities</u>	<u>Evaluation</u>
Low cost	High cost
Reliability	Fairly good
Perceptivity	Excellent
Process Audit Capability	Moderate
Action Propensity	Moderate

With proper counseling and assistance, it should be possible to increase reliability, process audit capability and action propensity. At the same time, the field engineer function should be made scalable in various ways and its precise role in the overall mission of assuring corporate safety should be identified and measured.

The criteria for

- (1) identification of work, and
- (2) evaluation on measurement

follow:

Exhibit 16 - 2.

- A. Training and Qualifications.
- B. Consultation with line management to assist in developing a comprehensive, effective safety program.

C. Present Primary Preventive Outputs

1. Search out, general
2. Accident Investigation and Review
3. Accident/Incident Data Analysis (diagnostic)
4. Periodic Inspections
5. Approval of SWP's

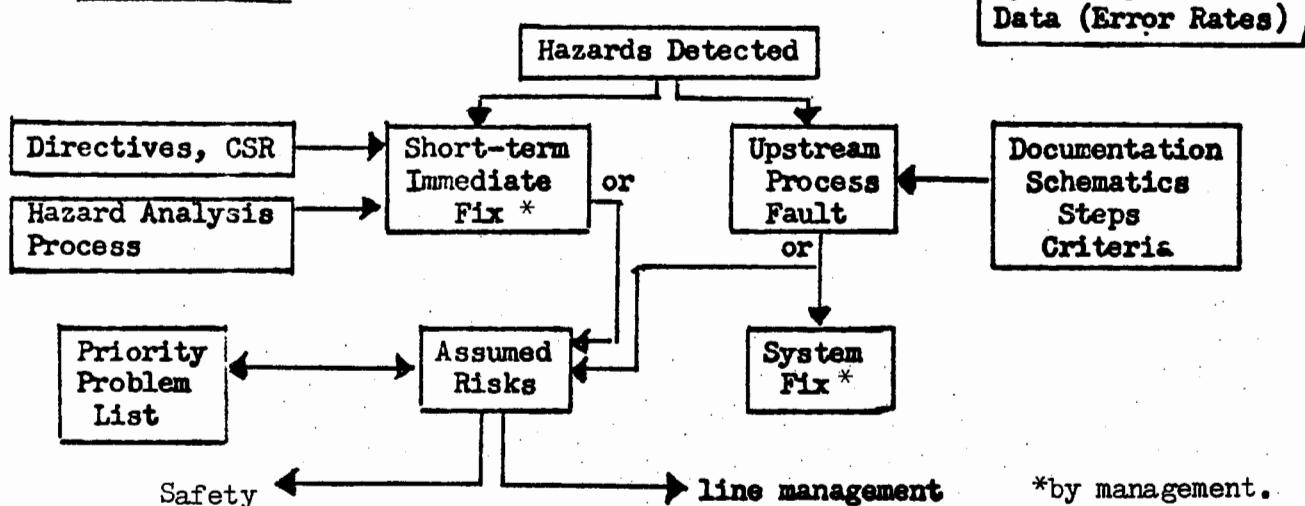
D. Proposed Preventive Outputs

1. Basic Planned Audits (see note)
2. Sampling Operations (scalable)

E. Inputs from Others

1. Annual Reviews - follow up
2. Topical Reviews - follow up as pertinent
3. Problem reports or referrals

→ D. Fix Schematic



E. Other Functions

1. Design review
2. Procedure review
3. Training
 - a. Employee safety meeting packets
 - b. Supervisor safety program
 - c. First aid training
 - d. Campaigns
4. Role in emergency planning.
5. Supervise plant nurse.
6. Process M. V. operator applications.
7. Fire duties
8. Aid evaluation of medical restrictions.
9. Issue personal protective equipment.
10. Other assignments (specify).

Exhibit 16 - 3.

- A. Training and Qualifications. Because of the tremendous range of detailed knowledge required, the importance of help and assistance from supervision and from expert specialists is emphasized, both for adequate safety coverage and for professional growth. A personal growth program developed with supervision and carried out with field assistance of supervision seems indicated.
- B. Program development skill will depend on the supervision, training and assistance provided by headquarters. For example, today only a few safety personnel can design a comprehensive monitoring program. The criteria as to what constitutes a "comprehensive, effective safety program" are less than adequate.
- C.1. Search out. This is a most valuable function when a good engineer uses his experience to ferret out hazards. The process, at its best, has been described as almost intuitive. As an adjunct of this function, the engineer develops and maintains a catalogue or inventory of hazards useful in planning his work, and very useful at any time of transition.
- D.1. Basic Planned Audit. An audit program should be developed with advice and counsel of supervision to cover agreed-upon topics.
 - a. Program Elements. A long list of topical concerns such as chemicals, personal protective equipment, ladders, etc. For each of these, criteria on the scope and nature of an audit should be established, particularly in the initial effort. Each engineer's plan would be tailor-made as to topics and schedule to fit his area.
 - b. Organization Elements. A planned audit of each organizational element scaled to the nature of the energy and work. In addition to the normal search out, a specific purpose is to detect any operation which is escaping the managerial control system (or can).

The purpose of this basic program is to provide the safety director with positive assurance that, in conjunction with other programs, a measurable degree of control is established corporate-wide.

The display for this audit duty would be along the following lines:

Program Element	Date	Findings
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
Place or Unit		
_____	_____	_____
_____	_____	_____
_____	_____	_____

D.2. Sampling Operations. No matter how small the time budget available for sampling, some time should be allocated to:

- a. Work sampling in high hazard areas
- b. Uncontrolled, random sampling of all operations or personnel.

Both of these should be designed to produce error rates and be defensible from a sampling viewpoint. This program will also require training and assistance in its early stages.

Exhibit 16 - 4.

System Operations Data. At least three programs should produce error rate data and other data for trend analysis and system assessment.

Fixes. The schematic for fixes and reporting should be made definite in order to provide the engineer with a guideline as to the action expected of him. Management is, of course, responsible for actual fixes. Again, in initial phases, training and assistance will be required to equip him to utilize functional schematics, steps and criteria in the manner developed by the operating divisions.

E. Other Functions. These are numerous and time consuming. Both the engineer and safety management must know the approximate time distribution between these and the primary preventive detection and fix work.

Establishment of Criteria

In describing the above schematic, some criteria (comprehensive program) have been alluded to.

It now seems feasible to begin to specify what criteria might be applicable to the audit function (see Figure IX-2 provided earlier). The audit schematic indicates that the field safety engineer will endeavor to assure the director and linemanagement that a specific organizational unit has an adequate system and is not failing from four viewpoints.

The corporate system includes such strong features as independent review, etc. Are they being applied?

The application of regulations, codes and standards, safe practices, and expertise is the principal thrust of the present work.

The role of changes, performance or technical troubles or problems, goal-budget-schedule tightness, changes or trade-offs inimical to safety, or high energy is forcefully clear in the semi-scale heater accident and other accidents. The field engineer may not be technically equipped to analyze work close to technological boundaries, but properly trained and assisted, he can detect the signs and signals of impending trouble.

The program elements the field engineer is to monitor seem clear. Note that two inputs are shown from Safety headquarters. Note also that the somewhat nebulous characteristics of the important function of search-out (previously described as intuitive) are now beginning to be defined by the nature of the audit.

Services by Safety Headquarters

The schematic sets the stage, not just for planning and measurement of the field engineer's work, but for measurement of the safety headquarters service role. Take any specific aspect of the field engineer's work, or one in which he is weak, and list the assistance supervision recently provided.

Exhibit 17

Safety Program Improvement Projects

Monitoring Systems

1. General
2. Critical Incident Studies
3. Safety Observation Plans for Supervisors
4. Analysis of past plans
24. Logs, etc.

Information System

5. General
6. Supplemental Reporting
7. Use of Current Data
8. MORT Analysis
9. Library Search (With AEC Headquarters)

Improve Hazard Analysis Process

10. Scaling Mechanisms
11. Criteria for Procedure Development
12. Hazard Analysis Process (including Human Factors and Independent Review)
13. Job Safety Analysis
14. Self-Discipline Method for Scientists start?
26. Special Hazard Analysis - Handling Casks with Cranes

Risk Assessment System

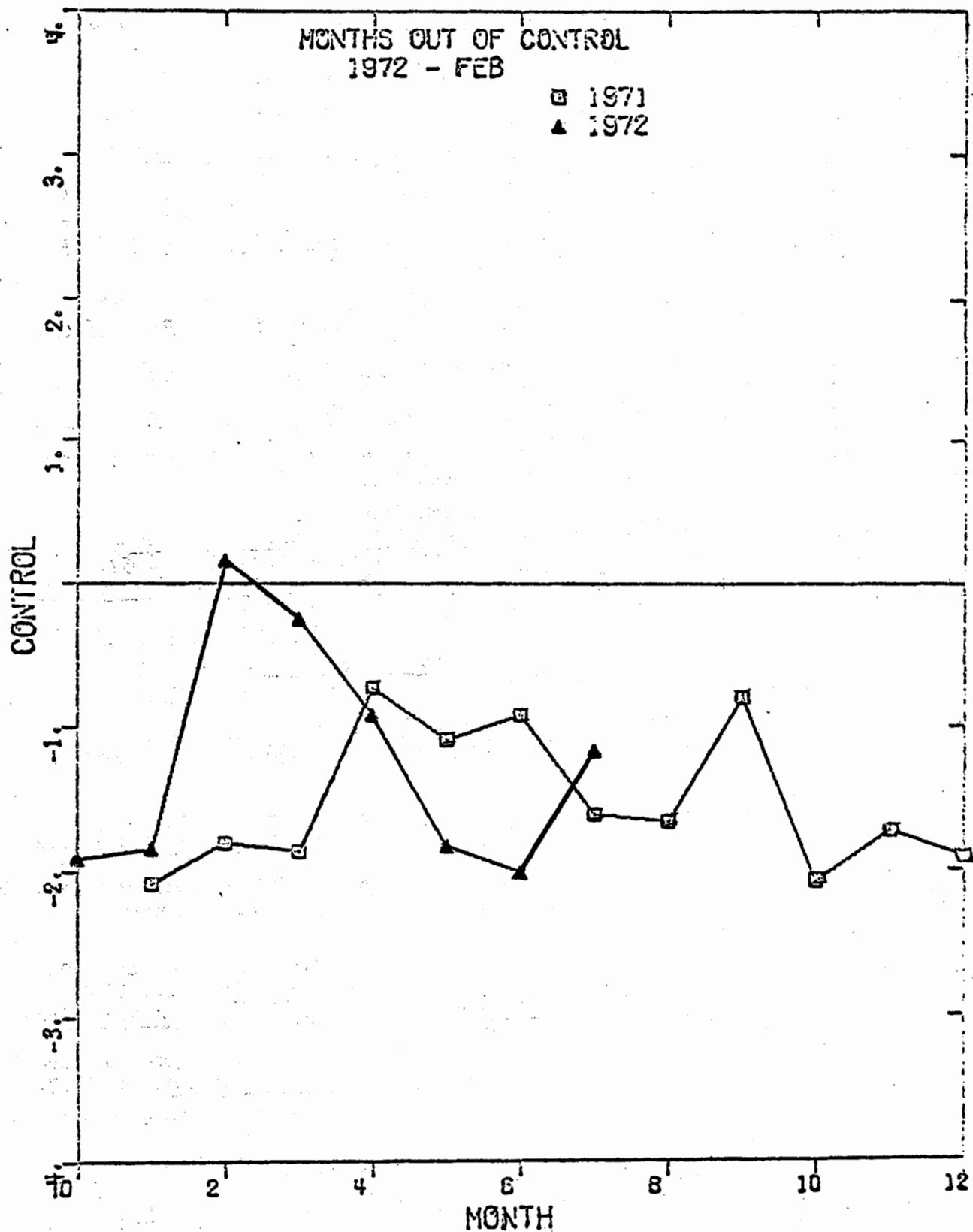
15. Safety Program Schematics) Combined as (1) Functional Schematics,
16. Safety Program Descriptions) (2) Steps, (3) Criteria, (4) Monitor Points
25. Safety Program Review
17. Risk Projection Methods
18. Risk Evaluation Feedback to Supervision (transferred to Monitoring)
19. Management Reports
 - a. Priority Problem Lists
 - b. War Rooms

Management Principles

20. Policy Revision
21. Goals
22. Breakthrough Organization
23. Innovation Diffusion
27. Acceptance of Proceduralized Systems
28. Error Reduction Philosophy and Practice
29. Safety System as Management System.

Exhibit 18. Computer-Prepared Feedback

INJURY CONTROL CHARTS-OTHERS



References

- Aerojet Nuclear. Managing by Objectives. 1971
- Policies and Procedures, Standard Practices (divisional) Detailed Operating Procedures.
- Air Force. Team Approach to Motor Vehicle Collision Investigation. Scott Air Force Base. 1967.
- Study Guide for Investigation of Aircraft Accidents. Military Airlift Command. 1966.
- An Acceptable Individual Risk Criterion. Norton A.F. Base. 1968.
- Allen, C. H. Effect of Management Attitude on Prevention and Control of Industrial Accidents. 1965. Univ. of California, Los Angeles.
- Allison, W. W. "High Potential Accident Analysis." ASSE Journal. July 1965.
- Altman, James W. "Behavior and Accidents." Journal of Safety Research. Sep 1970.
- American Institutes for Research. Experimental Study of Home Accident Behavior. 1965.
- Performance of Nuclear Reactor Operators. 1968.
- American Engineering Council. Safety and Production. Harper & Row, 1928.
- American National Standards. Radiological Safety in Design and Operations of Particle Accelerators. Dept. of Commerce. 1969.
- American National Standards Inst. Method of Recording and Measuring Work Injury Experience, Z16.1.
- Method of Recording Basic Facts Relating to Nature and Occurrence of Work Injuries, Z16.2.
- American Society of Safety Engineers. "Scope and Functions of the Professional Safety Position." ASSE Journal. Dec. 1966.
- "Search I." ASSE Journal. Jan. through June 1970.
- Selected Bibliography of Reference Materials in Safety Engineering. 1967.
- Ammons, C. H. Laboratory Study of Accidents. Montana State Univ. 1957.
- Anello, C. On Maximum-Likelihood Estimation of Failure Probabilities in Presence of Competing Risks. Research Analysis Corp. 1968.
- Armed Services Explosives Safety Board. Explosives Accident/Incident Abstracts.
- Atomic Energy Commission. Electrical Safety Guides for Research. 1967.
- "Operational Safety Standards." Atomic Energy Commission Manual.
- Quality-Assurance - Program Requirements. 1969.
- Safety Guidelines for High Energy Accelerator Facilities. 1967.
- Attaway, C. D. "Safety Performance Indicator Fills Management Need." ASSE Journal. Mar 1969.
- Bennett, Arthur & Schoeters, Tec. Financial Times. London, Jan.2, 1973.
- Berelson, Bernard and Steiner, Gary A. Human Behavior, Inventory of Scientific Findings. Harcourt, Brace and World. 1964.
- Bird, Frank E. & Gernain, George L. Damage Control. American Management Assn. 1966.
- Bird, Frank E. & Schlesinger, Lawrence E. "Safe Behavior Reinforcement." ASSE Journal. June 1970.
- Bracey, H. J. "Investigation into Effectiveness of Safety Directors as Influenced by Selected Variables." Dissertation Abstracts Intl. Jan 1970.
- Bradley, Joseph H. We Are Reporting Ground Accidents But We Are not Investigating Them. USC. Inst of Aerospace. 1967.
- Braunstein, Myron L. & Coleman, Orel F. "Information-Processing Model of Aircraft Accident Investigator." Journal, Human Factors Society. Feb. 1967.
- Brenner, Robert & Mathewson, J.H. "Principle of Accident Effect Reporting." ASSE Journal. Jan 1963
- British Chemical Industry Safety Council. Safe and Sound. Summary National Safety News. Nov 1969.
- Brody, Leon. Human Factors Research in Occupational Accident Prevention. ASSE & Center for Safety Education, New York Univ.

REF

References, page 2.

- Browning, R. L. "Analyzing Industrial Risks." Chemical Engineering. Oct. 20, 1969
____ "Calculating Loss Exposures." Nov. 17, 1969.
____ "Estimating Loss Probabilities." Dec. 15, 1969
____ "Finding the Critical Path to Loss." Jan. 26, 1970.
Canale, S. "System Safety Measurement and Control." Annals of Reliability and Maintainability. July 1966.
Caro, Francis G. "Approaches to Evaluative Research: A Review." Human Organization. Summer 1969.
Carter, Eugene E. "What are the Risks in Risk Analysis." Harvard Business Review. July-Aug 1972.
Catlin, R. J. Radiation Accident Experience - Causes and Lessons Learned. AEC 5/69.
Chapanis, Alphonse. "The Error-Provocative Situation." Symposium on Measurement of Safety Performance. NSC. 1970.
Christensen, Julien. "Overview of Human Factors Consideration in Design." National Safety Congress. 1972.
Churchman, C. West. "Suggestive, Predictive, Decisive and Systemic Measurements." Symposium. NSC. 1970.
Committee on Safety & Health at Work. Report to Parliament. Her Majesty's Stationery Office. 1972
Crawford, Paul L. "Psychological Aspects of Accidents." Safety. Autumn 1965.
Currie, Robert. "Human Factors Engineering is Optimizing Safety and System Effectiveness." National Safety News. Aug. 1968.
____ System Safety and Industrial Management. NSC. 1968.
Davis, D. R. "Human Errors and Transport Accidents." Ergonomics. Nov 1958.
Diekemper, Roman F. & Spartz, Donald A. "Quantitative and Qualitative Measurement of Industrial Safety Activities." ASSE Journal. Dec 1970.
Driessen, Gerald J. Cause Tree Analysis: Measuring How Accidents Happen and Probabilities of Their Causes. American Psychological Assoc. 1970.
Drucker, Peter F. The Practice of Management. Harper & Row. 1964.
Dukes-Dubos, Francis N. M.D. "The Place of Ergonomics in Science and Industry." ASSE Journal. Oct. 1972. (Originally in AIHA Journal)
Edwards, W., Lindman, H., Phillips, L.D. "Emerging Technologies for Making Decisions." New Directions in Psychology II. Holt, Rinehart & Winston. 1965.
Ericson, D. System Safety Analytical Technology - Fault Tree Analysis. Boeing. 1970.
Farish, Preston T. System Safety Criteria for Use in Preparation or Review of Procedures. Marshall Space Flight Center. 1967.
Farmer, F. R. Siting Criteria - New Approach. United Kingdom Atomic Energy Auth. 1967
Fine, William T. "Mathematical Evaluations for Controlling Hazards." Journal of Safety Research. 1971
Flanagan, John C. Psychological Bulletin. Psychological Assoc. July 1954.
Foundation for Research in Human Behavior. The Obstinate Audience. 1965.
Garden, Nelson B. & Dailey, Carroll. High-Level Spill at the Hilac. Univ. of Calif. Lawrence Radiation Laboratory. 1959.
Garrick, B.J. Effect of Human Error and Static Component Failure on Engineered System Safety Reliability. Holmes and Narver. 1967.
Gates, Marvin & Scarpa, Amerigo. "Risk Optimization." ASSE Journal. July 1970.
Gausch, John P. "Safety and Decision-Making Tables." ASSE Journal. Nov. 1972.
____ "Loss Control -- and the Organized Safety Effort." National Safety News. Oct. 1972
General Services Administration. Building Fire Safety Criteria. 1972.
Gibson, James J. "Contribution of Experimental Psychology to Formulation of Problem of Safety." Behavioral Approaches to Accident Research. Assn for the Aid of Crippled Children. 1961.
Goode, H. P. "New Evaluation of Accident Frequency Figures." Natl. Safety News Jan. 1949.

References, page 3.

- Greenberg, Leo. "Planning and Organizing a Graduate Program in Occupational Safety and Health." ASSE Journal. October 1972.
- "Analyzing Work Injury Data with an Electronic Digital Computer." ASSE Journal. Dec. 1972.
- Greene, Kurt & Cinibulk, Walter. Quantitative Safety Analysis. QRC (Silver Spring, Md.) 1971.
- Grieve, G. G. "Finding the Facts." National Safety News. July 1943.
- Grimaldi, John V. "Management and Industrial Achievement." ASSE Journal. Nov 1965.
- Gumbel, Emil J. "Statistical Theory of Extreme Values and Some Practical Applications." Natl. Bureau of Standards Applied Mathematics Series. 1954.
- Haddon, William Jr. "The Prevention of Accidents." Preventive Medicine. Little, Brown. 1966.
- Hammer, Willie, "Why System Safety Program Can Fail." Government-Industry System Safety Conference. NASA. May 1971.
- Hannaford, Earle S. "New Concept of Job Safety Analysis Includes Worker and Supervisor." National Safety News. Nov 1965.
- Hayes, Daniel F. "Reflections on System Safety and the Law." Government-Industry Safety Conference. NASA. 1971.
- Heinrich, H. W. Industrial Accident Prevention. McGraw-Hill. 1959.
- Hernandez, H. Paul. Safety Guidelines for Accelerators. Lawrence Radiatn Lab. 1969.
- Herzberg, Frederick. "One More Time: How to Motivate Employees." Harvard Business Review. Jan-Feb 1968.
- Hixenbaugh, A. F. Fault Tree for Safety. Boeing. 1968.
- Hughes, Charles L. "Safety Motivation." National Safety Congress Trans. 1969.
- Insurance Institute for Highway Safety. Driver Behavior. 1968.
- Johnson, W. G. [Effects of Changes] Time Exponential. NSC. 1967.
- New Approaches to Industrial Safety. Industrial & Commercial Techniques (London) 1970.
- "Overview of Accident Prevention." Journal of Industrial Medicine. 1962.
- "Park Management for Safety." Management Planning Conference. National Park Service. 1967.
- Product Safety. Industrial & Commercial Techniques. 1970.
- "Safety and Accident Investigation." Federal Regulation of Product and Industrial Safety. Federal Bar Association. 1967.
- "Report on Federal Safety Competition." National Safety News. Aug 1964.
- with Ashworth, Ray, Economos, James, Kreml, Franklin M. and Stewart, George C. Time for Decision. Amer. Bar Assn, NSC, Northwestern U. 1957.
- "Super Secret and Super Safe." National Safety News. Oct. 1945, Feb. & June 1946.
- Jones, D. F. Human Factors - Occupational Safety. Ontario Dept of Labor. 1970.
- Journal of American Insurance. A Brief History of Standards. Nov-Dec 1969.
- Juran, J. M. Managerial Breakthrough. McGraw Hill. 1964.
- Kanda, K. The Expansion of the System Safety Analysis in the Realm of Probability. Boeing. 1967.
- Kepner, Charles H. & Tregoe, Benjamin B. The Rational Manager. McGraw Hill. 1965.
- Kling, Alan L. "Meeting the Challenge of Emergency Planning." Natl Safety News Nov '67
- Kogan, Nathan & Walloch, Michael A. "Risk Taking as a Function of the Situation, the Person and the Group." New Directions in Psychology, III. Holt, Rinehart and Winston, 1967.
- Krikorian, M. See Search I. ASSE
- Lateiner, Alfred Management and Controlling Employee Performance. Lateiner. 1969.
- Levens, Ernest. "Hazard Recognition." National Safety Congress Trans. 1969.
- "Processes, Search I." ASSE
- Levitt, Theodore. "Production-line Approach to Service." Harvard Business Review, Sep-Oct 1972.

References, page 4.

- Littauer, S. B. "Analytical and Mathematical Studies of Accident Causation." Traffic Safety. June 1957.
- Livingston, William L. How Economics Guide Applied Research on Fire Protection Systems. Factory Mutual Research. 1967.
- Lundberg, B. The Allotment-of-Probability-Share. Aeronautical Research Inst. of Sweden. 1966.
- Mackenzie, E. Duncan. "On Stage - for System Safety." ASSE Journal. Oct 1968.
- Mathewson, J.B. & Brenner, R. "Analysis of Accident Statistics." ASSE Journal, Aug. 1956
- McFarland, Ross A. "Application of Human Factors Engineering to Safety Engineering Problems." National Safety Congress Transactions. 1967.
- "Human Factors Engineering." ASSE Journal. Feb 1964.
- McGlade, Francis. "Psychology in Safety Management." ASSE Journal. Nov 1967.
- McIntyre, G.B. et al. A Technique for Acquisition, Storage, and Retrieval of System Safety Information (Air Force RAIDS System). Martin-Marietta. 1970.
- McKie, Ronald. The Company of Animals. Brace and World. 1966.
- Miller, C. O. Aerospace Safety, Selected References. Inst. of Aerospace Safety and Management, USC. June 1968.
- "Hazard Analysis and Identification in System Safety Engineering." ASME/AIAA/SAE. Reliability and Maintainability Conference. 1968.
- "The Safety Information Challenge." ASSE Journal. Sep 1966.
- Montgomery, L. C. System Safety Information Exchange. Jet Propulsion Laboratory.
- Moser, W. C. "Why Safety in an Industrial Organization." National Safety Congress Transactions. 1964.
- National Academy of Engineering. Public Safety: A Growing Factor in Modern Design.
- National Aeronautics and Space Administration. Government-Industry Safety Conf. 1971.
- System Safety. NASA Safety Manual, Volume 3. 1970.
- National Fire Protection Assn. General Management Responsibilities for Effects of Fire on Operations.
- National Safety Council. Accident Facts. 1972.
- Accident Prevention Manual for Industrial Operations. 1969.
- "Has Safety Progress Ended?" National Safety News. Oct. 1969.
- Fundamentals of Industrial Hygiene. 1971.
- Motor Fleet Safety Manual. 1970.
- Report on State of the Art of Community Support and Models. 1968.
- "Safety Performance Measurement in Industry." Journal of Safety Research. Sep 1970. (full report of Symposium partially covered in Appendix M)
- Supervisor's Safety Manual. 1967.
- National Safety News. Draft Guideline For Lockouts and Tags. Nov 1970.
- "Slip Study Suggests Solutions" and "Outdoor Falls" (the latter by Davenport, T. R.). Sept. 1972.
- National Technical Safety Information Center. Progress Report. 1969.
- National Transportation Safety Board. Special Study of Risk Concepts in Dangerous Goods Transportation Regulations. 1971
- Pipeline Accident Report, Phillips Pipe Line Company Propane Gas Explosion. 1971.
- A Systematic Approach to Pipeline Safety. 1972.
- Waterloo, Nebraska School Bus Train Accident. Sep 1968. This and many other reports, particularly in occupational-related areas such as railroads and pipelines are quite valuable. A safety professional should have a sample of such reports, and probably should be on the list for future.
- Nertney, R. J. Effectiveness of Project Engineering Performance at MTR, A Critical Incident Study. Idaho Nuclear. 1965.
- Field Evaluation and Control of Personnel Behavior. Phillips Petroleum. 1965.
- Guidelines for Analysis of Step-by-Step Procedures. Idaho Nuclear. 1967
- Shift Crew Performance Evaluation at Nuclear Test Reactors. AEC. 1965.

- erences, page 5.
- elson, Dan S. The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis. Danish Atomic Energy Commission. May 1971.
- O'Shell, H.E. & Bird, F.E. "Incident Recall." National Safety News. Oct 1969.
- Patterson, D. E. and DeFatta, V. P. A Summary of Incidents Involving USAEC Shipments of Radioactive Materials, 1957-61. AEC. Nov. 1962.
- Pearson, Marion W. "Pareto's Law and Modern Injury Control." Journal of Safety Research. June 1969.
- Peters, George A. "Product Liability." Machine Design. Mar 28, 1968.
- "Human Error: Analysis and Control." ASSE Journal. Jan 1966.
- Petersen, Daniel. "Accountability - An Overlooked Key." ASSE Journal Feb 1969
- Techniques of Safety Management. McGraw-Hill. 1971
- Phillips, C. Briggs. Causal Factors in Microbiological Laboratory Accidents and Infections. U.S.Army. 1965.
- Pinkel, I. Irving. "Data Requirements Analysis in Support of System Safety." NASA Government-Industry Safety Conference. 1971
- Planek, Thomas. "Developmental Problems in Safety Research." National Safety Congress Transactions. 1969.
- et al. "Industrial Safety Study." National Safety News. Aug 1967.
- in State of the Art Community Support and Models. NSC. Mar. 1968.
- Pope, W.C. "Computers in Safety Management." National Safety News. May 1970.
- & Cresswell, T. J. "New Approach to Safety Programs Management." ASSE Journal. Aug 1965.
- , Nicolae, E. R. Safety Aids Decision-Making. Dept. of Interior. 1968.
- Rasmussen, Jens. Man-Machine Communication in the Light of Accident Records. Danish Atomic Energy Commission. July 1969.
- Recht, J. L. "System Safety Analysis." National Safety News. Dec. 1965.
- Reynolds, P. W. "What Managers Need." Industrial Protection (London). Jan. 1970.
- Rigby, Lynn V. Nature of Error. Sandia. 1970 (previously by Amer.Soc.for Quality Control)
- Rockwell, T. H. "Research Needs in Occupational Safety." ASSE Journal. Jan 1963.
- "Safety Performance Measurement." Journal, Industrial Engineering. Jan-Feb 1959.
- & Bunner, L. R. "Information Seeking in Risk Acceptance." ASSE Journal Feb 1968.
- Roethlesberger, F. J. Man-In-Organization. Harvard. 1968.
- Rook, L. W. Reduction of Human Error in Industrial Production. Sandia Lab. June 1962.
- Sandia Laboratories. Description of Human Factors Reports. Nov. 1972.
- Recommended Safety Guides for Industrial Laboratories and Shops.
- Santos, Frank "Chemical Industry - What is its Future?" National Safety News Aug 1967.
- Satterwhite, H. G. & LaForge, R. M. "A Comparison of Three Measures of Safety Performance." ASSE Journal. Mar 1966.
- Schroeder, H. M. "Safety Performance Measurement." Symposium. NSC. 1970.
- Schulzinger, M. S. M.D. The Accident Syndrome. Thomas. 1956.
- Seiler, J.A. Systems Analysis in Organizational Behavior. Irwin. 1967.
- Simonds, R. H. & Grimaldi, J. V. Safety Management. Irwin. 1963.
- Smith, L. C. "Ingredients of an Organized Training Program." National Safety News. Jan 1967.
- Stanford Research Institute. General Framework for Analysis of Costs of Traffic, Home and Public Accidents. 1964.
- Starr, Chauncey. "Social Benefit vs. Technological Risk." Science. Sep. 19, 1969.
- Stein, R.J. & Cochran, J.L. Method for Hazards Identification. NASA 1967.
- Suchman, E.A. & Munoz, R.A. "Accident Occurrence and Control Among Sugar-Cane Workers." Journal, Occupational Medicine. Aug. 1967.
- Surry, J. Industrial Accident Research - A Human Engineering Appraisal. Toronto Univ. 1968.
- Swain, Alan D. Design Techniques for Improving Human Performance. Industrial and Commercial Techniques (London). 1972.

References, page 6.

- Swain, Alan D. Development of a Human Error Rate Data Bank. Sandia. 1970.
(Previously by Department of the Navy)
- Human Element in System Development. Sandia. 1970. (Previously by Institute of Electrical and Electronic Engineers)
- Safety as a Design Feature in Systems. Sandia. 1965.
- Work Situation Approach to Improving Job Safety. Sandia. 1969. (Previously by ASSE)
- Tarrants, W. E. "Application of Inferential Statistics to the Appraisal of Safety Performance." ASSE Journal. Mar 1967.
- "Applying Measurement Concepts to the Appraisal of Safety Performance." ASSE Journal. May 1965.
- "Role of Human Factors Engineering in Control of Industrial Accidents." ASSE Journal. Feb 1963.
- "Management of Accident Control." ASSE Journal. Feb. 1972.
- Thune, H. P. "How to Investigate Accidents." Industrial Supervisor. 1969.
- Thurston, Phillip H. "The Concept of a Production System." Harvard Bus. Review
- Turner, B. T. Management of Design. Industrial & Commerical Techniques. 1968.
- U. S. Steel. Safety Program. 1964.
- Vesely, W. E. "Fault Tree Applications within the Safety Program of Idaho Nuclear Corporation." Government-Industry Safety Conference. NASA 1971.
- Vilardo, Frank "Human Factors Engineering." National Safety News. Aug 1968.
- Walton, Richard E. "How to Counter Alienation in the Plant." Harvard Business Review. Nov-Dec.1972.
- Weiner Associates. An Evaluation of Some Self-Regulatory Standards with Respect to Consumer Product Safety.
- Wiest, Jerome D. "Hueristic Programs in Decision Making." Harvard Bus. Rev. Sep-Oct 1966.
- Wilson, C. E. "Making a Performance Audit." National Safety Congress Trans. 1969.
- Windsor, Donald G. "A Survey Team's Evaluation." National Safety Congress Transactions. 1969.
- Wood, Robert C. in Governing Urban Society. Academy of Political and Social Sciences. 1967.

References on Change Phenomena

(References to Juran on control of unwanted change and achievement of wanted change, Kepner-Tregoe, Berelson and Steiner, and the author, are in the general list of references because they relate directly to safety. Adaptation to change and innovation is included in Chapter 35, "Motivation, Participation and Acceptance" and references therein are also in the general reference list.)

Henry Adams. Education of Henry Adams. Houghton Mifflin, 1918.

Robert Ardrey. The Territorial Imperative. Atheneum, New York, 1966.

H. G. Barnett. Innovation: the Basis of Cultural Change. McGraw-Hill, 1953.

Edward Bellamy. Looking Backward: 2000-1887. Dolphin Paperback, 1951.

Peter F. Drucker. Landmarks of Tomorrow. Harper & Row, 1959.

Enterprise Publications. Adjusting to Change - Ground Rule for Successful Living. Chicago. 1963. An employee distribution publication.

Fabun, Don. The Dynamics of Change. Prentice-Hall, 1967. This has an excellent bibliography on the phenomena of change.

Fabun, Don. Dimensions of Change. Glencoe Press, 1971.

Fortune. The Changing American Market. Hanover House, 1955.

Fortune. U.S.A. The Permanent Revolution. Prentice-Hall, 1951.

John K. Galbraith. The Affluent Society. Mentor Book, 1958.

Carl E. Gregory. Management of Intelligence. McGraw-Hill, 1967.

Olaf Helmer and Ted Gordon. Social Technology. Basic Books, 1967.

Eric Hoffer. The Ordeal of Change. Harper & Row, 1963.

Eric Hoffer. The True Believer. Harper & Bros., 1951.

Aldous Huxley. Brave New World Revisited. Harper & Bros., 1958.

Herman Kahn and Anthony J. Wiener. The Year 2000: A Framework for Speculation on the Next Thirty-three Years. Macmillan, 1967.

Konrad Z. Lorenz. King Solomon's Ring. Apollo Editions, 1952.

Marshall McLuhan. Understanding Media. McGraw-Hill.

Emmanuel G. Mesthene. How Technology Will Shape the Future. Processed paper, Harvard University, September 1967.

Lewis Mumford. The Story of Utopias. Compass Books, 1962.

Gunnar Myrdal. Beyond the Welfare State. Yale, 1960.

Claire Russell and W.M.S. Russell. Human Behavior. Little, Brown & Co., 1961.

Richard R. Salzman. The Impact of Change. Research Institute of America, 1964.

Donald A. Schon. Technology and Change. Seymour Lawrence Book, 1967.

William L. Thomas, Jr. Man's Role in Changing the Face of the Earth. University of Chicago Press, 1956.

Alvin Toffler. The Future as a Way of Life. Horizon, Summer, 1964.

Alvin Toffler. Future Shock. Random House, 1970.

Arnold J. Toynbee. A Study of History. Oxford University Press, 1947.

Arnold J. Toynbee. Civilization on Trial. Oxford University Press, 1948.

U. S. Cabinet Secretaries. Communities of Tomorrow Conference. December, 1967.

Norbert Wiener. Cybernetics. John Wiley & Sons, Inc., 1948.

Norbert Wiener. The Human Use of Human Beings. Doubleday & Co., 1954.

Robert C. Wood in Governing Urban Society: New Scientific Approaches. The American Academy of Political and Social Sciences, May, 1967.

REFERENCES ON HUMAN FACTORS ENGINEERING

An Index of Electronic Equipment Operability (Evaluation Booklet),
Pittsburgh, Penn: American Institutes for Research.

An Index of Electronic Equipment Operability (Report of Development),
Pittsburgh, Penn: American Institutes for Research.

An Index of Electronic Equipment Operability (Data Store),
Pittsburgh, Penn: American Institutes for Research.

An Index of Electronic Equipment Operability (Instruction Manual),
Pittsburgh, Penn: American Institutes for Research.

Mil-STD 1412, Human Factors Design Criteria for Military Systems
Equipment and Facilities.

Bennet, E.; Degan, J.; & Spiegel, J. (Eds.), Human Factors in Technology,
New York: McGraw-Hill, 1963.

Chapanis, A.; Garner, W. R.; & Morgan, C. T., Applied Experimental
Psychology, New York: John Wiley and Sons, Inc., 1947.

DeGreen, K. (Ed.), Systems Psychology, New York: McGraw-Hill, 1970.

Damon, A.; Stoudt, H. W.; & McFarland, R. A., The Human Body in Equipment
Design, Cambridge, Mass.: Harvard University Press, 1966.

Fitts, P. M., Engineering psychology and equipment design, Chap. 35 in
S. S. Stevens (Ed.), Handbook of Experimental Psychology, New York:
John Wiley and Sons, Inc., 1951.

Fogel, L. J., Biotechnology: Concepts and Applications, New York:
Prentice Hall, 1963.

Gagne, R. M. (Ed.), Psychological Principles in System Development, New
York: Holt, Rinehart, & Winston, 1962.

Gagne, R. M.; E. A. Fleishman, Psychology and Human Performance, New York:
Holt, Rinehart, & Winston, 1959.

Harris, D. H.; Chaney, F. B., Human Factors in Quality Assurance,
New York: John Wiley and Sons, Inc., 1969.

Howell, W. C.; and Goldstein, I. L., Engineering Psychology, New York:
Appleton-Century Crofts, 1971.

Lindson, P. H.; and Norman, D. A., Human Information Processing: An
Introduction to Psychology, New York: Academic Press, 1972.

McCormick, E. J., Human Factors Engineering, 3rd Edition, New York:
McGraw-Hill, 1970.

McFarland, R. E., Human Factors in Air Transport Design, New York:
McGraw-Hill, 1946.

- Meister, D., Human Factors: Theory and Practice, New York: Wiley-Interscience, 1971.
- Meister, D; & Rabideau, G. F., Human Factors Evaluation in System Development, New York: Wiley, 1965.
- Morgan, C. T.; Cook, J. S.; Chapanis, A.; & Lund, M. W., Human Engineering Guide to Equipment Design, New York: McGraw-Hill, 1963.
- Murrel, K. F. H., Human Performance in Industry, New York: Reinhold Publishing Co., 1965.
- Parsons, H. M., Man-Machine System Experiments, Baltimore, Md.: The Johns Hopkins University Press, 1972.
- Singleton, W. T.; Easterby, R. S.; & Whitfield, D. (Eds.), The Human Operator in Complex Systems, London, England: Taylor & Francis Ltd., 1969.
- Singleton, W. T.; Fox, J. G.; & Whitfield, D. (Eds.), Measurement of Man at work: An Appraisal of Physiological and Psychological Criteria in Man-Machine Systems, London, England: Taylor & Francis Ltd., 1971.
- Stok, T. L., The Worker and Quality Control: Bureau of Industrial Relations, University of Michigan, 1965.
- Swain, A. D., Design Techniques for Improving Human Performance in Production: Industrial and Commercial Techniques Ltd., 30-32 Fleet Street, London E. C. 4, January 1972.
- Woodson, W. E.; & Conover, D. W., Human Engineering Guide for Equipment Designers, 2nd Edition, Berkely, Calif.: University of California Press, 1964.

INDEX

The underlined references below index the principal discussions of a topic. The parenthetical references index the MORT diagrams and outline. Note that the MORT diagrams (pages 149-156) and the fourth generation MORT list (pages 159-163) are also indexed to the pertinent text.

- Acceptance 337, Appendix I
Accident 25-26, 140, (149, 162)
Accident Rates
(See Incidence analysis)
Accountability (150, 159), 198
AEC i, 8, (160), 412, 422, numerous others
Aerojet ii, 10, 14, 118, Exhibits 1-18, numerous others
Alternatives 90, (151, 160), 186, 208, 219, Appendix B
Amelioration 140, (149, 152, 153, 162)
Analysis methods (149-151, 160), 188 248-259, 380
Arrangement (153, 161) 269
Audit 212-3, 361, 371, 453
Barriers 33-36, 141, (149, 152-3, 161-2), 218, 268
Breakthrough 119, 208
Budgets (150, 155, 159), 189
Catastrophe 206, 229, 343, 250
Change 27, 59-77, 114, 121, (150-1, 155, 161), 211, 233, 253, 262, 270, 385
Cause analysis 137, (150), 398, 401
Codes (see Standards)
Conceptual phase (151, 153, 160), 237-265
Configuration control (162), 270, Exhibit 3
Consequences 219
Construction 18
Control 118, 208
Controls (153, 161), 267, 362, Exhibit 18
Costs 176, 232 (also see Investment)
Criteria (150, 159, 160) 185, 207, 220, 238
Critical incidents 116, (150, 155, 160), 187, 233, 262, 361, Appendix D, Exhibit 13
Data analysis 372, 415-434
Delays (150, 155, 159), 189, 191, 306
Design 97, (149, 151, 161), 223-289
Deviations 114 (156), 334
Directives (150, 159), 193
Disposal (151, 161), 270
Documentation (151, 162), 271
Efficiency 107-110, 177
Emergencies 140, (152, 155, 161), 270, 306
Employee relations 181
Energy 31-36, 141, (149, 153, 161-2)
Enforcement (156), 335
Environment (153, 161), 269
Environmental Chamber case 135, Appendix A2
Environmental Impact (160), 259, Appendix E
Error 27, 49-57, 117, 123, (154-5, 160), 250, 273-280, 331, 357 tolerance limits, 52
~~Error Sampling 358/359~~
Failure-Mode & Effect 216, 250
Fault Tree 143, 250-53
Feedback 113, (150), 198, 299, 337 (also see Monitoring)
Fire 41, (152), Exhibits 10-11
Fix Controls (160), 343
Goals 4, 113, (149, 159), 206, 237
Hazard 28, 93, 253
Hazard analysis process 5, 105, 114, (149, 151, 160, 162), 223-289
Hazard identification 98, 248
Health (160), 373
HE Press case Appendix A3
High potential (150), 211, 233
Hilac case 135, Appendix A1
Human Factors Engineering (153-4, 161) 273-280
Incidence analysis 415-434
Incident 27, 140, (149, 162)
Incident Recall (See Critical Incidents)
Independent Review (151, 153, 162), 283-289, Exhibits 5-11
Information systems 114, (149, 150, 159, 160), 262, 343-409
Innovation Diffusion (156), 338, Appendix H
Inspection (149, 151, 154, 161, 163), 269, 312, Exhibit 12
Investigation (150, 159), 375-89, Appendix J
Investment/Benefit/Value/Threat 256-8
Job Instruction Training 301
Job Safety Analysis (155), 301, 317, 321, 333
Key word index 116, 400
Known precedent (150, 159), 343
Lawrence ii, 62, 135, 228 and others
Life cycle 98, 148, (151, 160), 225, 263
Line responsibility (150, 159), 190

INDEX

Index, page 2.

Logs (155), 304
Maintenance (149, 151, 154, 161, 163), 250, 269, 311
Management needs 205
systems 114-130, 139, (149, 159), 173-221, 199
role, 96, 175-184
Management Oversight and Risk Tree 6, 12, 21, 133-171, 383
Matrix 37-47, 420
Measurement 129, 415-434, Appendix K
Medical service 140, (152), 373
Method vs Content 103-106
Monitoring 5, 99, 114, (150-1, 153, 155, 160-1), 343, 351, 395, 446, Exhibit 15
MORT, examples Appendix A
Motivation (151, 156, 161), 337-342, Appendix G
Motor vehicle 19
National Safety Council ii, 7, 81, 110, 412, others
National Aeronautics & Space Adm 11, 225-6, 239-41, 412
National Transportation Safety Board 11, 80, 83, 217, 231
Operability (151, 161), 269
Organization, safety 193
OSHA 6, (160), 178-180, 260
Participation 114, Appendix G
Peers (150), 453
Performance 107-110, 114, 127, 177
Personal conflict (156), 338
Policy 113, (149, 159), 175-184
Practicality 15, 182
Pre-Job Analysis (155), 293
Priority Problem Lists (150, 160), 234, 435-9
Probabilities 4, 210, 216, 218
Procedures 127, (151, 153, 154, 161), 269, 315-324, 408, Appendix F
Program, safety 202, 445
measurement, (149, 150, 162)
Projections 415-434
Public protection 180
Quality assurance 281-2, 365, Exhibit 4
Radiation 42, 427
Rates (150, 160), 211, 432
Recorded Significant Observations (See Critical Incidents)
Regulations 5, (160), 178-180
Rehabilitation (152)
Reliability 263, 281-2, Exhibit 4
Rescue (152)
Research 97, (150, 159)
Research Work 18, 19
Review (see Hazard Analysis Process, Independent Review)
Risk 28, 33, 46, 85-91, 114, (149, 160), 237
residual, 91, 99, 139, 220
Risk Assessment System 90, (149, 159, 160), 205-221, 346, 435
Safety Precedence Sequence 98, (160), 225
Safety Program review 131, (150, 162), 211, 371, 445-456
Sandia ii, 275, 318, 421, and others
Scaling 5, 44, (151, 160), 238-248, Exhibit 2
Schematics 193-5, 304, 369, 446, Exh.14
Selection, personnel (151, 156, 161), 325
Sequences 54, 79-83, 382
Services (150, 162), 195-197, 455
Staff (150, 159), 192
Staff, safety 96, (150, 162), 445-456, Exhibit 16
Standards (150, 159, 160), 260, 262, 281
Suggestion systems (155)
Supervision 96, (149, 151, 155, 161, 163) 297-310
Symbols, Tree 143
Systems 14, 75, 111-130, Appendix B, Exhibit 1
System Safety 3, 95-102, 225-232
Tasks (154, 155), 276, 332
Test (151, 153, 161), 269, 281
Training (150-1, 155-6, 159, 161), 195, 300, 327
Transfers (155), 303
Transition 23, 102, 170, 457-61, Exh.17
Transportation 19, 230, 250
Triggers (149, 150), 233
Unsafe Acts and Conditions 27, 56, (155), 404
Upstream processes 113, (160), 367
Values 175, 207
Vigor (150, 156, 159), 200
Warnings (153), 268
Welfare 175
Work Flow Process 113, 291-342
Work Permit (155), 332
Worst Potential Lists (see Priority Problem Lists)