InComTec

in the United Kingdom, Germany, Holland, Scandinavia, Switzerland and South Africa

New approaches to SAFETY IN INDUSTRY

INDUSTRIAL & COMMERCIAL TECHNIQUES LTD.

30-32 FLEET STREET, LONDON E.C.4. (LUDgate Circus 7757)

- ★ Public seminars and courses on wide range of techniques in industry and commerce.
- ★ Private seminars on Company premises.
- ★ Textbooks and Reference Manuals.
- ★ Home Study Courses.
- ★ Calculators and Counters.

InComTec **INDUSTRIAL AND COMMERCIAL TECHNIQUES LTD.**
30 FLEET STREET, LONDON, E.C.4.

Tel: 01-583 7757
Cables: Incomtec London E.C.4.

Directors:
J. R. Blinch (Managing)
A. R. Brackenridge, F.C.A.
D. Jordan
Professor R. W. Revans, M.Sc.Tech., Ph.D., M.I.Min.E.
B. T. Turner, M.Sc., C.Eng., F.I.Mech.E., M.I.C.E.

N E W A P P R O A C H E S T O

S A F E T Y I N I N D U S T R Y

by

WILLIAM G. JOHNSON

Former General Manager of the U.S. National Safety Council

Printed in England.

January, 1970.

NEW APPROACHES TO SAFETY IN INDUSTRY

W. G. Johnson

INTRODUCTION

Improved technological methods for attaining high ideals of safety are available today. The methods spring largely from the U.S. military, aerospace and atomic energy industries, where a high goal has been set: "First Time Safe". The U.S. record of the weapons, space and reactor programs attests to the effectiveness of the methods.

System safety analysis concepts have been highly developed by the U.S. Defence and Space agencies and existing specifications require forms of analysis which provide a high degree of protection of both systems and personnel, where necessary by complex and sophisticated methods.

On the other hand, U.S. occupational injury rates in general, after several decades of downward trends, have been on a plateau for the past decade, and have shown some signs of turning up in recent years. Large companies with the best programs have not found that "more of the same" will renew progress. The situation has been the cause of widespread concern in business and government.

A full industrial application of systems techniques would be costly and impractical at present, that is, we cannot redesign and rebuild the plant. But a considerable number of essentially new concepts and procedures are available today for use individually or collectively to build a fuller system of control over work hazards, and thereby upgrade conventional industrial programs. And, new products, new machines, new materials provide a steady flow of opportunities for innovation and improvement.

The emphasis in this monograph will be on occupational safety applications, but applications of system safety to product, public, and transportation accidents are also desirable and practical.

In Sections II and III of this monograph we have, with the kind permission of the National Safety Council, reproduced two recent publications of the Council:

1. Systems Safety Analysis, J.L. Recht, now Manager, Statistics and Library Department, NSC, June, 1966.
2. System Safety and Industrial Management, Robert Currie, Assistant to the General Manager, NSC, July, 1966.

These two documents are used as basic material in a one-week course in System Safety Analysis now offered by the Council several times a year.

The ideas discussed in the two system papers are treated as integral with this material. Consequently, their separation as Sections is awkward. However,

one larger assumption may be even more burdensome, namely, we have assumed that the content of an excellent basic manual, such as NSC's Accident Prevention Manual for Industrial Operations, constitutes a usable distillation of the wisdom and experience of the industrial safety movement in the U.S. And there is nothing to be gained by attempting a restatement in new words of ideas which have been so thoroughly reviewed by a host of experienced experts.

New approaches to safety in industry are assumed to be grafted onto and melded with the basic, time-tested approaches which have proven so effective in the industrial development of this country.

There are signs and warnings that the past safety methods may not be fully adequate to cope with present and future challenges. Also, there is the hope that new methods may give us improved insight into the safety process.

Some concepts more or less new to safety can be borrowed from other fields of control of work, such as quality and error control. Some have not been fully tested as safety concepts, and require an experimental orientation in a safety application.

The new approaches hold great promise for renewing the safety progress recorded prior to this decade. They are more soundly based in management incentives and the management process, as well as technically superior. They are likely to deal more realistically with the exasperating human variable. Most important, they may give us insight into the safety process which will permit all of us to more rapidly evaluate our own experiences and those of others.

If we say that safety is just one specialized aspect of reliable control of work we have taken a giant step toward a useful orientation toward management's objectives. And when we incorporate the concept that accidents are one member of the broad family of errors and malfunctions, we take two additional steps - first, we continue to show awareness of management's problem of control, and second, we open the literature on error and error control for safety adaptation. Errors are, in some respects, easier to study than accidents and there are more of them to study and develop control ideas.

A brief enumeration of some of the facets of the concept we call "safety" (and shall be developing in more detail) may be helpful:

A. Safety is mission oriented.
   In business this orientation puts long-term profitability first. The constraints of time, budget, and work performance are the "practical" side. We seek to make the place run more efficiently!

B. Hazard identification is No. 1

The rapid pace of technological change and the information explosion require that we develop an efficient information network, and use the kinds of analytic techniques which can help guard against oversight.

C. Risk evaluation and control employ concepts of:

1. The full life cycle of the process, operation, or product.
2. Relate errors to accidents, and consider anything which degrades or upgrades the process (quality, waste, reliability).
3. What can happen, will happen - given sufficient time.
4. First things first - catastrophe and major hazard analysis are primary.
5. Amount and quality of analysis and planning equated to the hazard and carried to the point where additional steps have been evaluated but cannot be recommended due to time, cost or technical problems.
6. The solutions thus give management data for judgment of the residual risks to be accepted. In other words, where to "back off" in control.
7. Open-mindedness.
8. Engineering, where feasible, is the preferred method of control.
9. A concern for people suggests human factors engineering study, and adequate procedures, training and supervision to minimise the stresses inherent in man-machine-environment systems.
10. The concern for people also dictates improved communications to build acceptance of innovations.

D. The accident is conceived as a complex series of events, energy transfer modes and barriers, and involves error (unsafe acts and unsafe conditions) and change.

E. Accident investigation is multi-factorial and seeks to trace all sequences and factors to their organizational roots.

F. Measurement of performance goes beyond accident rates and attempts to quantify various aspects of the safety program and the actual operations.

Even though the mark of the systems approach is thorough and complete coverage of hazards and potentials, the concepts are separable and usable individually. Don't reject them just because you can't use all. Begin where you are, and build.

In the National Safety Council's one-week "Fundamentals" course, it

was long customary to use interest cards. Some common questions voiced by the students were:

How can I sell management on safety?
How can I maintain interest of supervisors? of employees?
Are safety committees a good idea?
Are posters any good?
Are contests worthwhile?
How to inspect for safety?
Are USA-ASA rates meaningful?

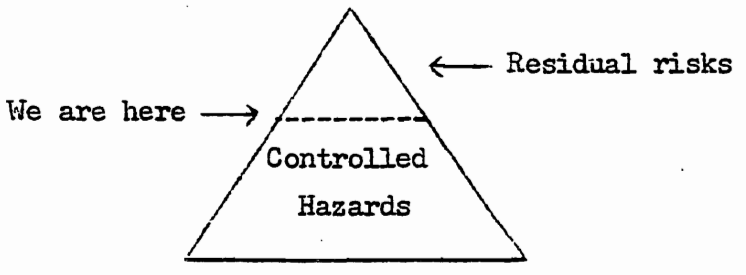
We shall suggest that these may not be the right questions! The real questions may lie one step further back and be in a general form: "Where is your organization in the planning and execution of a program of reliable control of work?".

The program features (and even gimmicks and slogans which have been common in the U.S.) all may have their usefulness. But for the future they should be seen as only parts of a broad, well-based process of getting acceptance of safe and sound procedures. A more useful point of departure may be to ask, "How and why do people change their behaviour?" There are some scientific findings which can be useful. Then the program features can be designed as a comprehensive plan to attain an objective at <u>all levels</u> in the organization.

In general, as one examines the literature of industrial safety, one finds a wellnigh overwhelming mass of topical material, rather than <u>method</u> or <u>principle</u>. It would seem fair to urge an emphasis on <u>Method</u> versus <u>Content</u>, or perhaps more appropriately a use of <u>Method</u> to handle <u>Content</u>.

Our concern for improved methods stems not so much from any failure of the old methods as from a desire to attain even greater success. Many U.S. companies have attained a high degree of safety, but they seek ways of further improving.

A pictogram of a mountain has expressed the idea:



How can we reach the summit?

REVIEW OF OUTSTANDING U.S. INDUSTRIAL SAFETY PROGRAMS

Management Policy and Direction

There is broad agreement that vigorous top management leadership is an essential and conspicuous feature of the best corporate safety programs in the U.S.

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 either put safety first or ranked it side-by-side with the other principle corporate objectives.

The report* of a working party on U.S. safety practices (an excellent and concise reference) says:

> "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 of top management:

1. Welfare of the employee.
2. Costs of accidents and injuries.
3. Efficiency and effectiveness of the organization as a system.

Although all three of these motivational forces are commonly found, the statement of a particular organization is not likely to contain all three, 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, the outcome was publication of many examples, rather than a consensus.

If any given combination of the three 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 such top leadership in other organizations, we can profitably examine the nature and force of the three motivations.

---

* Safe and Sound, British Chemical Industry Safety Council of the Chemical Industries Association, Limited, 1969.

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, A T & T, Kodak, and General Motors, just to cite a few other prominent examples, have powerful concern for employee welfare.

The welfare motivation cannot be depreciated 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 trade association. But is the safety professional in a favourable position to change an attitude? Not so likely.

The <u>costs of accidents and injuries</u> 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, or major fires in general). Costs may be high if public and product liability is involved. In all such organizations, cost reduction may be used as powerful motivations.

However, in a typical low or medium hazard organization, 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.

One seemingly effective technique has been to equate accident losses to the amount of sales needed to recoup the losses.

The efficiency 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.

A Canadian wood products company says, "Safety and efficient operation are one and the same thing. They cannot be separated."

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 duPoint plant 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.
>
> 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.

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 draws, in part, on British experience, may be particularly helpful*. After describing pre-World War II emphasis on physical safeguarding and post-War emphasis on training, he says:

> While American industry consistently improved its work injury rates, safety specialists studied and discussed the reasons. One expert, a member of a British study group published his observations in the magazine of the British Iron and Steel Federation:**

---

* Grimaldi, John V., "Management and Industrial Achievement," Journal of ASSE, November, 1965.

** Barry, R., "The Real Difference", Safety, No. 14 (Autumn 1961), a publication of the British Iron and Steel Institute.

"If guards in themselves prevented accidents, we would be in a position to show the Americans a thing or two. One forms the impression, rightly or wrongly, that they are lagging far behind us in this field. If organized training in itself led to good safety records, we could act as their advisers. And whilst they can show us a few tricks in the protective clothing and equipment trade which we haven't yet picked up, they cannot tell us a great deal about the quantities in which it should be issued. In a good many cases, we are way ahead of them in this respect.

"How, then, do you answer the British safety officers' questions: 'What have the Americans got which would explain their superior safety records?'

"...the answer is...that the Americans have the right attitude of mind to create good safety records."

This singular attitude merits some philosophical inquiry since it is basic to safety achievement. The question is, does training impart such wisdom? When it is recalled that the British expert reported his colleagues "could act as...advisers" to the Americans' training programs, doubt is cast on the likelihood that training in itself is responsible for any notable differences between the observed work injury rates.

However, there may be one distinguishing feature in American safety programs. They usually are intensive. The inescapable conclusion, therefore, is that it is the intensity of the United States' training activity which generates the noted stronger safety motivation and the inducement probably is the easily recognizable implication that management wants its work done safely.

If one were to examine closely the safety motives of American workers, it is possible that in addition to a personal wish to avoid injury, there also is a distinct desire to work safely because the employer expects them to. This stimulation is subtle in many instances.

Employer safety activity in America largely is voluntary. Although the states and the federal government regulate certain hazardous exposures, the implementation of safety requirements generally is left to the employer. He initiates and directs the activity according to his needs and judgment largely without governmental persuasion.

Therefore, while the programs teach safety principles they demonstrate management's voluntary interest in accident prevention. The effect doubtless is inestimable. The employer's action in inaugurating a safety function and staffing it, usually with qualified junior-type executives who have been delegated the responsibility for safety, clearly suggests that he wants an effective safety performance - and it is a very dull employee indeed who does not respond accordingly.

Later Grimaldi has these observations:

Safety specialists intuitively recognize the motivational effect of management's interest in safety and repeatedly assert that it is the basis upon which safety achievement is founded. In their efforts they urge management to give more tangible expression to its desire for accident prevention. However, it is not often realized that at the employee level, the mere fact that a safety activity is in place is a clear expression of managerial interest (except for instances where the activity is obviously deemphasized by organizational and economic impositions).

> Therefore additional expressions of managerial interest, alone are not likely to have a significant, if any, further influence. Amplification of the desired managerial effect is more certain when managers apply the same vigorous, and positive administrative persuasiveness that underlies success in any business function.
>
> 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.

Somehow we safety professionals are still weak in the language and conceptional 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 managerial failure to establish reliable control of work, as an error resulting from poor management or managerial omission, 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* 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. And when we examine the role of "change" in accidents we'll also see some interesting relations to efficient production.

Other motivational forces which appear to have been potent with U.S. 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 in the U.S. have been seen primarily for their values in reaching smaller employers, but their effects on leaders from larger organizations has probably also been great.

Further, it is common for management to take an active part in community

---

* Pope, W.D. and Nicolai, E.R., Safety Aids Decision-Making, U.S. Dept. of Interior, Personnel Management Publication No. 13, August, 1968.

safety affairs as civic leaders. And it appears that such participation has reinforced in-plant safety by supplying a strong, comprehensive philosophy.

A factor in U.S. safety not widely discussed is management's concern for its 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 is said to be the topic on which it is easiest to "get along on", not that safety grievances and union issues may not at times also be sore points. But, particularly as on-the-job programs have been extended to off-the-job concerns, safety has been the basis for a real bond of mutual concern of manager and employee.

We commonly say that safety "begins" with top management. But it may well be that the concepts and practices of leading U.S. businessmen are the end of several decades of evolvement and mutual influence, rather than the beginning. And if we wish to take a 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.

Line Organization 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 corporate 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.

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 three types:

1. General programs in management and supervision,
2. Human relations and communications,
3. Safety.

Most of the larger companies have their own 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 labour departments make available a wide variety of courses. Recently, community safety councils have intensified their supervisor training offerings. However, from comments, it appears easier to make training conveniently available in England than in broader reaches of U.S. geography. Considering the critical importance of the training needs of smaller establishments, there is no substitute for a comprehensive network of training opportunities.

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, chaired by senior executives, with revolving representation from first level supervision.

These three kinds of arrangements, with top leadership, can create a team approach.

Safeguarding the Work Place

In U.S. programs it has been generally agreed that physical safeguarding and control over environment, facilities and equipment are primary for two reasons:

1. Engineering is the preferred solution because it is easier to define standards and maintain continuing observation and permanent control.
2. A safe work place is evidence to employees of management's sincere interest in safety.

U.S. Steel's plans for attaining physical safety are typical of the best. 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 and 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 have adopted all applicable public standards and have gone so far as to promulgate NSC's comprehensive Manual as its internal guide (although it is not written in standards fashion).

Provision is customarily established for safety engineering review of all plans.

Inspection programs are carefully scheduled as appropriate - some daily by operator or supervisor, others weekly or at some other suitable periodic intervals and by management and by technical specialists as required. Checklists are desirable.

Tool maintenance must be covered by planned arrangements, either departmental or plant wide.

The role of standards is a cause of concern in the U.S. The pace of development has been too slow under the voluntary system, and there are strong governmental pressures for improvement. At the same time, the leading corporations, whose personnel perforce do most of the work on 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 the states, because their internal standards are higher.

More recently the long-term role of standards has been called into question from another source - systems safety analysis. As will be seen, the goal here 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.

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 regulation, at least not by the conventional regulatory methods. Some new and potentially better regulatory methods have been discussed, 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 applied 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.

Directing the Employee

Directing the employee and motivating him are not without inter-relations. For example, the participation of leading craftsmen in the development of a job safety analysis will not only contribute to the analysis but also help build acceptance. But for analysis and planning it seems wise to separate the two aspects - direction and motivation.

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 the first time, but have a planned observation program to continuously monitor performance.

For convenience we shall 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 of 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? Or, where did the system fail?
   b. By inspections - if an unsafe practice is observed, was it covered? Or where did the system fail?
   c. By supervisory reports indicating degree of coverage.

"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."*

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 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.

---

* Accident Prevention Manual for Industrial Operations, National Safety Council, 1964, which contains substantial sections elaborating techniques for JSA-JIT-SO.

Obviously JSA may reveal needs for guarding, displays or signals, better equipment or physical arrangements. And it is understood the physical revisions are preferred. Or, the task may be eliminated by improved controls or equipment.

JSA offers valuable opportunities for using the safety motivation to support non-safety, efficiency controls and procedures. For example, the NSC Manual uses the job of planting a tree as one example for analysis. It seems clear that two results could stem from JSA - first, no injury; and second, the tree might be more likely to grow!

The four basic steps in Job Instruction Training are:

1. Prepare the worker to receive the instruction.
2. Present the operation - perform and describe.
3. Try out his performance.
4. Follow-up.

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.

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's happening.
2. The special follow-up to observe new employees, or new or changed tasks.
3. A required number of <u>recorded</u> 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 break-downs and the measurement of performance.

Now, 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 has developed some experience and standards as to spans of

control and 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 totally new employees.

We come finally to the matter of rule observance 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 back-ground of clear rules, clear understanding, and a limited tolerance for variations.

Motivating the Employee

It is in the area of motivation of employees that we encounter great difficulty in briefly summarizing the best U.S. practice. We encounter a well-nigh overwhelming mass of specific program features, each with a substantial group of proponents. Recipes for developing enthusiasm, maintaining interest, etc., are as numerous as the corporate entities themselves.

Two conclusions seem tenable:

1. Each corporation with a successful program has put together a related series of activities which have had pragmatic success.
2. Little or no basis exists for testing the significance and value of a specific activity separated from the context in which it was utilized.

These two conclusions, in turn, lead to two observations:

1. The corporations are intensely practical and pragmatic, but also include a complement of the scientific - medical, social and psychological specialists. Decisions to introduce specific programs are made in a specific context of prior programs, and are not scientific decisions, but neither are they without scientific background. Often they have been tested in one plant or one division.
2. There is a considerable void between the practitioners of industry and the scientists - in safety. Even some companies whose corporate

success is founded in research have not seen a need for safety research, nor even that safety is researchable!.

Therefore, we seem to have a choice of several courses:

1. Adopt the entire complexity of some good corporate program - which would ignore the considerations which made the program justifiable to that corporation's management. And no two companies are the same.
2. Or, we could pick and choose programs until we had a jig-saw puzzle solution which "looked good".
3. We could try to develop a method of program analysis which would be more systematic and analytic, and would provide some rationale for program synthesis and evaluation.

The last alternative seems preferable. But before we are ready we shall want to examine some concepts of system analysis, innovation, change and error, so that whatever motivational complex we select will reflect what we know about accident mechanisms and controls.

Program Audits

Audits of all aspects 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 programs. One company reports two to four man-weeks as a normal requirement for a biennial audit. Most audits use corporate headquarters personnel, but some also use operating personnel from similar plants. Naturally, either type of personnel would bring to an audit a thorough knowledge of corporate practices and expectations.

Unfortunately it is difficult to see how a one-plant company could provide itself with an equivalent audit.

Role of the Safety Professional

The NSC Industrial Manual says that the duties and responsibilities of the safety director ordinarily include:

"1. Formulating, administering, and making necessary changes in the accident prevention program.
2. Submitting, directly to the officer in charge, regular monthly, weekly, or daily reports on the status of safety.
3. Acting in an advisory capacity on all matters pertaining to safety as required for the guidance of management, the general manager, superintendents, foremen, and such departments as purchasing, engineering and personnel.

4. Maintaining the accident record system, making necessary reports, personal investigation of fatal or serious accidents, investigating accidents through his staff, securing supervisors' accident reports, and checking corrective action taken by supervisors to eliminate accident causes.

5. Supervising or closely cooperating with the training supervisor in the safety training of employees.

6. Correlating safety work with the work of the medical department to ensure proper selection and placement of employees.

7. Making personal inspections and supervising inspections by his staff and by special employee committees, for the purpose of discovering and correcting unsafe conditions or unsafe work practices before they cause accidents.

8. Maintaining outside professional contacts to exchange information with others and to keep the program up-to-date.

9. Making certain that federal, state or local laws, ordinances, or orders bearing on industrial safety are complied with.

10. Securing necessary help or advice from state labour departments or insurance carriers on matters pertaining to safety and health.

11. Starting activities that will stimulate and maintain employee interest.

12. Directing the activities of his staff so that the accident prevention program will be efficiently operated. It is expected that the safety director may delegate certain responsibilities to his staff engineers, such as acting as secretary for certain safety committees.

13. Controlling or supervising fire prevention and fire fighting activities where they are not responsibilities of other departments.

14. Setting standards for safety equipment to be used by plant personnel.

15. Approving designs of new equipment to be used in plant work areas.

16. Recommending provisions for safety in plans and specifications of new building construction and repair or remodelling of existing structures."

A more functional enumeration of safety tasks to be performed will be found in Section III (Currie), pages 39-42.

Grimaldi, cited earlier, continues his observations on the role of management, and establishes some directions for development of the safety professional:

> "I suggest, therefore, that safety achievement cannot rely on such conventional approaches as employee training and plant inspections. The accident problem appears too complicated for such simple methods to solve. It is also too extensive to be dealt with casually.
>
> The basis for effective control it seems is firmly fixed in the management decision making process. The method essentially is a disciplined approach to risk evaluation and control. Its application is basically the same whether the concern at the moment is to eliminate employee injuries, safeguard the plant from destruction or make a profitable decision in the market place. I believe the steps to take are:

Investigate the operation, process, project or system aggressively to identify each inherent risk to individuals and the enterprise.

Evaluate each risk to determine those with no purpose or merit.

Eliminate the purposeless risks.

Ascertain that the tolerable risks are controlled to prevent accidents or severe consequences if an accident should occur.

Correct any uncontrolled hazards.

Follow-up periodically to assure that the controls are maintained and no new intolerable risks are introduced.

In these considerations it may be evident that the role of the safety specialist will change in character. The customary inspection, safety promotion and training activities will be more or less subordinate to his loss prevention counselling of the plant's managers.

The degree to which the conventional approaches engage the specialist doubtless will be a function of his ability to analyze and marshall facts, his experience and the opportunity given him to provide such a contribution. His value to the safety effort will depend significantly on his ability to:

Develop loss control information which enables managers to make sound decisions, rather than endeavouring personally to convince employees to have a greater safety awareness.

Persuade management action rather than attempting to correct hazardous situations on his own.

Teach the methods for solving safety problems, rather than providing the answers."

Because the duties of a safety director are so manifold and diverse, and because his is a position of considerable force and indirect authority in a well-run company, the indirect nature of the authority must be made clear. General Motors has as one of its seven principles: "Operate through supervision".

The British Chemical Industry working party made a correct and concise statement:

"All the large companies have corporate safety departments. In four of these they report to the member of the board responsible for industrial relations or personnel, in the fifth to the chief engineer. In every organization the top safety man has ready access to the most senior level of management in the company. Downwards, there is an outflow of advisory and consultative services, coupled with an auditing service. The central safety department also operates a clearing-house for the reception, classification and dissemination of information. The communications system, on which the success or failure of a department operating in this way depends, is very good.

At plant level, the larger plants have a safety manager or director, one or more safety engineers, a fire chief and staff assistants. The smaller plants may have a safety engineer only. Whatever the set-up,

> functionally there is no difference. The safety staff advise, guide and counsel local management, help prepare safety codes and practices and supervise the fire protection service. They feed information and co-ordinate activities. They do not play any part in the day-to-day operation of safety programmes, although they will help in their preparation. They do not perform the bread-and-butter work of accident prevention by making out requests for maintenance work to be done to remedy unsafe physical conditions, by arranging for obstructions to be moved from gangways, and oil patches to be cleaned from floors. The only exception to this is where a 'safety inspector' is also employed - a lower-level member of the safety department staff involved in the issue of permits to work and supervision of work where the hazards are high. Safety staff are involved in accident investigation, but not solely responsible for it. One plant manager expressed it in this way, 'I look at our safety supervision as our consultants, our experts, our missionaries, our follow-uppers, our conscience, and many other things. And they are very necessary. But they alone can't get safety. Plant safety is not their prime responsibility. The prime responsibility belongs with the line - the people who supervise others.' Besides placing the responsibility firmly on management, this philosophy prevents any over-lapping of accountability on the part of employees."

Titles may or may not be important. The terms "Safety Director" and "Manager, Safety Department" are common. Both carry connotations of authority. But when managements in the better companies refer to roles, they commonly use "our safety advisor" or "our safety consultant". Perhaps such terms, which consistently clarify the role, would be preferable.

Similarly, we hear safety directors refer to "my safety programme". Is this wise? Or even correct?

Considerable emphasis, and some success, in the U.S. and Canada on professionalization of safety has stemmed from the work of the American Society of Safety Engineers. Further progress would seem to hinge as much on improving safety concepts as on an upgrading of personnel.

SYSTEM SAFETY ANALYSIS

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

Bell Telephone Laboratories developed and Boeing 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 probabilities, and second, do this for the "life cycle" of the operation.

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 procedures involved, but also brought about a reorganisation and strengthening of the space agency's safety organization for manned space flight programmes.

The manned space flight program involves an essentially new idea: First Time Safe. The mission is simply not one 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.

The U.S. Atomic Energy Commission has employed systematic analysis of the "maximum credible catastrophe" to assay the design of atomic reactors. 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.

Systems safety analysis has not only improved our technological capacities, but has also begun to raise public expectations as to what is possible in product, transportation, and occupational safety. Therefore, the corporate future holds both the threat and the promise that system safety procedures must be applied.

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 available for the analysis are both inadequate.

In order to provide adequate material for initial study we have incorporated two pre-existing documents.

Recht, in Section II, gives a brief background of systems safety, some basic definitions and examples, and then provides an elementary discussion of three specific techniques: (1) Failure Mode and Effect. (2) The Fault Tree, and (3) THERP (the human error rate prediction).

Currie, in Section III, borrows text material from Charles C. Miller, Institute of Aerospace Safety and Management, University of Southern California. Currie presents discussion on the following topics:

1. Definitions.
2. History.
3. The "Known Precedent" concept, which has legal as well as safety implications.
4. Safety management.
5. Dealing with the "information explosion".
6. Life cycle, that is, the scope of safety covers all phases: concept, definition, design, production, operation (including training and maintenance) and ultimate disposal.
7. System effectiveness, and the relation of safety to reliability, quality, operability, maintainability, etc.
8. Failure analysis.
9. Relation to law.
10. Safety tasks.
11. Communication of safety information.
12. Anatomy of system safety.
13. Innovation.
14. An extended list of references.

(It is suggested that these two basic presentations be read and studied. The ideas these two men have discussed are not repeated in the material which follows.)

At some point we can anticipate the question, "Is that idea really new, or is it just new jargon?" The answer, in many instances, will be, "No, it's not new. But the principle is made explicit rather than hidden in content or context." And the explicit principle or method helps us in subsequent analyses of different subject matter.

We can proceed in this discussion by borrowing liberally from a paper on System Safety (undated) produced by the U.S. National Aeronautics and Space Administration (NASA) to describe its own program.

> "System Safety means different things to different people; in fact, it has probably been defined a little differently by every individual who has ever made the attempt. It may be generally described, however, as 'The application of sound technical and management techniques and principles to the safety aspects of a system or program throughout its life-cycle with the objective of reducing hazards and risks to an acceptable level.' But semantics is an age old problem, and as a result, others words are frequently included in the definition such as 'optimum degree of safety,' 'within constraints of cost, time, and operational effectiveness,' or 'consistent with program goals, resources, and time constraints.' These words and others are all pertinent, but rather than quibble over such wording, let's concentrate on a list of System Safety basic objectives. These objectives may be stated as follows:
>
> 1. Identification of all potential hazards throughout the preliminary analysis, definition, design and development, and test and operations phases of program, through application of engineering and analysis techniques.
> 2. Positive action to eliminate, reduce, control, or compensate for the hazards as soon as they are identified.
> 3. Development of emergency procedures, techniques and systems to handle the residual risks.
> 4. Knowledge of those residual risks which must be accepted by line management after all other recourse has been exhausted.
>
> In manned Space Flight a safety program has been implemented which includes System Safety as a management system to integrate all those technical and management efforts designed to eliminate and control hazards and thus meet these objectives."

In a section on evolution of the program, we find this comment:

> "A method to accomplish early identification of hazards, take positive action for their elimination or control, and provide management <u>risk visibility for decision making</u> was needed."

The headings under Safety Program Elements are:

1. System Safety.
2. Safety Research.
3. Accident Investigation.

4. Information.
5. Motivation.
6. Training and Certification of Personnel.
7. Safety Appraisals.

Items 2 to 7 do not sound greatly different than a conventional program, with the exception of specific provision for the needed research. Most corporate programs are deficient in this respect. Pragmatic experience is usually used, and often works well enough. But as time goes on, and problems become more complex, we have few solid facts to guide us.

Later in the paper we find 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 already seen in outstanding U.S. programs? Yes, it is. The documentation of 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. Additionally, there is greater emphasis on the importance of detailed documentation.

The primary System Safety Requirements are defined as:

1. A system safety plan.
2. Hazard analyses.
3. Hazard reduction sequences.

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 reviews.

Hazard analysis, of course, covers the life cycle, and has three phases:

1. "Preliminary hazard analysis involved 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 in this analysis. This analysis should 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 their 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, and trajectory analyses must be used and extended wherever appropriate in the detailed hazard analyses."

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 of these analyses 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."

The hazard reduction precedence sequence is listed as:

1. Design for Minimum Hazard.
2. Safety Devices.
3. Warning Devices.
4. Special Procedures.
5. Residual Hazards.

The first step, design, is intended to cover physical safeguards. And the statement on residual hazards is especially good:

> "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."

One authority on systems safety has said that the four major aspects of systems safety are:

1. A set of specialised analytic techniques.
2. Concern for the full life-cycle of the product or activity, including data feedback and re-study, re-call, or re-design.
3. Open-mindedness concerning all practicable solutions or ameliorative factors - "Take off the Blinders!"
4. Assigned responsibility for safety to specialized personnel.

Another experienced system safety analyst listed some principle analytic techniques as:

Gross-Hazard Analysis

Classification of Hazards

Failure Modes and Effects (sometimes called "Hazard Modes and Effects")

Hazard Criticality Ranking

Fault Tree Analysis

Energy Transfer Analysis

Catastrophe Analysis

System-Subsystem Integration (Inter-Face Analysis)
Maintenance Hazard Analysis
Human Error Analysis
Transportation Hazard Analysis

We shall want to discuss some of these topics below. (The failure mode, fault tree and human error analyses were treated by Recht.)

Mission Orientation. It is clear in the military and space documents that system safety is "mission-oriented," that is, the goal must be accomplished. And the goal for a corporation is obviously long-term survival as a profitable organization. Thus, even though a corporation says that employee protection is the first and primary consideration, survival comes first. Survival does not mean sacrifice of safety - it does mean better management, better safety, and above all, a premium on knowledge, skill, energy and imagination. These are the crucial challenges to the safety professional.

Constraints. In the military documents, the constraints of time, money and mission performances are assumed to be defined by the government agency. These constraints pose real dilemmas for the private sector. In the military or other government programs, the constraints are defined by government and are therefore supplied externally to the contractor. In ordinary business, management must eventually, by act or by omission, place the time, budget, and production and marketing limits on the safety work. Lingerie which would give the housewife's morning coat the same degree of protection in the kitchen as would a survival suit in space wouldn't sell for a variety of reasons.

Particularly in product safety, there may be no more difficult decisions than, "How much safety analysis is enough?" and, "How much safety will sell?" Certainly "None" is the wrong answer to both questions. But, "How much is enough?" In product safety in the U.S., only the courts will give final answers to specific situations. We do know judicial yard sticks are going up fast.

Hazard Identification. This has been said to be "Number One". The task can be seen as having three elements:

1. Practical experience in the operation,
2. Information on "known precedents",
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

fellow who inspects and observes carefully. One writer 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 are:

(1) His analytic process is not monitorable.

(2) His analytic process usually cannot quantify the relative merits of alternatives.

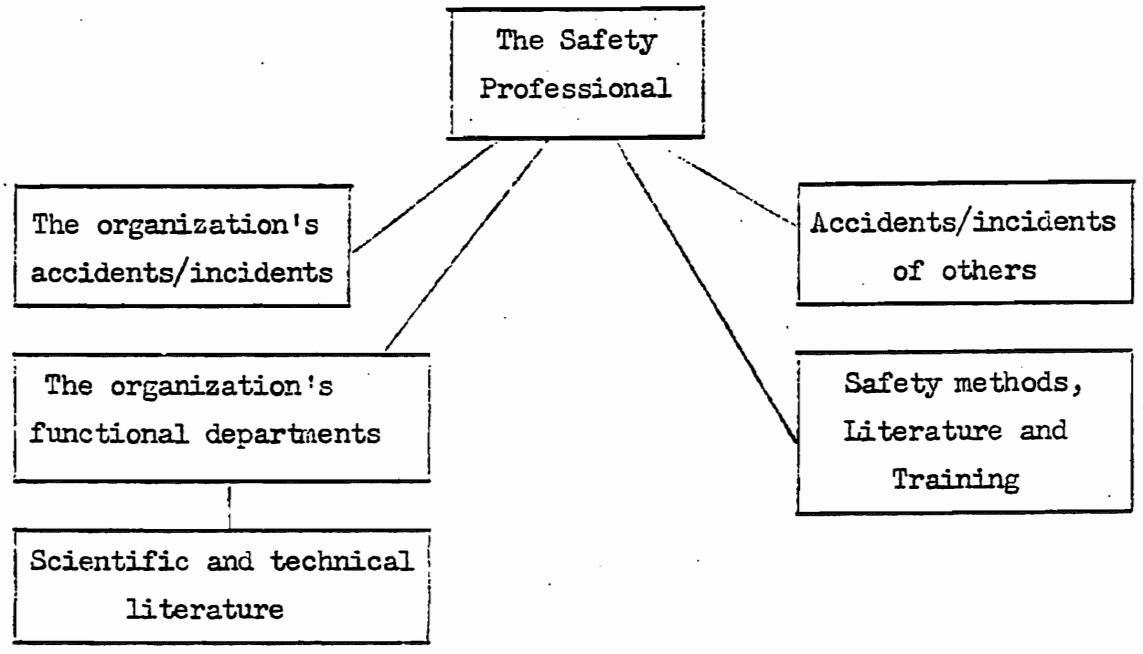
(3) His process breaks down in complex situations.

(4) Graphic analytic forms are unavailable, and therefore teaching and persuasion are weak.

(5) Thousands of combinations of potentials must be learned.

After an accident it's common to hear someone say, "Who would have thought that would happen?" The "Who" is the person who had the same accident earlier! Or better, the safety engineer. The safety engineer must have effective access to information, or his organization is condemned to make all the mistakes for itself.

Information scientists today talk about "information networks" capable of handling the information explosion. The safety professional must give thought to the nodes in the network upon which he will rely. A basic network would appear to have the following minimum essentials:



The pictogram suggests reliance on others for general information - the flow is too great to monitor for safety alone.

The diagram also suggests the need for rapid and effective communications through trade association or similar channels and through safety groups.

Each safety professional should develop a detailed and specific set of information arrangements.

The system safety analysis procedures, seen one way, are simply a methodical way to guard against oversight - including oversight stemming from habit, prejudices, or failure to measure and estimate.

Life Cycle. This concept has to be lived with 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 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.

First Things First. Now - this can't be a new idea! We saw that U.S. business said, "Tackle the major hazards first". But, how many times we see a great effort expended on a little problem! And how many times we see people "live with" a risk we "Can't do anything about". The systems approach suggests that management always have before it a list of residual risks, with the largest risk on top of the list. Action is more likely!

Equate Analysis to Hazard. We do not now have any easy or simple way to equate analysis (and action) to degree of hazard. We can put a floor under minimum analysis with a premise that every hazard identified and every change of importance should have at least a scrap of paper on which analysis and review (if there was any) is recorded. Beyond that only the constraint of time and practical experience guide us.

Does Hunch = Heur
don't think so
but analysis = Algorith
Algorithm, Heuristic
& Hunch

If we want posters for safety engineers we can try these two:

When Analysis Stops All Else is Hunch

No Analysis = all Hunch

Trace Causes to Roots. The systems methods help us trace causes to roots. We must ask why a condition came into existence and why it was permitted to exist, find out on what basis a manager at some level decided to accept a risk, and cumulate a factual basis on the need for broader programs (such as a supervisor training program). Theoretically, every accident is traceable to an act or omission of management, and it should be so traced, or pin-pointed at another point of breakdown.

Openmindedness. We are constantly trapped by the old ways of doing things. Yet, the history of man-in-space show that "insurmountable" hazards can consistently be reduced or eliminated by a combination of innovation and research - and money!

For example, take some ordinary ladder accidents. List the causes. Ask, "What happens if --?" Then describe the concepts of instrumentation necessary to control ladder hazards. We'd probably start with "Tilt" lights and bells to control placement. We could install a gate which won't open until the tilt light is off. We can ring a bell when a man reaches out too far.

Or, since displays and signals require training, engineer a non-tippable ladder, or install a fixed ladder.

Someone will say, "The ladder weighs too much, and is too expensive". Heavy? Pick it up with a lift truck. Costly? Start a list of tasks on which ladders are used, and then list ways to eliminate or reduce the tasks. Fun?

Inter-face Analysis. The formal term for this aspect of analysis is "system-sub-system" integration. This is systems jargon, but good jargon. It asks what happens when two parts of the system inter-act. Has any problem or hazard "dropped between the chairs?" An example would be an insulated wire too close to a heater when the product is assembled. Or, controls too far apart

for the smaller operators. The history of systems safety is heavy with evidence that problems cluster at interfaces and, therefore, that integration analysis is highly productive.

It is illuminating to examine some accident case histories or reports to see at what interface the theoretical controls broke down.

Independent Safety 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.

This is hardly news in occupational safety, but it was re-discovered in military development, is still news in product safety, and to a degree in transportation safety, e.g., the railroads.

Risk Reduction Techniques. There is nothing new about the idea of designing things so people can use them, but the full-scale application of human factors engineering is still too rare, particularly in occupational and product safety. There is nothing new about the idea that, when things go wrong, we can be protected by redundancy, fail-safe devices, and monitors which signal, but again full-scale application of such principles is far from complete.

Residual Risk. This concept has three important aspects:

1. The residual risk is a management decision.
2. The number and type of residual risks is known and ever present.
3. The risk acceptance was a decision based on analysis and quantification to the degree practical.

The notion of "calculated risk" is old, at least in the U.S. military establishment. The next time you hear the statement, "It was a calculated risk", after an accident, just ask to see the calculations!

All human activity is fraught with risk. There is no such thing as absolute safety. But we are all entitled to know what risks have been left in an activity, by whom, and why.

Concept of an Ideal System. To hypothesize a system of full control of hazards has two advantages:

1. It may turn up some things we can do tomorrow, and haven't been doing.
2. It gives us a goal against which to measure our present status, effectiveness, and performance, and in so doing it helps determine what to measure.

Attaining Major Goals. In a complex industrial 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 have come to be called PERT (Program Evaluation and Review Technique). PERT Charts are a tremendous aid in planning and in measuring progress. Most safety professionals who have used PERT charts swear by them.

PERT charts are particularly useful on one-time projects, or change-overs, or other new goals - for example, a forty-hour safety training course for all supervisors. What steps are needed? What comes first? Second? Etc.

Milestones, points at which progress is assessed, are sometimes 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.

Goals. 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 a one percent reduction in accidents next year, we can make a plan. If the goal is a 75 percent reduction in 5 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.

PROGRAMS
have
GOALS
which will attain
OBJECTIVES
which contribute to
THE MISSION

Shorter Range

Longer Range

ACCIDENT CONCEPTS

One common definition of an accident is an "unplanned event which results in personal injury or property damage". But an accident is much more complex than "an event".

We are concerned here, not so much with trying to establish a single, precise definition of an accident, as to examine the anatomy of accidents to see where a variety of concepts suggest different kinds of intervention and prevention, or amelioration of results.

Schulzinger has offered two descriptions of accidents:

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."

One of the most useful attempts to show the multi-factor background of an accident was the "Dynamics of Home Accidents" developed by NSC's Home Safety Conference in the mid-50's. (See Figure) Unfortunately, no parallel occupational diagram has been developed.

From this concept, a national conference concerned with home accidents developed the following definition:

> "An accident sequence is a chain of events, or a series of interactions between a person and the environment or agent, including the measurable or recognizable consequences. The consequence may be, for example, a slip or fall which does not result in any injury, or it may include unintended injury, death, medical expense, or property damage".

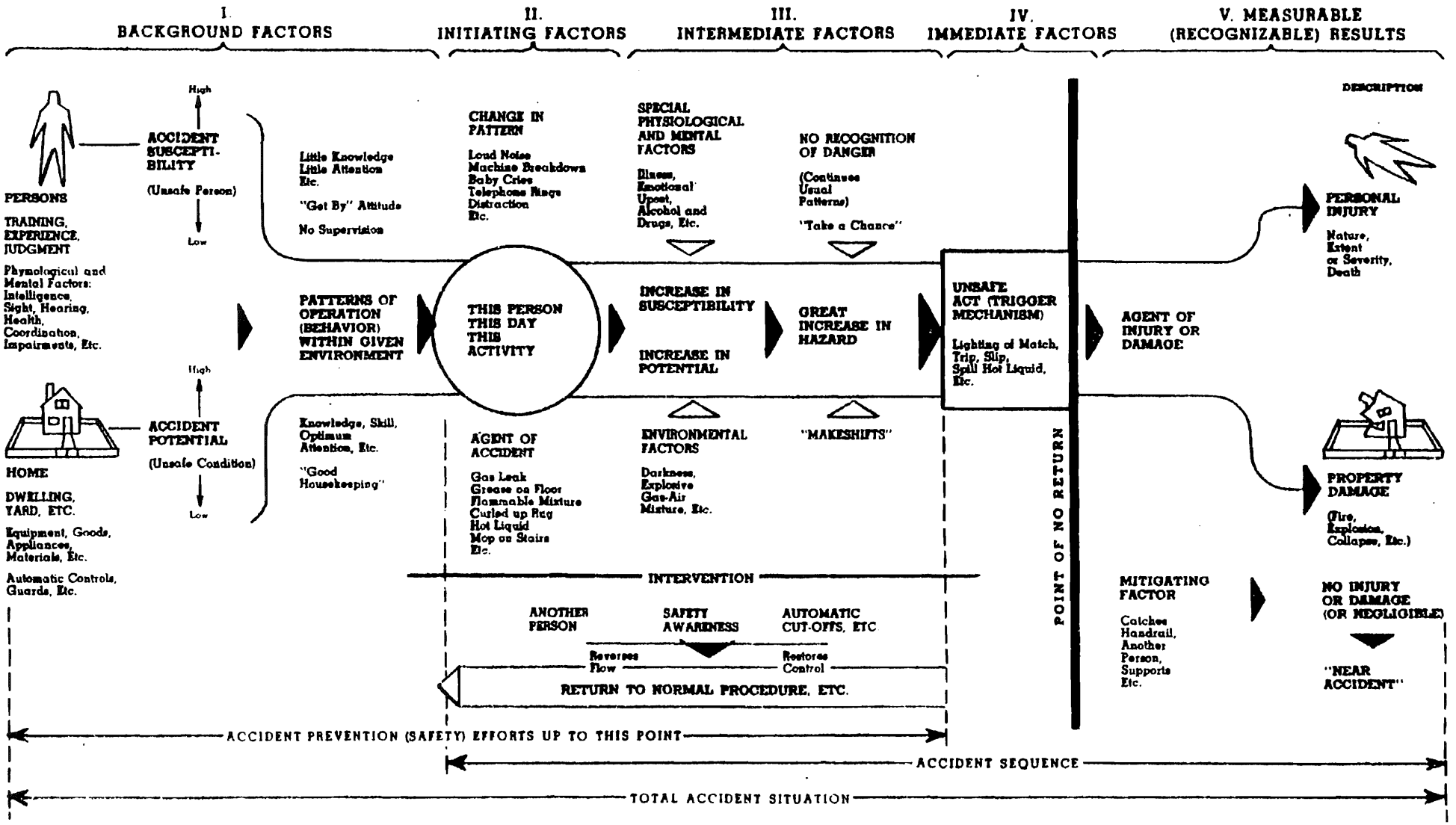
The purpose of exploring these concepts is to:

1. Establish the multi-factorial nature of accidents.
2. Suggest that there are usually a number of points at which the sequence could have been interrupted (the accident prevented).

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

Work environment (including arrangement and signals)
Machine (including tools, and equipment and signals)

The Dynamics of Home Accidents



Material
Task procedure
Worker
Fellow worker (or other third party)
Supervision

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".

There are clear implications then for both accident investigation and prevention. The overly simplistic attribution of accidents to "human error" probably does safety more harm than good.

Energy transfer

Another useful set of concepts was developed by Gibson and Haddon. They began with the point that an accident is an abnormal or unexpected release of energy. This led to a classification of sources of energy:

1. Kinetic
2. Chemical
3. Thermal
4. Electrical
5. Radiation
6. Exclusion of oxygen
7. Exposure to elements.

More recently, the U.S. National Commission on Product Safety augmented the list it is using in its studies by adding:

8. Acoustic.
9. Biologic
10. Distinguishing types of radiation.

This concept seems to have several values:

1. Simplicity,
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. Provides a point of similarity to systems analysis of energy transfers,
5. Sensitizes us to energy build-ups,
6. Reminds us to consider a product or situation for all kinds of energy.

A little thought suggests that those accident studies which have involved just one of these energy types, or one product or operation, have usually produced more useful data than studies of all accidents.

Haddon added the concept that harmful effects of energy transfer could be handled by a succession of steps:

1. Prevent the build up
2. Prevent the release
3. Provide for slow release
4. Channel the release away - that is, separate in time or space.
5. Put a barrier between the energy source and men
6. Put a barrier on the man
7. Raise the injury threshold
8. Treat
9. Rehabilitate

He suggests that the earlier the preventive steps can interrupt the sequence, the better. And suggests that the greater the potential damage, the earlier should be the interruption, and multi-interruptions should be provided.

The value in this 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 kinds of steps.

The concept that a given situation (for example, a job analysis) provides a "margin of safety" is useful in combination with the concept of "margin of error". If the margin of safety is small and the margin of error large, we'll have numerous accidents, and vice-versa.

Error

Altman and Chapannis characterize accidents as errors.* The usefulness of this concept consists, not only in its value as explaining accident causation, but also in the fact that errors, in some respects, are easier to study, and there is a body of literature which may be helpful.

Peters** defines human error in the following terms:

"In theory, we would want to use a broadly oriented definition which

---

* Unpublished papers prepared for forthcoming NSC Symposium on Measurement of Performance.

** Peters, George A. "Human Error: Analysis and Control", Journal of ASSE, January, 1966.

> states that a human error consists of 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.
>
> In practice, the term may have any one of several specific meanings depending upon the nature of contractual agreements, the unique requirements of a particular program, the customary error classification procedures, and the emotional connotations involved with the use of a term which might be incorrectly perceived as possibly placing the blame on individuals or their immediate supervision.
>
> In the reality of situations where arguments of precisely what is or is not a human error are of less importance than what can be done to prevent them, the operational definition may be restricted to those errors (a) which occur within a particular set of activities, (b) which are of some significance or criticality to the primary operation under consideration, (c) involve a human action of commission or omission, and (d) about which there is some feasible course of action which can be taken to correct or prevent their reoccurrence".

Peters describes some error investigation and reduction techniques, useful in preserving mass market images, preserving a complex process system, or operational reliability of complex equipment, or in product liability litigation.

In more routine industrial situations, quantitative data are not likely to be obtainable, but qualitative use can be made of the logic and practice of error reduction, even while further research is going forward.

Some examples of points made by Altman may be illustrative:

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.

Chapanis begins one of his papers with the following case history:

> "In March 1962 a shocked nation read that six infants had died in the maternity ward of the Binghampton, New York, General Hospital 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 is to tell the nurse to read the labels more carefully. Yet the solutions we see even today on many occupational accident reports are equally unacceptable.

Further, Chapannis 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' 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, 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."

We can here only sample the kinds of insights and wisdoms which error analysis may bring. Recht's section, we remind you, contains material on error rate prediction and categories of errors.

Change

For any system of operation which has been going on satisfactorily (i.e. up to some standard), Change is the cause of a Problem, and when you find The Change distinctive to the situation, you find Cause.

This provocative thesis, which has considerable potential for safety, was developed in the course of some studies for the U.S. Air Force. The concepts were made explicit in a text book* and a one-week training course which has been widely used in U.S. business for quality control and other control of work.

The thesis has several implications:

a. A new and better method of problem analysis, particularly where cause is obscure, or where we want to dig out underlying causes.

b. Sensitivity to change (and the possible need for an offsetting counter-change) is a mark of supervisor excellence. Training to build sensitivity to change is possible.

c. Categories of work fraught with changes will be high hazard (e.g. construction and maintenance, or transfers to new jobs).

d. Feedback on actual conditions and operations is essential to detect change.

e. In systems theory, review and counter-change theoretically follow every change.

f. 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 counter-changes.

---

* Kepner and Tregoe, The Rational Manager, McGraw Hill, 1965.

Interestingly, a large proportion of the examples used in the training course cited above were accidents.

> A car manufacturer in the U.S. had serious quality control problems on an assembly line. This new cause analysis method (KTA) traced cause to weekly transfers of employees on seniority 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.
>
> An application of this method (KTA) to the grizzly bear accidents fatal to two girls in Glacier Park in 1967 also showed that the method had great capability to sort out pertinent information from irrelevant facts, and provided insight into preventive steps.

An analysis of routine accident reports from a number of corporations yielded two types of results:

1. Most reports were grossly deficient in identifying changes - they 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!

Regarding the role of change, Altman 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".

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

1. We can be sensitive to the nature of "change work" - maintenance and construction, R & D, etc.
2. We can be sensitive to change situations - transfers, new machines, new materials, new operations, shut-down, start up, etc.
3. We can strive to augment feedback to detect change.
4. We can explore training methods to sensitize supervisors to detect and react to change.
5. We have some new ideas as to what to seek in accident investigation.
6. If a major problem has obscure cause, we have available to us a sophisticated method (KTA) to search for the change which is cause.

One experiment in supervisor training for sensitivity to change is reflected in the three forms which follow. (The blank form will be used in a class exercise).

Some Awesome Changes. Current literature increasingly refers to the directional and exponential nature of change in modern society.

Directional means that change 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.

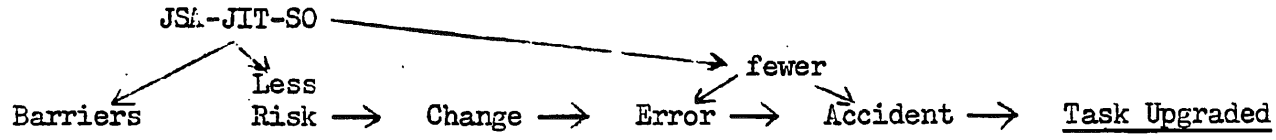
Exponential means that changes interact to compound the effects or exposure. Larger railroad cars or trucks are filled with more exotic material and go faster on roads with more traffic. New materials and equipment must be operated with less skilled and less motivated personnel. Thus, exposure to accidents tends to move as E^2, E^4, E^8, or E^{16}. The implications for the kind of control which will be needed are clear.

A Unified Concept?

If we begin to link together these concepts of energy, error and change, we see a sequence:

Energy → Risk → Change → Error → Accidents → Task Degraded

But if we inject



Remembering our early concern for selling management, this concept seems to have great appeal.

MOTIVATION AND BEHAVIOUR CHANGE

In reviewing outstanding U.S. programs, we ducked discussion of motivational programs until we had developed certain concepts. We now have some inkling of what systems safety has to offer, and we've explored concepts of error and change. We had already seen what JSA-JIT-SO had to offer in designing and stimulating wanted changes in behaviour and controlling unwanted changes.

Systems safety concepts run the risk of seeming to "de-humanize" the real people involved. Actually, they should have exactly the reverse effect. If systems safety has given proper attention to human capabilities, and sound procedures, we can fairly deal with the people involved. If human factors have not been carefully studied, we may be grossly unfair in demanding performance to a high standard. Failure to use known human factors techniques would be unethical, and could undermine a serious effort to train and motivate.

There are some further aspects of the human in the safety equation which need brief discussion if we are to have a sound, common ground to analyze motivational plans.

People. They have their similarities and their differences, and we attempt to handle these with approaches varying from human factors engineering to good human relations in supervision. 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.

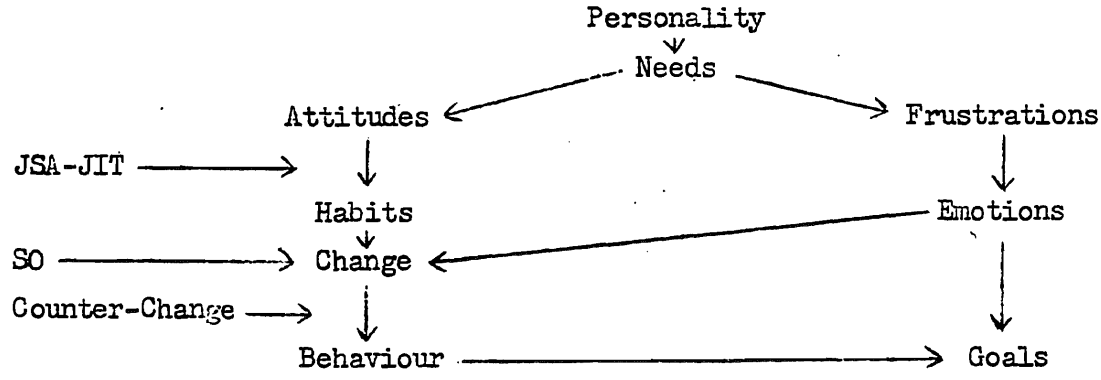
Attitude. There has been a lot of guff on attitudes in safety work, e.g. "Good attitude is all important". Actually, I could have a "wonderful attitude", and kill myself or someone else in the next five minutes if I don't know how to judge situations.

Fortunately the scientists have more useful ideas on attitudes. For example, that safety attitudes are information processing structures, and from this, that attitudes will be reflected in habitual reactions, good or bad.

This begins to tie back to our ideas of JSA-JIT-SO. That is, the person has been provided with some standards of safe behaviour (and can process information against those standards) and he has begun to form an attitude by habitual safe performance of a task.

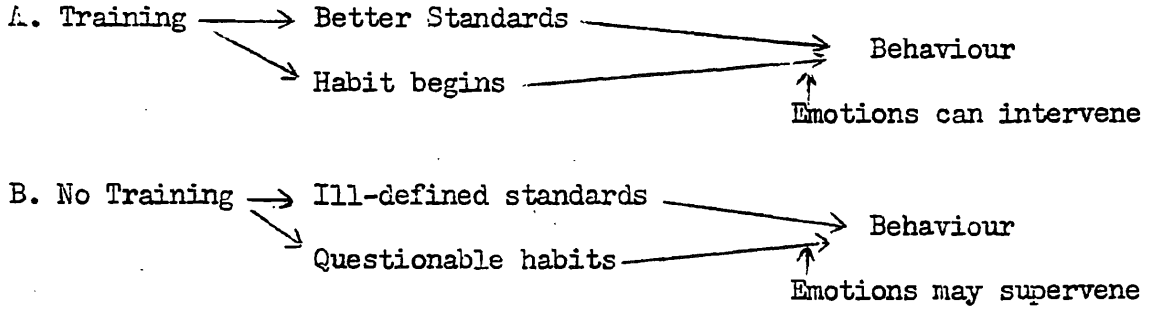
One of the foremost driver trainers in the U.S. said, "I don't give a damn about attitude. If a man doesn't know what to look for, and has no standards for judging what he does see, he'll have accidents". This may be something of an overstatement, but it does expose the fallacy in thinking that some vague kind of a "good attitude" produces safety.

Behaviour. What finally concerns us in safety is actual behaviour. We might then try a simple pictogram of the forces at work:



In this we imply that standards for habits have been provided and supervision has seen them in operation, so detects changes by observations and good, routine supervision, and counter-change restores safe behaviour.

We can use pictograms to trace two divergent sequences:



Innovation Diffusion. From studies of the introduction of innovations in U.S. agriculture and public health has emerged one simple way of analyzing and evaluating the mechanisms of change.

The process known as Innovation Diffusion 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 the individual can distinguish one stage from the other and can designate points in time when they went through each stage. The five stages are:

1. The awareness stage
2. The interest stage
3. The evaluation stage
4. The test stage
5. The acceptance stage

If the program planner knowns the process he can use it to better identify what stage the target person or groups has reached.

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.

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 affect him personally or his group.

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.

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.

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.

Now, two important and intensely practical points:

1. For stages 1 and 2, one-way communication may do the job.
2. For stages 3, 4 and 5, two-way communications are almost always necessary.

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 gets two-way, 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.

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.

Participation. We now see more clearly why participative activities are not just an option - they are necessary to success. The case histories of successful U.S. programs are replete with references to need for participation.

Participation can, obviously, take many forms. Committees are one of the forms very common in U.S. companies - 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 employee committees as such, there is most often great stress on other forms of worker participation.

There are three common forms of safety committees in the U.S.:

1. Corporate, or plant-wide - usually a management committee.
2. Departmental - usually a committee of foremen.
3. Area - a committee of workmen.

However, there are wide variations from this pattern, including plant labour-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.

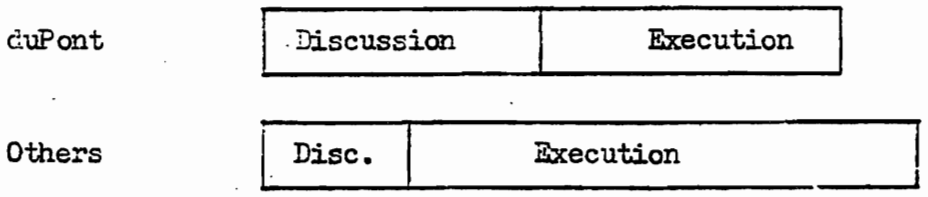
Written terms of reference for committees are essential. Meetings should be well planned. Follow up to secure action or disposition on recommendations should be unfailing. A record of accomplishment should be built.

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 lengthy, full discussion may be the best way to get there first.



The 5 E's. In the U.S. it has become common to refer to the 3 E's - Engineering, Education and Enforcement - as the three fundamentals of safety programming. However, a review of corporate program descriptions produces many references to two other E's - Enthusiasm and Example. Our review of background doctrine (particularly innovation diffusion) tells us why these are not optional, but necessary.

Social System. The plant or works is a social system involving many kinds of formal and informal relations. This suggests many considerations in designing a program. For example, who are the leaders among foremen? Among employees? Are they leading on safety?

Juran has dealt with the resistance to changes in business organizations and draws on the social sciences to suggest guidelines for diagnosis and planning.* Currie, in Section III, Table 5, has provided "Thirteen Steps for Innovation", and these deal primarily with social factors.

A Motivation Plan. Considering the complexity of an industrial situation and the difficulties in motivating human behaviour, it would be folly to proceed without an overall plan as well-based as possible and with some predictable bases for success.

To just start firing away with clever gimmicks, slogans, films, contests, etc., and hope for the best, is about as likely to succeed as an army fighting without a battle map and a battle plan.

---

* Juran, J.M. Managerial Breakthrough, Ch. 9, "Resistance to Change - Cultural Patterns," McGraw Hill, 1964.

A General Motors representative listed three essentials of their program as:

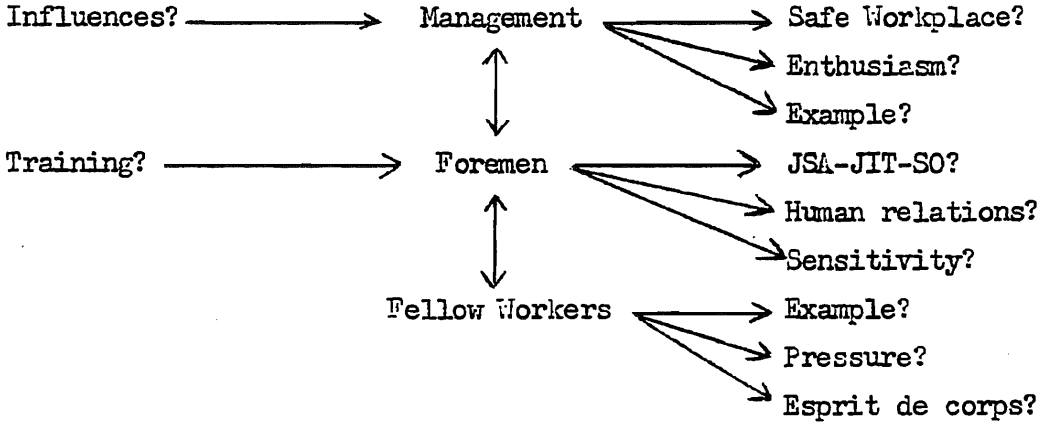
1. Formal training,
2. Participation,
3. A planned motivation program.

Good points, but I'd put them together under a planned program for behaviour.

Let us begin with a sheet of paper large enough for a war map - say 17 x 22 inches. Rule it into four quadrants.

1	2
3	4

In quadrant 1, put a picture of the elements of the social system:



In quadrant 2 put the pictogram of the individual from page 41 (tracing the steps leading to behaviour).

These then, are some things which will influence the workers. What's their status? What shall we plan to do to improve? Who are the leaders? Where do they stand on acceptance of any innovation?

In quadrants 3 and 4, list the communication modes used in your program:

One-Way Communications	Two-Way Communications
Posters	Participation in job analysis
Contests	Committees
Leaflets	Meetings - small, two-way
Plant Magazine	On-the-job - enthusiasm
Meetings - large, or one-way (films and speeches)	team spirit
	Example of management
	Informal
Leaflets to home ⟶	Family discussion

If we want to analyze communications in more depth, we can take our three or four major problems or problem units and make a sub-map for each special emphasis topic, entering only those activities pertinent in content.

We can begin to weigh content, variety, timing, and appeal.

We can now go over the charts again and begin to insert quantifying measures. How much training? How many meetings of each type? How many committees? How many posters or leaflets?

Then we can go back over the chart once more and try to assess quality in terms of actual effect, and be hard-nosed about this. Where possible measure changes in behaviour.

We could even insert names of leaders and innovators of significance, or write in names of ultra-conservatives who are special targets. Examples, at a management level, might be:

*Joe Cook, Chief Engineer, is on the Safety in Design Committee of the Mechanical Engineers.

*Al Bonnes, Research Director, is preparing a paper on uses of x metal.

*The Boss is mad over the errors in specifications for the widgets we bought.

*The Boss is even angrier that Zilch Mfg. Co. surpassed us in profits. (They got a safety award last year).

*The plant addition is three months behind - two small fires, and no PERT chart.

*The new training director is full of fire. Looks good.

*Mike Peters, foreman, Area 22, a real innovator - asked for suggestions on improving his program..

Examples at the employee level might be:

*The death of _____, a real leader, in a motor vehicle accident is being widely discussed (No seat belts).

*Some of the poster sketches sent in as suggestions are better than the mail-order stuff. Start a contest?

A time-line analysis of communications is also helpful in judging continuity and variety.

Dr. Francis McGlade, Chief, Education Branch, Safety Division, U.S. Army, prepared a most valuable summary of principles for a safety management seminar[1]:

> "The communication: must be placed in a prominent position where individuals are more or less 'forced' to look at the message, since it cannot be assumed that people will read the message simply because

1. McGlade, Francis, "Psychology in Safety Management", Journal of A.S.S.E., November, 1967.

a poster is hung on a wall; must be relevant to the activities engaged in by personnel within the environment in which the communication is presented; and should be removed when its effectiveness is considered to be exhausted. One research study indicates that specially designed safety posters which contained definite instructions remained effective for approximately three months.

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 'shotgun' 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 should be limited in number so that the recipient can readily absorb them.

There is yet another ingredient which should be woven through the communications fabric - the utilization of feedback. Unfortunately, safety management has used this tool sparingly in the past, if at all. The engineering concept of feedback refers to the ability of a complex system to check on its own performance and to correct it, if necessary. In the psychological context, it refers to the checking and correcting of behaviour.

All of us use the principle of feedback in our day-to-day communications. Most often this is done in a vague, careless, and sometimes expensive manner. Experiments have revealed that communications gain in speed and efficiency as more and more feedback takes place. Therefore, it is imperative that safety management make deliberate use of this technique in collecting, studying, and analyzing reactions of personnel to safety mass communications and the influence of such communications on accident-related behaviour".

In discussing motivation for safe performance, McGlade suggests an "internalized motivation" approach where opportunities are provided within the job itself to achieve satisfaction of needs.

"Internalized Motivation may produce better results but it is more difficult to administer. Administration of this approach in safety management can be made easier through application of some additional motivational guidelines: (1) rewards, such as monetary compensation, official recognition, and even praise; (2) immediate benefits are more attractive than remote ones, and therefore it may be wiser to plan and implement a series of short-range safety objectives than to establish one long-range goal; (3) familiarity can enhance motivation; (4) reciprocal interest should be included in motivational techniques

whenever possible; (5) the safety objectives should be commensurate with the abilities of the workers and relevant to the activities workers engage in, otherwise 'fear of failure' may be established as a motivating factor; and (6) motivation is facilitated by participation and involvement.

This last point may well be first in the hierarchy of motivational principles. People appreciate the opportunity to express their ideas and viewpoints and to have some part in the decision-making that affects them and their work. First-line supervision has employed this principle in accident prevention efforts to a marked degree and with excellent results. But top management has sadly neglected the use of this principle.

How many safety staffs in industrial and business organizations solicit the participation and personal involvement of other staff elements in developing and implementing safety campaigns and accident prevention measures? This happens infrequently and in those occasional instances is more or less a chance occurrence. There is a critical need for greater utilization of this principle in safety management at the higher levels.

A final word in regard to motivation. Too often punishment is employed as the primary motivational tool, hidden under the guise of 'discipline'. Punishment usually results in avoidance behaviour directed toward evading a given result, rather than in positive directed action toward the accomplishment of an objective. This is especially true if the punished person perceives it as being unfair. He then becomes hostile toward the punisher (this can include his supervisor, the foreman, management, and the entire organization). Such hostility spreads to include all objectives of the punisher, and not merely the objective associated with the specific punishment".

It will be readily apparent that our "battle map" (or maps for problems and problem departments) will hardly be adequate to contain all the needed analysis as communications are integrated and carried out in an operating organization. But we will have begun a substantive and valuable analysis of the overall program. And we shall be far from the gimmicks and novelties.

In Summary. Motivation is complex and difficult. Borrow from the sciences and the experiences of others. Have a plan.

If an idea isn't working - drop it - even it it was your pet.

Beware of one-way communications as anything but a start. Beware of speech-makers, even yourself.

Look for, praise, and help innovators and good examples.

ACCIDENT INVESTIGATION AND ANALYSIS

It would be easy to put accident investigation and analysis first in a discussion, because it is fundamental to a good program. Then we would ask, "What kind of facts do we need?" Now, having developed concepts of program and causation, we are in a better position to know what facts we need.

We shall assume multi-factorial causation, and we want to identify causes of causes "unto the third generation".

It is not uncommon to hear, "We need more information", when an accident is being discussed. Less frequently do we hear precisely what additional information is needed.

What facts to seek - level 1. Here we want to trace, at least:

1. Energy transfer and barriers.
2. What was the man trying to do?
3. JSA-JIT-SO sequence. If you do not have this strict sequence, you have a lower grade substitute.
   a. You have some job procedure, formal or informal,
   b. You have some training,
   c. You have some supervision.
4. What changes occurred, in equipment, arrangement and environment, personnel, procedures, tasks, supervision?
5. What were the specific errors by anyone?

Facts - level 2. What did immediate supervision do or not do:

1. Re the trigger episode?
2. Re precipitating factors?
3. Re background factors?

Facts - level 3. What did line management at higher levels do or not do?

Facts - level 4. What did staff departments do or not do regarding any of the factors?

Facts - level 5. What could top management have done to alter the contributing factors?

Analyzing the Facts. In analyzing the facts about an accident and tracing each of several (or many) errors to organizational roots we can use a matrix to challenge our work:

Factors	Trigger	Proximate Factors	Background Factors
Equipment and Material			
Arrangement & Environment			
Procedure			
Personnel			
Training & Supervision			

We ought to have one entry in the first column and entries on most lines in the other two columns - a total of 21 possible entries.

If we do this separately for accident occurrence and injury severity, we have two matrices and about 40 entries.

Something of this order should be our goal.

In the U.S. only the major accident reports of the National Transportation Safety Board provide numerous examples of this depth of study and analysis. Some other governmental reports are known to be complete in catastrophic matters. Corporate reports are, of course, privileged documents, so we don't really know how good they are.

Could more or less routine reports approach this detail? Yes. It is more a matter of what we look for and how we analyze, than it is cost. Stepping on toes is probably more of an obstacle. Perhaps people at higher levels must be educated to want to know their errors - of omission as well as commission.

Accident Report Forms and Questions

The standard Supervisor Accident Report of NSC asks these questions:

Length of Service: With Company?
On Present Job?

Occupation?

Nature of injury?

Description of accident.

What Job was Employee Doing, Including Tools, Machine, and Materials Used?

How Was Employee Injured?

What Did Employee Do Unsafely?

What Was Defective, in Unsafe Condition, or Wrong with Method?

What Safeguards Should be Used?

What Steps Were Taken to Prevent Similar Injuries?

What Other Steps Should be Taken to Prevent a Recurrence?

Our analysis suggests the following kinds of questions:

1. Does a JSA exist for this job? (Attach) Is the JSA complete and correct?
2. Did the injured (and others in the work crew) have JIT for this job?
3. Was there change in the material?
4. Was there change in the equipment?
5. Was there change in the job procedure?
6. Was there change in arrangement or environment?
7. Was there change in the man?
8. Was there change in supervision?
9. When did the changes (above) occur?
10. Were the changes known prior to the accident?
11. When did the supervisor last see the employee doing the task correctly? When did the supervisor last make a recorded safety observation on this employee?
12. When did the supervisor last see the employee before the accident? Any special contact or observation at that time?
13. Where was the supervisor at the time of the accident?
14. If there was unsafe equipment involved, when was it last inspected? What was its condition then? If o.k., when and how did condition change?
15. When was the next inspection scheduled?
16. What countermeasures should be introduced into the system to counter the undesired changes that occurred?

Some experimental use of these questions has shown them to be very revealing. For example, an engineer used the question, "When did you last see this man do this job safely?" In the first two accidents he got the answer, "Never". This occurred in a company which thought it had a tight control!

Mass Reporting. No accident report form of practicable length has yet produced adequate reports of accidents - occupational, traffic, home, farm or product accidents. This has lead to the concept that where mass statistics are to be collected, a "bi-level" system is needed. The routine report is boiled down to an absolute minimum. Supplemental reports are then designed for specific kinds of accidents on which more information is needed. When an adequate sample of special reports has been collected, the supplemental report is discontinued.

A Natural History? It has long been known that a blank sheet of paper is an adequate form for the skilled investigator. The present inadequacies of routine forms, and the concept of sequences of developments of factors, suggests that a detailed "natural history" of the sequence of developments provides the most generally useful record for subsequent analysis and action.

Frequency and Severity Matrix. In system safety analysis a matrix of frequency and severity of accidents/incidents is more and more frequently used to evaluate the degree of hazard.

Frequency can be grossly categorized (where study data are not available). Classes will normally vary on the order of exponents - that is an order of magnitude may be 10,000, 1,000, 100, 10, 1. Roman numerals are used below to show these kinds of variation.

Severity can be categorized as to criticality by a Department of Defense classification:

A. NEGLIGIBLE: Condition(s) such that environment, personnel error, design characteristics, procedural deficiencies, or subsystems or component malfunction will not result in major system degradation, and will not produce system functional damage or personnel injury.

B. MARGINAL: Condition(s) such that environment, personnel error, design characteristics, procedural deficiencies, or subsystem or component malfunction will degrade system performance but which can be counteracted or controlled without major damage or any injury to personnel.

C. CRITICAL: Condition(s) such that environment, personnel error, design characteristics, procedural deficiencies, or subsystem, or component malfunction will cause equipment damage or personnel injury, or will result in a hazard requiring immediate corrective action for personnel or system survival.

D. CATASTROPHIC: Condition(s) such that environment, personnel error, design characteristics, procedural deficiencies, or subsystem or component malfunction will severely degrade system performance, and cause subsequent system loss, death, or multiple injuries to personnel.

Thus, we develop a matrix for assessment of a hazard:

		Severity			
		A	B	C	D
Frequency	I	x			
	II	x			
	III		x		
	IV			x	
	V				x

We have placed x in areas which could be seen as representing some "normal" pattern of events in a poorly controlled situation.

Matrices of this type are coming into use in product safety.

MEASUREMENT OF PERFORMANCE

A good deal of attention in the U.S. is being given to improved measurement of safety performance. The standard ASA disabling injury rates almost universally used are good as far as they go. But more accurate and more meaningful (action-oriented) measurement of the underlying situation is felt needed.

"Industrial Safety Performance Measurement" is the subject of two symposia sponsored by the National Safety Council's Industrial Conference. The first has been reported. The second is in process. Eight scientists have prepared advance papers on specific aspects of the general topic. Written and oral critiques will be received from forty additional scientists prior to and during a symposium. Individual and group conclusions will be published, including recommended lines of investigation. Hopefully a demonstration project would develop in two to five years.

We can, perhaps, categorize our measurement problems under four headings:

1. Accident or incident rates.
2. Program measurement.
3. Situational measurement - what's actually going on in the plant?
4. Scientific studies.

For present purposes we can dispose of the fourth group with several recommendations:

1. Support independent research efforts better.
2. In larger plants, conduct scientific studies.
3. Watch the studies for findings, principles, and methods you can use.

In the meantime, pending better scientific development, we must use what pertinent data we have or can, in practice, obtain.

Accident Rates. Ideally we would use rates which included all accidents and near-accidents to measure performance. For a variety of reasons this is not feasible - comparability of data and availability of data being primary.

Standard Rates. In the U.S. the ASA (later USASI and now ANSI) rates are almost universally used. There are a variety of quarrels on definitions, but these are not significant, except to effect minor improvements in the ASA method. The principal problem is the relative rareness of the disabling injury as an event. And the second, related problem is that smaller units have wide random variations in rates. One year a unit looks good - the next year it is a dog! This latter is correctible by statistical evaluations. However, even for large corporations, the standard rate has provided no warning of impending trouble, nor what to do about it.

The chemical industry working party report provided us with a comparative study of U.S. and British rate methods, which is very useful in attempting rate comparisons. However, for our present purposes, the methods are more nearly the same, rather than different.

Serious Injury Index. In the U.S. the use of a rate incorporating injuries of types different or less serious than the disabling injury (as defined) are coming into increasing use. (One index includes medically attended eye injuries, fractures, sutured wounds, and work restricting injuries). This type of rate is an improvement, but far from an adequate measure of performance. It suffers from the same basic limitations as the ASA rate.

First Aid or Medical Treatment Injuries. Historically experience has shown that if comparisons of units are based on such reports, reports will dwindle, and infections will rise. If reporting declines, the loss of reports for prevention analysis is serious.

Damage Accidents. One U.S. company, Lukens Steel, has made outstanding use of damage accident reports. Its program was reported to the British iron and steel industry. However, here the primary emphasis is on the prevention use of damage incident 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 over disabling injury rates. On a premise that management is cost-oriented, the measure is a valuable addition to management incentives.

Frequency and Severity Rates. The disabling injury frequency rate and the severity rate (days lost per unit man-hours with time charges for permanents and fatals) are standard U.S. practice. Considerable discussion has surrounded combining these rates. This is mostly nonsense. The British method of using a frequency rate and average severity is just as good. Multiply the two and you have a "severity rate".

Both measures are useful. No combination will do what two measures will do.

Weighted Rates. There have been proposals for weighted rates - not only for frequency and severity of injuries and damage, but also for penalty provisions for repeated accidents from the same cause*. These efforts are worthwhile, but suffer from two limitations: (1) the factors measured are too limited, and (2) the weights are arbitrary and untested. However, where uniformity of application can be attained within an organization, such rates can be very meaningful.

---

* For example, C.D. Attaway, "Safety Performance Indicator Fills a Management Need", Journal of ASSE, March, 1969.

Bad Features of Rates. We must be aware that our rate measurement efforts may do harm as well as good. Three major problems are:

1. Rate differences of a minor nature are taken seriously,
2. Comparisons of units are thought to be valid,
3. Rate definitions warp programs.

A plant with a frequency of 2.54 is said to be better than a plant with a frequency of 2.67. This is not necessarily so. If any kind of statistical test of significance were applied to such numbers the most likely answer would be: "The plants are probably the same". And if the low rate plant was substantially smaller, the statistician would say: "The high rate plant may be better".

When rates are used foolishly and without safeguards, we should not be surprised if they generate scepticism.

Inter-unit comparisons are another problem. Dependent on the number of competing units we subdivide into "comparable" groups. But comparable within what limits? A plant with a five-year rate of 2.0 is almost unquestionably better than a plant with a rate of 6.0. But, for one-year rates, and considering differences in operations, age of plant, etc., is a plant with a rate of 2.0 better than a plant with a rate of 3.0?

In the U.S. the wide use of standard rates probably has three serious disadvantages:

1. The emphasis on return to work, in the opinion of some industrial medical specialists, may have undesirable side-effects on therapy, even though the overall purpose of rapid rehabilitation is sound.
2. The emphasis on frequency rates may warp attention to serious hazards according to their importance, for example, fires or electrocutions.
3. It also warps attention to minor accidents, damage accidents, and near-misses.

So rates can do harm, as well as good.

Program Measurement

A first step in program measurement is to have accurate data on the degree of coverage of the program. What percent of supervisors have had what kind of training? What numbers and kinds of hazards are turned up in the regular inspections of different kinds? How many foremen hold "5-minute tool box" meetings, and how often? These measurements would be numerous.

The second step in an ideal program is probably best represented by U.S. Steel. Safety Observations are scheduled. All results are tabulated by types of violation or unsafe act and by employee. So are accidents and other incidents observed in regular supervision. Entries are made daily, cumulated monthly, and forwarded to

management. Thus, both the supervisor and his supervisor have a continuous barometer reading on hazards, or as their forms put it, "Safety Awareness". Advance warning signs of trouble are given, and in accident investigation there is some kind of a system which can be studied to determine the point of failure.

A third step in program measurement is to fully utilize and integrate program data. This is to say that accident reports are, in effect, a test of the inspection system - why wasn't a hazard detected, or if detected, not corrected. And, if inspection data are inter-related, do we see repeated violations of the same type or in the same place. A chronic problem with inspection reports is failure to seek and deal with the cause behind the violation or condition.

Accident reports are really a harsh audit of the program system. What do they reflect in program breakdown? And when we refer to the cause behind the cause we are thinking of such questions as whether supervisors really have the time to do what is expected of them.

Situational Measurement

It is axiomatic that actual, operating systems deviate from manuals or other theoretical ideals. And second, that systems can only be operated effectively if there is some appropriate information feedback for control purposes.

U.S. railroads are a case in point. Operations do deviate from manuals, and accidents result. But, management has no reliable, independent information system to find out what is really going on. Supervision has first responsibility for observation. But management must question and audit the direct program data. The U.S. National Transportation Safety Board formally recommended the railroads reappraise their programs in this respect.

A generalization is possible - no matter how small a sample observation plan must be because of budget, there must be a sampling system or there is no control.

Sampling methods in the U.S. are not far advanced. Tarrants applied the Critical Incident Technique in one plant as a scientific study, but the method has not been widely repeated nor adapted for routine use.* The NSC Manual describes a "walk through" sampling method, but this would have many biases.

Probably the best present answer is to begin with a purely random method, e.g. every 20th or 50th name on the hourly payroll. If you can only go once a year to find out what a man's tasks and performance may be - GO. Preferably, go more often for better data.

---

* Tarrants, Wm. E., "Applying Measurement Concepts to the Appraisal of Safety Performance", Journal of ASSE, May, 1965.

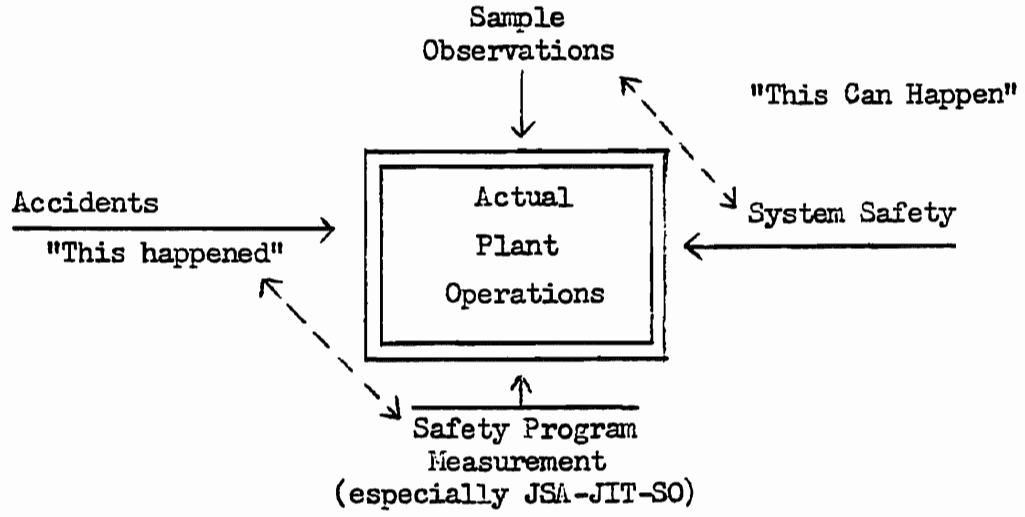
Naturally the observation method is pertinent. Shall it be casual or detailed, and undetected or direct? If the latter, what interview technique will be used? All these are good questions, and we want to be as scientific as possible. But, remember the comment, that fragmentary error data are useful.

Set up some sampling method, apart from the inspection system. Audit the auditors!

Summary

A variety of measurements of performance are needed. A planned program of measurement should be established. The program can provide invaluable data for management and control. At least until more experience is gained, no plan can provide valid inter-plant and inter-department comparisons - the problems are too varied.

Measurements of four principal types should be utilized, and have the effect of monitoring operations from divergent viewpoints. The four measurements provide cross-checks on one another.



Goals. Perhaps the biggest fault in safety planning is the failure to establish goals and plans which challenge and yet are attainable. The vague hope that "we can do better" is not enough. A program must be directed toward attainment of measurable goals - program goals as an intermediate step, and accident reduction goals as a final step.

We should have a picture of an ideal program to help in measurement and planning and to know how far we have to go.

SYSTEMS SAFETY ANALYSIS

a modern approach to safety problems

Developed in the aerospace industry to assure safe performance of hardware, the method can be extended to include any aspect of the man/machine/environment complex

By J. L. RECHT
Assistant Director Statistics Division

NATIONAL SAFETY COUNCIL
425 N. Michigan Avenue
Chicago, Illinois 60611

Systems Safety Analysis: an Introduction

Methods developed in the aerospace field hold promise for all industrial safetymen

By J. L. RECHT

WE have all heard that this is the space age. But, except for following the exploits of the astronauts and looking at pictures of the moon and Mars, most of us have not felt the impact of the new technology which has made the space age a reality. This new technology has produced new hardware — rockets, missiles, and supersonic aircraft — but these products are only the tangible results of the new analytical methods and new theoretical concepts which form the core of our advancing technology.

For those of us in the safety field, this situation is likely to change rapidly. Concepts currently in use in the aerospace industries—which can be described by the phrase "systems safety analysis"—are beginning to have important ramifications in other industrial fields.

Systems safety analysis is not an ill-defined approach to safety or a phrase that masks the same old approaches—it is in fact a concept so well-developed in the industries closely involved with space programs that recent Department of Defense military specifications require the application of systems safety analytical techniques as part of contract terms, and it appears that such requirements could spread beyond the aerospace industry. Systems safety approaches are also being utilized to analyze product safety in a few private industrial establishments.

In the years to come, safetymen will hear more and more about systems safety—and most of what they hear will be couched in the special vocabulary that has developed

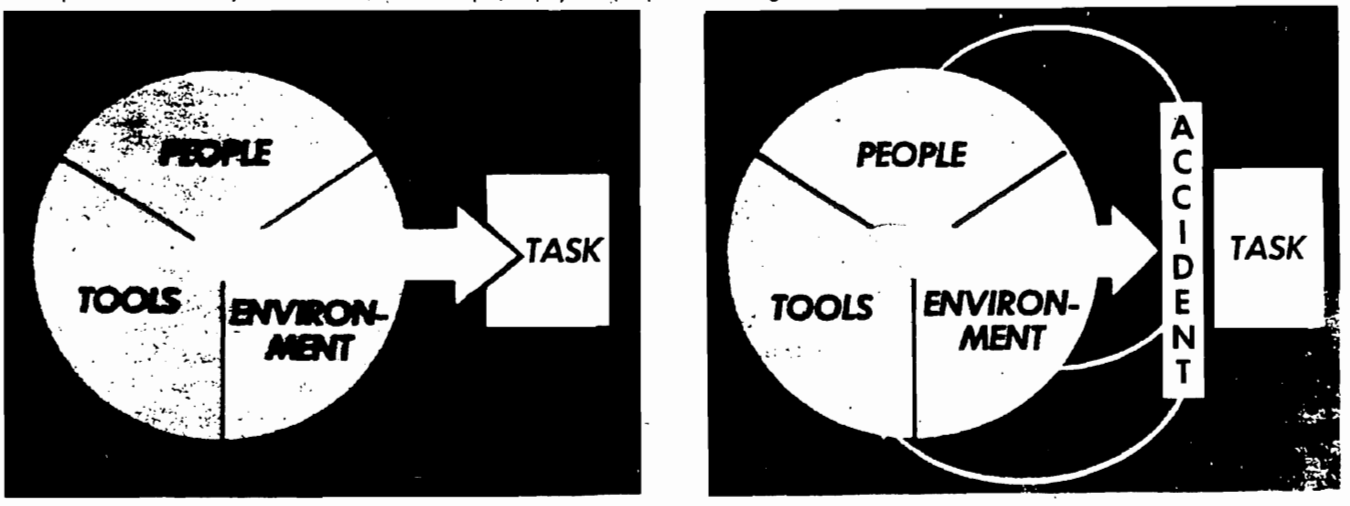
The author, assistant manager of the NSC Statistics Division, recently attended an intensive two-week course in systems safety analysis conducted jointly by The Boeing Company and the University of Washington.

To date, the systems safety analytical techniques alluded to in this article have not been utilized directly to solve occupational safety problems. They have been used almost exclusively to control the safety of very expensive and potentially very dangerous products of the aerospace industries — rockets, aircraft, etc.

It remains for the concept of systems safety, and those of its related techniques that are practical in the industrial safety arena, to be implemented by industrial safetymen.

In this and future articles we will attempt to open the door to the possible ways this implementation can be accomplished.

At the left is a generalized model of a system showing the elements "people," "tools," and "environment" combined to perform a task. The model at the right illustrates the effects of an accident on a system: the task performance is interrupted or degraded, and there may be impairment of the system elements; for example, injury to people or damage to tools.



among aerospace systems safety engineers.

Safetymen will not only hear about these techniques, they will have to understand them, for many will be called on to find ways of implementing them. And although complete implementation of systems safety analysis involves specially-trained engineers and rather sophisticated mathematical manipulations, safetymen will find that knowledge of the most rudimentary facets of these techniques can be of direct benefit in helping codify and direct their accident prevention programs.

Why systems safety?

The history of systems safety analysis really began in the aerospace industry. It was the result of the extremely high reliability and safety specifications demanded by the space and military requirements and the fact that the time-honored production sequence was no longer practical.

Until recently, when a new aircraft was developed, it was first designed, then an experimental model was built, and finally it was test-flown to determine its capabilities and flaws; the information obtained indicated the necessary design changes and the cycle was repeated until the performance specifications were met. Today's aircraft and missiles are so complex and costly and the specifications are set so high that this procedure had to be changed. Moreover, missile flight tests involve loss of the model with only limited telemetry data obtained. Today the "bugs" must be found and corrected as far as possible in the design stage using analytical techniques.

The result is the development of the systems approach to safety. The aircraft or missile is examined from this point of view and the effects of any failures or malfunctions on the operation of the aircraft are evaluated to determine the principal design defects which need to be fixed. For these complex systems, sophisticated analytical methods have been developed using high-speed computers. Thus the test pilot has been replaced by a systems safety engineer and a computer. The objective, "First time safe," is quite different from the objective of investigating accidents and preventing recurrences.

For simpler systems merely having an understanding of the systems approach can have great benefits. This article is an effort to introduce and *define* systems terminology. In future articles an effort will be made to explain the systems approach and to show how it can be applied to industrial safety.

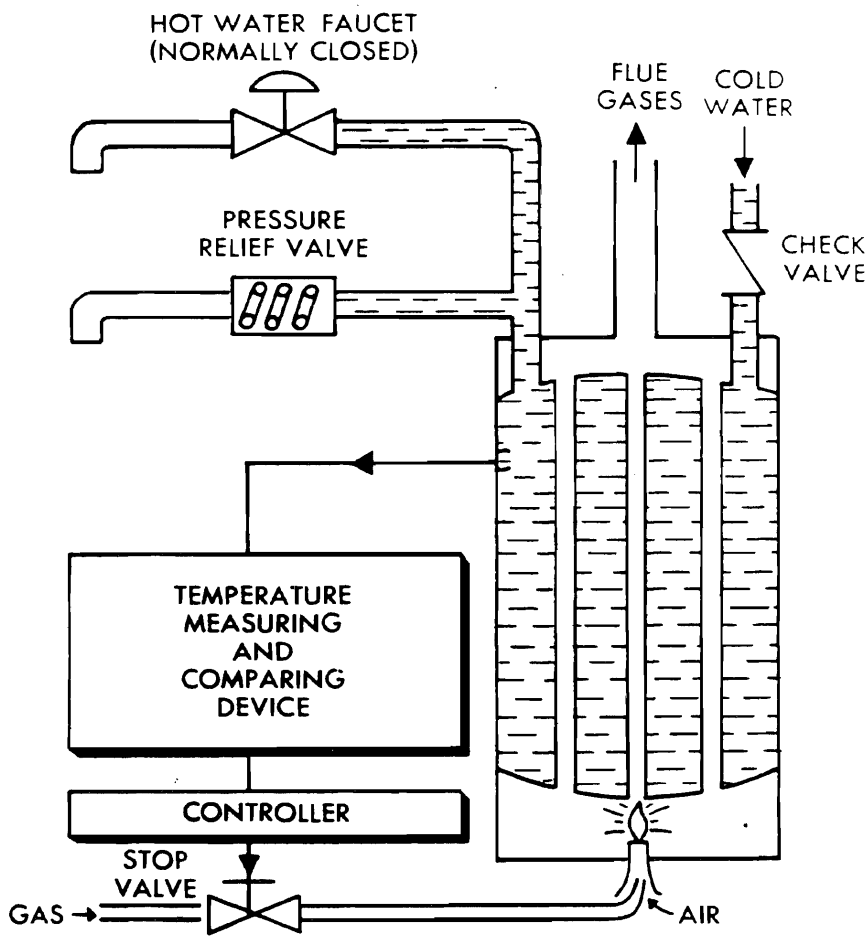
What is a system?

To understand the systems approach we should first have a clear picture of what a system is. Definitions tend to be restricting, but one which might serve our purposes is the following:

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.

EXAMPLE OF A SYSTEM

(DOMESTIC HOT WATER SYSTEM)



The main points to keep in mind are that a system is defined in terms of a task or function (it is task-oriented), and that the components of a system are interrelated, that is, each part affects the others.

The task or function which a system performs may be simple or complex. Sometimes it is convenient to break up a complex task into simpler tasks and consider subsystems of the larger system. Subsystems consist of part of the components of the over-all system and perform a portion of the over-all task.

System components

The components of a system can cover a wide range including machines, tools, material (i.e. hardware, chemicals, etc.), environmental factors, people, documents

(such as operating instructions, training manuals, or computer programs), and so on. As parts of a system, the components usually complement each other but it is essential to recognize that a failure or malfunction of any component can affect the other components and thus degrade the performance of the task.

The environment is an important consideration in a system since most systems will perform their task properly only under a given set of conditions. A component that works well at normal temperatures may be placed in a system near another component that generates high heat and thus the first component will not function properly. The environment in which the components operate must always, therefore, be considered as a part of a system and be included in any examination of a system.

A sample system

An automatic gas hot-water heater is a good example to use in illustrating the elements of a system. The task of the system is to provide hot water in our house at all times. In order to perform this task a system is used whose components consist of a water tank, a gas heater, a temperature measuring and comparing device to regulate the system, a controller (actuated by the temperature measuring device) to turn a valve, a gas valve to control the flow of the gas, a pressure relief valve (to permit excess pressure to escape if the gas heater fails to shut off), a cold water intake pipe, a hot water pipe leading to the faucets, and an exhaust pipe for the flue gases from the gas heater.

From the view of task performance, we can examine the system to see in what ways failure or malfunction of the components can stop delivery of hot water when we want it, or, more importantly, when the system might get out of control and the tank rupture or gas escape. The interrelations of the components are apparent to anyone familiar with the operation of such a heater and we can trace through the system the effects of any component breakdown.

Another example which is not completely mechanical is the system for waking you up in the morning. The task is waking you at the desired time. The system components consist of an alarm clock, you, and the environment. The clock (which here is a subsystem) must be in good working condition to perform the task, but this is not sufficient. The clock must be wound, the time set correctly, and the alarm button pulled — you perform these operations.

In addition, if the clock is kept under conditions of abnormal heat, moisture, dust, and so on, it will eventually fail to function as it should and the alarm system will not perform its task.

Again it is relatively easy to see the interrelationships of the components and the effects of any malfunction on task performance.

Analyzing systems

Having established the concept of a system, the next step is the analysis of systems—especially complex systems such as aircraft, communications networks, or production lines. It is in this area—the analysis of complex systems — that great progress has been made in recent years in the aerospace industry which holds great promise for application throughout industry.

It is not possible in an introductory article to describe in detail each of the analytical methods which have been developed. However, it might be helpful to indicate briefly the main techniques in order to clarify the nature of the systems approach to safety.

No matter which method of analysis is used, it is important to have a model of the system. Most models take the form of a diagram showing *all* the components. This makes it easier to grasp the interrelationships and simplifies tracing the effects of malfunctions.

Methods of analysis

There are four principal methods of analysis: failure mode and effect, fault tree, THERP, and cost-effectiveness. Each has a number of variations and more than one may be combined in a single analysis.

Failure mode and effect

In the failure mode and effect method, failure or malfunction of each component is considered including the mode of failure (such as, switch jammed "on"), the effects of the failure are traced through the system, and the ultimate effect on the task performance is evaluated. Failure mode and effect analysis is straightforward assuming that the analyst is thoroughly informed about the system. One drawback of this method, however, is that it considers only one failure at a time and thus some possibilities may be overlooked.

Fault tree

In the fault tree method an undesired event is selected and all the possible happenings that can contribute to the event are diagrammed in the form of a tree. The branches of the tree are continued until independent events are reached. Probabilities are determined for the independent events and after simplifying the tree, both the probability of the undesired event and the most likely chain of events leading up to it can be computed.

This is a very powerful analysis technique but has the drawback of requiring a fairly heavy mathematical background and a good computer to obtain the maximum benefits of the method. Boeing Company has refined the fault tree method to a high degree and has found it practical for analyzing aerospace products.

THERP

THERP, technique for human error prediction, developed by Sandia Corporation, provides a means for quantitatively evaluating the contribution of human error to the degradation of product quality. It can be used for human components in systems and thus can be combined either with the failure mode and effect or the fault tree methods.

Cost effectiveness

In the cost effectiveness method, the cost of system changes made to increase safety are compared with either the decreased costs of fewer serious failures, or with the increased effectiveness of the system to perform its task, to determine the relative value of these changes. Ultimately all system changes have to be costed, but this method makes such cost comparisons explicit. Moreover, cost-effectiveness is frequently used to help make decisions concerning the choice of one of sev-

eral systems which can perform the same task.

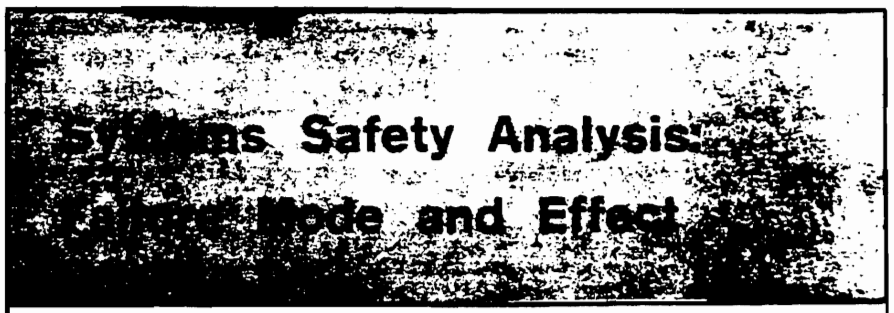
In all of these analytical methods the main point is to measure quantitatively the effects of various failures within a system. In each case probability theory is an important element.

Zero defects programs

In the aerospace industry there are a number of programs called "zero defects" programs with such interesting names as: Pride, Aware, Esky, Project Sterling, and others. These are primarily quality control programs aimed at motivating greater attention to product quality. They are not systems safety analysis programs in the strict sense. Safety naturally should be improved but this is a secondary rather than a primary objective of these programs. ZD programs are a consequence of the extremely high specifications now set for aerospace products.

The industrial safety engineer might well ask what all this systems analysis has to do with him. The answer to that question, and the major point of this article, is that anyone can use and profit from the systems approach to safety. The systems notion helps to enlarge one's viewpoint. Becoming oriented in terms of task performance and being forced to visualize the interrelationships of all the components of a system helps to bring most accident possibilities into consideration automatically and in an orderly manner.

The systems approach to safety can help to change safety engineering from an art to a science by codifying much of our knowledge. It can change the application of safety from piece-meal problem solving (putting a pan under the leak) to a safely designed operation (avoiding the leak itself). We can apply the question "what can happen if this component fails" to the various elements of the systems and come up with adequate safety answers *before* the accident occurs instead of after the damage has been done.



Systems Safety Analysis: Failure Mode and Effect

Failure mode and effect analysis is one of the four principal methods used by systems safety engineers. This article gives a general outline of its main aspects

By J. L. RECHT

IN OUR FIRST article on systems safety analysis
the basic terms and concepts were introduced and brief descriptions were given of the four principal methods of analysis. In this article one of the analytical methods — failure mode and effect — will be discussed in some detail.

First, however, it would be well to review the basic definition of a system:

A system is an orderly arrangement of components that are interrelated and that act and interact to perform some task or function in a particular environment.

The main points to keep in mind are that a system is defined in terms of a task or function, and that the components of a system are interrelated; that is, each part affects the others.

No matter which method of analysis is used, it is important to have a model of the system. Most models take the form of a diagram showing all the components. This makes it easier to grasp the interrelationships and simplifies tracing the effects of malfunctions. The system we shall use for the purpose of illustrating failure mode and effect analysis is the domestic hot water system. A simplified model of such a system is on the facing page.

FM & E form

Once the model or diagram is drawn, the only other paperwork needed is a form similar to the one shown. There are many variations possible in the layout, depending upon how elaborate an analysis is needed. What is shown is a suggested minimum for practical use.

The entries in the various columns of the form should be as follows:

- Component — list the individual component being considered. (It is sometimes important to consider two or more component failures together as well as separately.)
- Failure or Error Mode — show the exact manner (or mode) in which the component can fail; there will frequently be several failure modes for a single component.
- Effects on System Operation — indicate the effects on the other components in the system for each specific failure.
- Effects on Task Performance — indicate in detail for each specific failure how it affects the overall performance of the system with respect to the system's task.
- Hazard Classification — estimate the seriousness of the specific failure. A simple four-way hazard classification used by the military can be applied here:

1. Safe: Failure will not result in major system degradation, and will not produce system functional damage or contribute to system hazard or personnel injury.
2. Marginal: Failure will degrade the system to some extent without major system damage or personnel injury, but can be adequately counteracted or controlled.
3. 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.

4. Catastrophic: Failure will produce severe degradation of the system which will result in loss of the system or death, or multiple deaths, or injuries.

• Failure Frequency — estimate the average time between failures for each specific failure mode. An easily applied classification is as follows:

1. Probable: one failure in less than 10,000 hours of operation.

2. Reasonably probable: One failure in 10,000 to 100,000 hours of operation.

3. Remote: One failure in 100,001 to 10,000,000 hours of operation.

4. Extremely remote: One failure in more than 10,000,000 hours of operation.

Estimates of failure frequency can be made from accident experience, test results from component manufacturers, comparison with similar equipment, judgment, engineering data, etc.

• Detection Methods — this column can be helpful in indicating the need for better detection in serious cases.

• Compensating Provisions and Remarks — this column is to be used for commenting on what should be done (or possibly on what has not been done) in order to avoid the consequences of the specific failures.

In the form shown we have given a few sample entries for the domestic hot water system.

Analysis objectives

When the form is completely filled in, the objectives of the analysis become clear — to determine the probable and reasonably probable critical and catastrophic failures, and to find ways of modifying the system so as to reduce the failure frequencies or to offset the consequences of these failures.

In evaluating failure frequencies, an important consideration is the life of the system. Every system has a limited useful life. This can be estimated in hours of operation. For example, we might say the domestic hot water system can be expected to last about ten years, or roughly 85,000 hours of operation.

A failure that has a frequency of occurrence once in 500,000 hours of operation is obviously a remote possibility for a single hot water system. But for six hot water systems during a ten-year period this failure is likely to occur. For many hot water systems, for example in a housing development, the failure is almost certain to occur.

It is important, therefore, to keep in mind the expected life of the system (and the number of such systems, if you have more than one) when deciding on the need for immediate action on the basis of failure frequencies.

It is also valuable to know whether or not there is any way of detecting that a failure has occurred in those cases that can be critical or catastrophic so that immediate countermeasures can be taken. Lack of detection methods increases the likelihood that a specific failure will lead to the worst possible consequences.

Any serious hazardous situation unquestionably must be fixed and there are many ways to do so. Looking just at the equipment (and disregarding personnel, location, etc.) the various fixes might include: hazardous condition detection, failure sensing devices, fail-safe devices, redundant components, interlocks, protective devices, compensating equipment, self-repairing or self-adjusting equipment, and escape subsystems.

Reliability vs. safety

A system is designed to perform a task and therefore reliability of performance is a prime consideration. In general, complex systems are less reliable than simple systems. Thus the more components there are in a system, the more likely it is that the system will have lower reliability.

This is also true of components added to increase safety. The added components may increase safety but will decrease system reliability. This means that a trade-off must be made.

From the systems safety viewpoint an especially important type of fix for a probable or reasonably probable failure is redundancy. This refers to component duplication, that is, having two components in the system to perform the same function so that failure of one of the two will not interrupt the function of the system. A common term for this arrangement is having a "back-up" component.

In order to maximize both safety and reliability without impairing either, redundant components should be held to two for a single function. The actual component with one back-up component provides the best trade-off. Additional back-up components may improve the level of safety somewhat but by increasing the complexity of the system they will reduce the reliability of the system to perform its task properly.

Similar considerations apply to the other methods of fixing hazardous situations.

They should be built into the system in such a way as to increase safety without impairing task performance.

Cost factors

The cost of fixing a hazardous situation and the effectiveness of the particular technique used to fix it should be evaluated. These elements may be added to the FM & E form as additional columns. A more elaborate modification would be to compute: 1) the cost of a particular failure, 2) the estimated reduction in the failure frequency for that component after fixing the situation, 3) the cost of fixing the hazardous situation, and 4) the net saving for the life of the system.

The details of cost-effectiveness analysis will be covered in a future article, but it should be noted here that such items can and are being used today in various ways in FM & E analysis.

FM & E limitations

Failure mode and effect analysis has some limitations that should be made explicit. In most instances one component is examined at a time, whereas it often happens that malfunctions of two components at the same time can result in far more serious consequences than each component failing separately. There is no restriction on the number of components that can be considered simultaneously except that the number of combinations quickly becomes prohibitively large. This also applies to very complex systems with very large numbers of components — even examining them one at a time can be enormously time-consuming. In both cases it is possible to overlook some possibilities that should be considered.

On the other hand, failure mode and effect analysis has the advantage

Sample FM&E Form

This partial analysis of a home hot water system illustrates the typical format taken by failure mode and effect systems analysis.

COMPONENT	FAILURE OR ERROR MODE	EFFECTS ON		HAZARD CLASS.				FAILURE FREQUENCY	DETECTION METHODS	COMPENSATING PROVISIONS AND REMARKS
		OTHER COMPONENTS	WHOLE SYSTEM	1	2	3	4			
Pressure relief valve	Jammed open	Increased operation of temperature sensing, controller, and gas flow due to hot water loss	Loss of hot water, greater cold water input, and greater gas consumption	x				Reasonably probable	Observe at pressure-relief valve	Shut off water supply, reseat or replace relief valve
	Jammed closed	None	None	x				Probable	Manual testing	Unless combined w/other component failure, this failure has no consequence
Gas valve	Jammed open	Burner continues to operate. Pressure-relief valve opens	Water temperature and pressure increase. Water→steam			x		Reasonably probable	Water at faucet too hot. Pressure-relief valve open (observation)	Open hot water faucet to relieve pressure. Shut off gas supply. Pressure-relief valve compensates
	Jammed closed	Burner ceases to operate	System fails to produce hot water	x				Remote	Observe at output (water temperature too low)	
Temperature measuring and comparing device	Fails to react to temperature rise above preset level	Controller, gas valve, burner continue to function "on." Pressure-relief valve opens	Water temperature too high. Water→steam			x		Remote	Observe at output (faucet)	Pressure-relief valve compensates. Open hot water faucet to relieve pressure. Shut off gas supply
	Fails to react to temperature drop below preset level	Controller, gas valve, burner continue to function "off"	Water temperature too low	x				Remote	Observe at output (faucet)	
Flue	Blocked	Incomplete combustion at burner	Inefficiency. Production of toxic gasses				x	Remote	Possibly smell products of incomplete combustion	No compensation built in. Shut down system
Pressure-relief valve & gas valve	Jammed closed Jammed open	Burner continues to operate, pressure increases	Increased pressure cannot bleed at relief valve. Water→steam. If pressure cannot back up cold water inlet, system may rupture violently				x	Probable + reasonably probable = reasonably probable	Manual testing of relief valve. Observe water output (temperature too high)	Open hot water faucet. Shut off gas supply. Pressure might be able to back up into cold water supply, providing pressure in supply is not greater than failure pressure of system

of being quite simple to use and provides an orderly examination of hazardous situations in a system. It forces the safetyman to ask new questions, to obtain new information, and most important, it focuses his attention on the really critical weaknesses in the system that require action. On the whole, the advantages far outweigh the disadvantages and it is evident that FM & E analysis can reduce the safetyman's failures and increase his effectiveness.

Systems Safety Analysis: The Fault Tree

Of all the methods for conducting systems safety analysis, perhaps the most promising is the fault tree. Like other methods, it can be a useful tool even without mathematics

By J. L. RECHT
Assistant Manager, NSC
Statistics Division

IN OUR second article on systems safety analysis one of the four principal methods of analysis—failure mode and effect—was discussed in some detail. In this article a second analytical method — the fault tree—will be described.

Although the fault tree method of analysis is only four years old, it has already been successfully applied to some very knotty safety problems in the aerospace field. Its success has gained it acceptance not only within the aerospace industry, but also by the Department of Defense, which has made fault tree analysis a requirement in its contracts for design of new missiles and aircraft.

At the present time fault tree analysis is being used exclusively for product safety — safety of missiles, aircraft, and automobiles. The technique is used by the design engineers in the design stages of these products.

Potential for safetymen

Although it is a new technique, it seems to have great potential for application in a much wider area. The safety engineer (possibly with an assist from his own product engineers) can certainly find uses for this analytical method not only with respect to existing systems in his plant but also for setting specifications on new or replacement equipment.

Fault tree analysis was first conceived in 1962 by H. A. Watson of Bell Telephone Laboratories in connection with an Air Force contract for study of the Minuteman launch-control system. Further development and refinement of the technique resulted from the combined efforts of the study team, which included A. B. Mearns. The problem of determining the likelihood of an inadvertent launch of a missile was successfully solved. The Boeing Company later modified the fault tree technique so that simulation with high-speed computers was possible. D. F. Haasl, R. J. Schroder, W. R. Jackson, and others contributed to this important development.

Because of this rapid growth in sophistication, it is possible to consider fault tree analysis on three different levels of complexity:

1. Simply draw a fault tree and examine it without performing any calculations;
2. Draw a fault tree and perform the calculations with a desk calculator or slide rule;
3. Draw a fault tree and devise a computer program for performing the calculations.

In this article the first two levels will be discussed and the requirements for the third level will be indicated.

What is fault tree analysis? According to A. B. Mearns, the first fault tree analysis was made to study *unlikely* events in complex systems. This view can be expanded: a fault tree can be constructed for *any* event that can occur in a system. It is important to remember, however, that only one event is analyzed in a single fault tree.

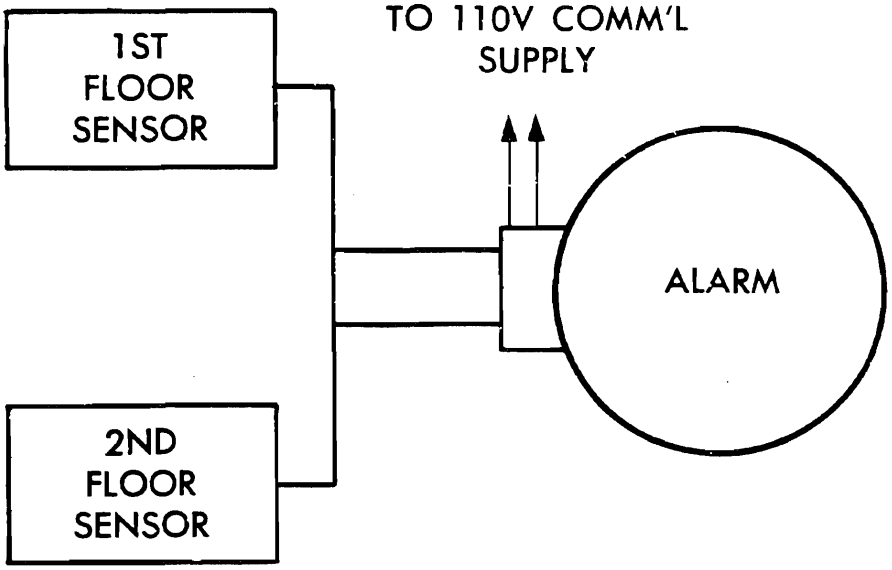
To do a fault tree analysis, first an undesired event of sufficient importance is selected—this could be a catastrophic event (such as inadvertent launch of a missile) or an undesired event of smaller magnitude (such as failure of a power press interlocked guard). Next it is necessary to reason backwards from this event to visualize all the ways in which it could occur. These "causes" or contributing factors are in turn broken down into the events which lead to them, and so on. The events are diagrammed in the form of a tree with the undesired event at the top. The branches are continued until either "independent" events are reached or there is little reason to continue due to lack of information or insignificance of the contribution of additional breakdowns. An "independent" event would be one which does not depend upon other components in the system for its occurrence.

Making the tree

A fault tree is really a logic diagram that traces all the events and combinations of events that can lead to the undesired event. For uniform representation of these events certain symbols are required.

One group of symbols, called "gates," indicates whether a single event or a combination is required to produce the next event higher up the tree. They also may indicate whether or not limiting conditions

A Sample Home Fire Alarm System



are involved, such as one event happening before another when both are required to pass through a gate. Other symbols are needed for the events themselves to indicate whether they are "normal," "independent," or "insignificant."

The real strength of the fault tree symbolism lies in the fact that the symbols can readily be translated into algebraic terms so that the tree can be simplified. It can be mathematically reduced, so to speak, to its bare bones. All duplications can be eliminated and the most important independent events identified. If the frequency of occurrence (or probabilities) of the independent events is known or can be approximated, then the relative importance of the various independent events in producing the undesired event can be calculated.

A sample tree

For the purpose of illustrating the fault tree method of analysis we will use a home fire alarm system. As shown in the diagram there are sensing devices on the first and second floors with wires connected to the alarm, which is powered by the ordinary 110-volt commercial power supply. The undesired event selected for analysis is "a fire with no alarm."

Examining the tree, it is seen that the undesired event can come about if there is a fire on the first floor with no alarm given OR a fire on the second floor with no alarm.

A fire on the first floor with no alarm involves having a fire on the first floor AND having the alarm unable to respond to the fire. (There is also an added condition that the alarm fails prior to the fire.) The alarm can fail to respond if the first floor sensing device fails OR the alarm is inoperative. The fire alarm will become inoperative if either the alarm itself fails OR there is no power to the alarm system OR the sensing lines fail. There will be no power if the power line fails OR the commercial power is cut off at the source.

Similarly the branch involving a fire on the second floor can be traced. The transfer symbol shown under "fire alarm inoperative" indicates that corresponding elements in the first floor branch should be repeated beginning with the transfer symbol.

This represents the simplest level of fault tree analysis—drawing the tree and examining it. Since it requires precise and detailed knowledge of a system to draw a fault tree, completing the tree forces the analyst to learn more about the system.

For a complex system it is often necessary to assign various branches of a tree to specialists in order to be sure that the event sequences are correctly portrayed.

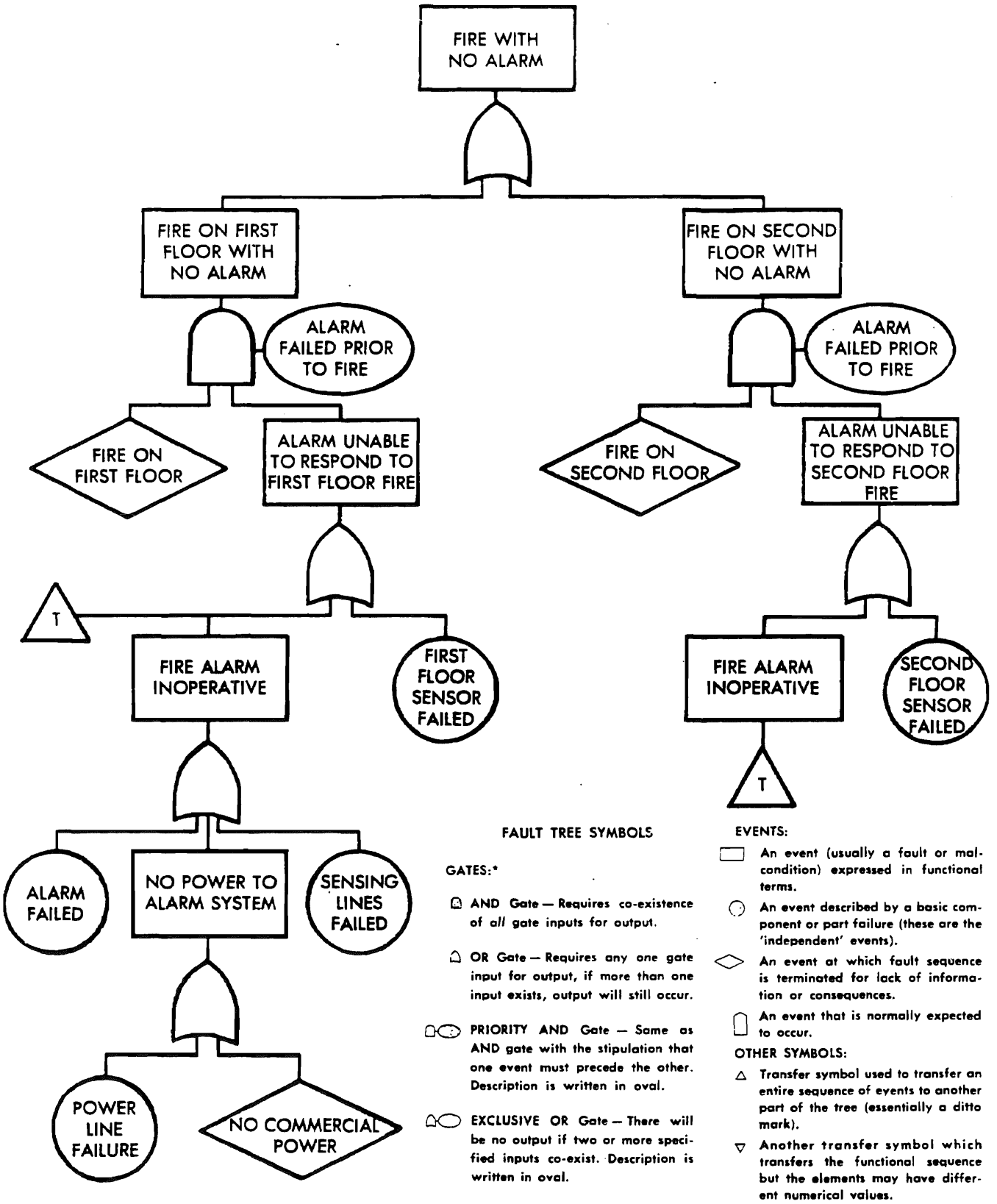
There are important benefits to be gained from learning precisely what can go wrong and how this will affect the system. The analyst gains new insight and sees new possibilities; he can see what new data is needed for prevention purposes; and he will come up with better answers because they will be based on examination of the whole system rather than a single component.

Introducing calculations*

The second level of complexity in fault tree analysis involves calculation. What is needed are the frequency of occurrence figures for the events symbolized with circles. These frequency numbers are usually MTBF figures, that is, "mean time between failures," and they apply to the separate components. The sources for these numbers are varied—accident experience, test results from component manufacturers, comparisons with similar equip-

*This description of the calculations involved in fault tree analysis is intended only as a glimpse of the procedures. Readers who want to pursue the mathematics further can consult: *Fault Tree Analysis: The Study of Unlikely Events in Complex Systems*, by A. B. Mearns, Bell Telephone Laboratories, Inc., Whippany, N. J.; *The Application of Fault Tree Analysis to Dynamic Systems*, by R. J. Feutz and T. A. Waldeck, Boeing Co., Seattle; *Advanced Concepts in Fault Tree Analysis*, by D. F. Haasl, also at Boeing Co.

Fault Tree Analysis of the Home Fire Alarm System



FAULT TREE SYMBOLS

GATES:*

AND Gate — Requires co-existence 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.

EXCLUSIVE OR Gate — There will be no output if two or more specified inputs co-exist. 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 rectangle.

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.

An event that is normally expected to occur.

OTHER SYMBOLS:

Transfer symbol used to transfer an entire sequence of events to another part of the tree (essentially a ditto mark).

Another transfer symbol which transfers the functional sequence but the elements may have different numerical values.

*NOTE: Inputs always enter gate at bottom and output always occurs at top of gate so that any event sequence moves upward from the ends of the branches toward the top of the tree.

ment, engineering data, judgment, and so on.

Next the fault tree should be converted into algebraic terms using Boolean algebra. Boolean algebra sounds strange and possibly difficult until you realize that it is understood by any 7th or 8th grader who has studied the "new math" now taught in grade schools. They learn the algebra of sets, which is a form of Boolean algebra. Actually all that is needed are about ten simple rules that can be learned thoroughly in a couple of hours.

The AND relationships in the tree are represented by multiplication signs and the OR relationships are represented by plus signs. Starting at the top of the fault tree each of the events is written in algebraic form step by step until the entire tree has been expressed in terms of the "independent" events (those symbolized with circles or diamonds). The terms of this long algebraic expression can be greatly simplified using the Boolean rules. The MTBF figures or estimates of frequency of occurrence can then be substituted in this simplified expression and the relative importance of the various terms evaluated.

Typically it will be found that some event sequences are thousands of times more likely to induce the undesired event than other event sequences. Thus it is relatively easy to find the chief combinations of events that must be prevented to reduce the likelihood of the undesired event happening — even when the MTBF figures are not completely accurate.

The calculations enable the analyst to determine the over-all likelihood of the undesired event, the combination of events most likely to lead to it, the single event that contributes most to this combination, the most likely paths through the tree to the top, and many other relationships. In addition, if the system is modified in any way, the fault tree can be changed to reflect the modification and new calculations performed to determine the effect of the innovation. In fact, numerous modifications can be made and the effects of all of them can be simultaneously evaluated.

In its original form the fault tree was confined to faults or malfunctions of equipment. But there is no need to restrict the method in this manner. With sufficient information on human error frequencies, human as well as mechanical malfunctions can be included in the fault tree.

Computer simulation

It is clear that the fault tree method is a powerful and efficient technique for systems safety analysis. It is limited primarily by the skill of the analyst and the availability of the basic numbers needed to indicate frequencies of certain events. However, if the system being analyzed is quite complex, the calculations can be tedious and the lack of failure frequency data can become serious handicaps. To overcome both of these problems, Boeing Company has developed ways of simulating fault trees on high speed computers.

Briefly stated, this computer method requires that the fault tree be constructed as usual. Then either the MTBF figures or figures obtained by sophisticated sampling techniques applied to the frequency distributions for primary faults are used to designate time intervals in the life of the system during which a particular fault will occur. Coexisting faults will form event sequences that will ascend the tree and in some cases will reach the top of the tree. These combinations are recorded and after sufficient computer runs, the same sorts of information about the events will be obtained as would be in the non-computer calculations.

The computer format has an additional advantage, however, in permitting a more realistic situation to be used by allowing for repairs to be made to correct some faults. In the life of any system repairs or maintenance activities are performed and this reduces the likelihood of specific undesired events happening. Introducing repair times into hand calculations offers no theoretical difficulties but it is much easier to incorporate in a computer program.

Systems Safety Analysis: Error Rates and Costs

By J. L. RECHT
Assistant Manager,
Statistics Division, NSC

PREVIOUS ARTICLES on systems safety analysis have described the development of the technique in the aerospace industries, and the potential uses it has for industrial safety engineers. Two of the four major methods used to accomplish systems safety analyses—the failure mode and effect analysis and fault tree analysis—have been described.

In this concluding article, the remaining two primary techniques will be covered: 1) THERP (technique for human error rate prediction) and 2) cost effectiveness.

Also included is a brief bibliography of some primary sources of information on systems safety analysis for those who wish to further investigate its possible uses in the industrial safety arena.

THERP

Both the failure mode and effect and the fault tree methods of systems analyses require that probabilities be established not only for the hardware, but for the human factors involved in system functioning.

The most useful method of deriving these probabilities is embodied in the technique for human error rate prediction developed by Sandia Corporation, and abbreviated THERP.

In discussing accident prevention many people refer to the "human element," and use this expression to indicate that human behavior is an unknown factor in any operation, and therefore unpredictable. This notion is only partly true, and recent careful examination of it by human factors experts has shown that there is much that is predictable in human behavior.

A single action or performance may be difficult or impossible to predict, but when an action or performance is repeated many times, there are numerous aspects that are predictable. For example, a person's bowling score for a single line might be difficult to predict and, if correctly forecast, would merely be a lucky guess. But for an entire season, a person's average bowling score can be predicted fairly accurately (given some prior information of his bowling skill). It is this idea of being able to predict results for repeated actions that underlies the current analysis of human factors in systems safety.

Human factors specialists have approached the problem of human error by using a "behavior" as the basic unit of evaluation. A "behavior" is considered to be a specific step or action in a given task. Each behavior is assumed to be analyzable into three prime aspects: 1) inputs or stimuli, 2) mediating or decision processes, and 3) outputs or responses. Examples of inputs are: dials or scales, labels, and spoken or written instructions. Mediating processes include identification, recognition, and manipulation. Outputs cover operating levers or switches, positioning objects, and giving oral or written responses.

THERP is a quantitative method for evaluating human error. It requires the use of a human error classification system and probability computations. The method of analysis was developed for reducing production defects due to human error in a manufacturing process. But with only slight modification this method is also applicable to human error sources of accidents and can thus be helpful to safety engineers in devising accident countermeasures.

The human error classification system developed by L. W. Rook Jr. as a part of the THERP method is shown in Fig. 1. The purpose of this error classification system is to provide categories suggestive of the corrective action or countermeasures to be taken. Rules for each category can be developed to help determine the needed countermeasures.

Minimizing human errors in a system can be accomplished by: 1)

Fig. 1. System of Human Error Categories

Error due to acts which are:	Errors due to behavior components of:		
	Input (I)	Mediation (M)	Output (O)
A—Intentionally performed	AI	AM	AO
B—Unintentionally performed	BI	BM	BO
C—Omitted	CI	CM	CO

Note: A—behavior that is properly a part of the task being performed; B—behavior that is not properly a part of the task being performed; C—behavior that should have been performed as a proper part of the task.

The final article in our series on systems safety analysis discusses two more analytical techniques—THERP and cost effectiveness

proper selection and training of personnel for the specific behaviors involved in the system, and 2) redesigning the system so as to improve inputs, simplify mediation processes, and insure accurate outputs. Careful classification of human errors will point to the specific action or remedy required to reduce future errors. For example, an AI type error (intentionally performed action with an input error) indicates that instructions are not clear or that a necessary indicator (scale, dial, or label) is difficult to read, inaccurate, or not understood. Once it is recognized that the error is of this type, it is usually a simple matter to correct the situation.

THERP also involves the concept of a basic error rate, that is, a human error rate that is relatively consistent between tasks requiring similar human performance elements (or behaviors) in different situations. The THERP method assesses the basic error rates in terms of their contributions to specific system failures.

Briefly stated, THERP analysis proceeds as follows: select the specific system failure (or undesired event) to be studied, identify all human operations (or behaviors) performed that affect the event and their associated basic error rates, and compute the probabilities that specific human errors will produce the system failure. The errors are classified in accordance with the error table (Fig. 2) and the system is altered, i.e., specific corrective actions are introduced. The basic error rates are adjusted by an amount that might be expected from the new procedure and the probabilities are recalculated.

The process is repeated until an acceptable level is obtained for the probability of the undesired event. In short, the system is changed on paper and the effects on human error rates due to corrective action are calculated until the analyst is satisfied that the particular failure is unlikely due to human error.

More elaborate methods are also available to determine by probability computations how critical specific human errors are for degradation of system performance. These techniques, however, also depend upon basic human error rates.

Basic human error rates are usually expressed in terms of the number of errors per million operations —based upon prior experience in similar situations. Some representative error rates are shown in Fig. 2 to illustrate the range and magnitude of such measurements. (Warning: this data should not be used for computational purposes without additional background information —specifically, under what conditions these rates can be expected to be valid and the probable error in each rate.)

Fig. 2. Representative Human Error Rates (Compiled from various sources)

Task Element			
Action	Object	Error	BER*
Observe	Chart	Inappropriate switch actuation	1128
Read	Gauge	Incorrectly read	5000
Read	Instructions	Procedural error	64500
Connect	Hose	Improperly connected	4700
Torque	Fluid lines	Incorrectly torqued	104
Tighten	Nuts, bolts	Not tightened	4800
Install	Nuts, bolts	Not installed	600
Install	O-ring	Improperly installed	66700
Solder	Connectors	Improper solder joint	6460
Assemble	Connector	Bent pins	1500
Assemble	Connectors	Omitted parts	1000
Close	Valve	Not closed properly	1800
Adjust	Mechanical linkage	Improper adjustment	16700
Install	Line orifice	Wrong size installed	5000
Machine	Valve port	Wrong size drilled and tapped	2083

*Basic error rate (errors per million operations).

Unfortunately the greatest restriction on the use of quantitative human error techniques is the lack of sufficient error rate data. However, now that the need for such data is known, human factors specialists are working to improve both the quantity and quality of these measurements. Refer to the bibliography for more detailed information on how to use these important figures.

Cost effectiveness

Cost effectiveness analysis is the

technique used to weigh system performance against dollars of cost. It can be applied to choosing one of several systems that might perform a given task or to evaluating various suggested changes in a single system. Since money is always limited, cost effectiveness analysis can be final in ruling out an otherwise desirable system or system modification if the gain in performance proves to be too small to justify the cost.

Cost effectiveness analysis, a way of measuring performance versus cost, helps the decision-maker to make better evaluations and therefore better decisions. However, this method should not be the only element in making decisions—the time required to modify the system or changes in personnel requirements may carry more weight than a modest difference in cost.

Determining the cost of a new system or system modification requires the use of the ordinary principles of cost accounting. A detailed list of the cost elements is compiled, the dollar value of each element is determined, and the total cost is cumulated. For systems analysis purposes, however, there are several additional considerations that should be carefully observed. Any cost comparisons of more than one system must be uniform, that is, the costs must be calculated on the same basis and insofar as possible use the same cost elements. Next, for most system modifications, only the "incremental" costs should be evaluated and compared. Incremental costs include only those additional costs directly due to the modification and exclude the costs that may be involved but would be incurred if no modification were made. Finally, it is important to include research and development, installation, *and* operating costs (including indirect items). The tendency is to concentrate on installation costs since they usually involve capital expenditures. But it may happen that the operating costs of the modified system are fairly high and thus this aspect should not be neglected in the analysis.

When cost effectiveness analysis is applied to accident reduction or prevention, the analyst needs detailed accident costs for the various degrees of severity and estimates of the probable reduction in accident occurrence that will result from the modified system. It is apparent to any safety engineer that accident reduction estimates are difficult to ascertain. But the use of the three methods of analysis described in these articles undoubtedly will contribute greatly to more accurate estimates in the near future.

It was pointed out in the first article that methods of systems safety analysis can be combined in a single analysis. Actually this is an ideal—a combined analysis method that embodies all the concepts and aspects of these separate techniques. But progress towards this ideal has already been made. G. A. Peters and F. S. Hall have shown (see bibliography) that it is possible to combine failure mode and effect analysis, THERP, and cost effectiveness analysis in a single "hazard analysis table." Similar advances using fault tree analysis are also possible.

Systems safety analysis is firmly established in the aerospace industry with systems safety departments and system safety engineers devoting full time to the application of the concepts and methods to product safety. There is ample reason to believe that these successful techniques can be equally useful to safety engineers in their field. It is hoped that the series of articles of which this is the last, will encourage safety engineers to study the methods in greater depth and apply them in their plant safety programs.

BIBLIOGRAPHY

1. *Advanced Concepts in Fault Tree Analysis.* D. F. Haasl. Paper presented to the System Safety Symposium, Seattle, June 8-9, 1965.

2. *The Application of Fault Tree Analysis to Dynamic Systems.* R. J. Feutz and T. A. Waldeck. Paper presented to the System Safety Symposium, Seattle, June 8-9, 1965.

3. "Design for Safety." George A. Peters and Frank S. Hall. *Product Engineering,* Sept. 13, 1965.

4. *Elimination of Potential Sources of Critical Human-Induced Failures in Space Systems.* T. A. McDonald, D. B. Parker, and E. W. Pickrel. Paper presented at the symposium and workshop on the Quantification of Human Performance, Albuquerque, N. M., August 1964.

5. *Human Engineering Guide to Equipment Design.* C. T. Morgan et al. McGraw-Hill Book Co., Inc., 1963.

6. *Human Error Quantification.* J. W. Altman, L. W. Rook, and A. D. Swain. Sandia Corp., reprint SCR-610, April 1963.

7. *An Index of Electronic Equipment Operability.* American Institute for Research, Data Store, AIR-C43-1/62-RP (1), Jan. 31, 1962.

8. "Method of Inadvertent Launch Analysis." Bell Telephone Laboratories, *Launch Control Safety Study,* Section VII, Vol. 1, Sept. 15, 1962.

9. "The Quantification of Safety." Herbert J. Kolodner. *Journal of the American Society of Safety Engineers,* March 1965.

10. *Reduction of Human Error in Industrial Production.* Sandia Corp. Technical Memorandum SCTM 93-62(14), June 1962.

Reprinted from National Safety News

National Safety Council, 425 N. Michigan Ave., Chicago, Ill. 60611

M66609 Printed in U.S.A. 111.17-12

SYSTEM SAFETY

and

INDUSTRIAL MANAGEMENT

National Safety Council
Chicago, Illinois

July, 1968.

ACKNOWLEDGEMENTS

The National Safety Council gratefully acknowledges the contributions made to this monograph by Charles O. Miller, Institute of Aerospace Safety and Management, University of Southern California, Los Angeles.

The monograph was prepared by Robert Currie, Assistant to the General Manager, National Safety Council.

TABLE OF CONTENTS

FOREWORD

The background of this document is not unlike that of the field it attempts to describe. It came into being, not because of some preplanned effort to produce a definable result; but rather as a synthesis of thoughts that are germane to system safety.

It is what it is -- a discussion of the role of system safety in industrial management. The ideas in this document are not unique, but are taken from those experienced in system safety -- namely the aerospace industry and in particular, the U.S. Air Force Systems Command. Its text and references should be of value to safety practitioners, managers of industrial systems, and students of either discipline.

CHAPTER I

INTRODUCTION

The Basic Challenge

Products produced by industry must be designed for consumer protection and the products produced by industry for industry must be designed for operator protection. Of the many social doctrines developed during the administration of President Johnson, consumer protection is one of the most dramatic. It has -- and will have -- a profound effect on the people and profession of design engineering and system safety.

Congress, the courts, and many consumer-oriented agencies are involved in this swelling campaign on behalf of the consumer. Their sentiments are rapidly being translated into action by legislation and legal precedent.

Two key words -- safety and reliability -- are being repeated over and over again. The issues involved: product liability, guarantees and warranties -- and the staggering costs that may accompany them. Expensive litigation, based on stringent products liability law, is an equally vital factor.

To you involved in safety, these are important, highly volatile issues. They will have an increasing effect on the products produced by your company and may determine the success or failure of your company.

Products liability represents a rich legal arena that attracts lawyers just like California drew the '49ers. And the similarity doesn't end there. Many of the legal prospectors who mine the products liability lode are just as rough and tenacious as the old sourdoughs. A $200,000 judgment against a company is the vein of pure gold that many an aspiring plaintiff's counsel dreams of tapping.

Unlike the grizzled miner, the modern lawyer isn't operating alone in an un-charted wilderness. Plaintiffs' lawyers have a "trade association", just as every segment of industry does. Called the American Trial Lawyers Association, it has recently given seminars in every State of the Union on the subject of products liability.

In 1967, more than 100,000 products liability cases were introduced. A number of individual awards exceeded $100,000. Few companies, or the designers who work for them, can afford to gamble when the stakes are this high.

The real question is what can be done to prevent accidents and prevent them in an evermore efficient manner.

Hypothesis

It is hypothesized that safety has become an effective and an increasingly integral part of industrial management -- especially systems management. Yet this role is by no means complete nor is it fully recognized. Thus, problem areas faced by the industrial and product safety discipline are:

(1) Incomplete understanding of the meaning of safety in the systems environment.

(2) Organizational and philosophical conflicts between safety and other disciplines within the engineering and management hierarchy.

(3) Difficulties inherent in evaluation, i.e., measuring, effectiveness of accident prevention effort.

(4) Inefficiencies in communications flow pertaining to accident prevention.

The principal hypothesis is threaded throughout this document and is summarized in the last chapter. True to the doctrine of accident prevention, attention is paid to what occurred historically only to be more productive, i.e., prevent accidents more effectively in the future.

CHAPTER II

SAFETY AND SEMANTICS

The Problem Defined

A number of representative definitions of "safety" have been collected to show the extreme variability in general understanding of the term "safety". (30:3)* These are reproduced in Table 1. Subsequently, informal safety definition quizzes have been given to scores of students routinely upon their entry into safety courses at the Institute of Aerospace Safety and Management of the University of Southern California. Each time, the result was the same -- the variability of student response was equal to that apparent in Table 1.

It may be concluded that safety and semantics is a fundamental problem in the role of safety and management; indeed, in safety as related to any activity. It should not, however, be unexpected. Industrial innovation is dynamic. When this is coupled with the complexity and the explosion of industrial technology, it is obvious that definition of terms is of major significance.

Safety Defined

To man, safety -- or lack of it -- is a commodity experienced since his conception in life. To be sure, man lives in varying degrees of "freedom from danger", the dictionary meaning of the term. (3) But to the human variable in our society, safety is a very personal thing. It is ingrained in each individual's psychophysiological make-up so deeply that his life preservation behaviour is a constant contest between the conscious and subconscious mind.

To members of the enlightened industrial engineering and management complex, safety has evolved to further meaning, beyond the innate abstraction common to all men. To such people, safety denotes a characteristic of their product. It pertains to the physical and mission well being of the personnel involved in the development, test and operation of the product and the product itself. It applies also to the product's related equipment and facilities.

---

* Numbers in parenthesis represent references and detailed location of information if appropriate; in this case Reference 30, page 3.

Table 1

REPRESENTATIVE DEFINITIONS OF "SAFETY"

1. Freedom from hazard.

2. Freedom from those conditions which can cause injury/damage to personnel, equipment, or property.

3. Freedom from those man-machine-media interactions that result in:
   (a) Damage to the system
   (b) Degradation of mission success
   (c) Substantial time loss
   (d) Injury to personnel.

4. The protection of men and equipment from the hazards that exceed the normal risks within the operational requirements of a healthy community.

5. Maintaining efficiently, the physical and mechanical well-being of men and equipment to the degree acceptable within the operational requirements of a healthy community.

6. The elimination of preventable accidents.

7. Confidence of mind and reliance on equipment that is sustained only by active and aggressive pursuit of all paths to maximum proficiency without stint.

8. The situation which exists when humans involved in or affected by the operation of a system are relatively free from threats of death or injury being inflicted by such system.

9. The optimum degree of freedom from danger of hazard to life, health or property; or from the occurrence of undesired incidents or events in any element of the system's operations.

10. Action taken toward the prevention of loss in manpower, material and time during the system life.

11. A specialized form of overall reliability which involves actual or potential loss of life; or actual or potential loss of the system.

12. The professional way to do things.

13. Conservation of system capability.

To the practitioner of the industrial and product safety discipline, safety has still additional meaning. It entails common threads of a philosophy, including limits of the discipline, and specific tasks to be accomplished in the interests of accident prevention. Such limits and tasks are characteristic of one of management's basic principles - division of work.

Therefore, in the industrial and product safety field several commonly accepted precepts appear. These include:

(1) Relative freedom from danger: One may have a goal of zero accidents, but he may choose to function with a probability of something less desirable than zero accidents. The criteria for hazard acceptability are developed using factors present in any management decision process. There is no logic that precludes delineation of something as an objective so long as the methods to achieve that objective are subject to the compromises ever present in society.

(2) Men and equipment loss or damage: When one seeks or applies accident prevention measures, it becomes obvious that cases involving equipment loss or damage are perhaps as important as cases involving only injury to personnel. Fundamental categories in the safety process are hazards to equipment, tools and machines, operators, property in the environment, and contiguous personnel. Taken in their broad meaning, these terms cover all possible recipients of damage, both animate and inanimate.

(3) Mission oriented: There are pre-eminent jobs to do besides saving lives and equipment, whether it is a matter of national defense or producing a product. This is, however, the least recognized precept among non-professionals in safety. It conflicts with personal exposures to dangerous situations and does not necessarily agree with precepts followed by most safety practitioners in other areas, (e.g. automobile or industrial safety).

(4) Progressive activity: With either military or industrial endeavours, there is a business involved, and a business is a thing which must develop to exist in the future. If it is not healthy, i.e. progressive, it will be an ineffective cripple or not survive at all. This point is closely allied to (3) "mission oriented".

(5) Timeliness: Time is a dimension often forgotten. It becomes involved here in one's ability to communicate and act on information prior to its becoming a statistic in accident causation. This is the before-the-fact, the "first time safe" concept, accident prevention feature.

Thus it should be obvious that industrial and product safety goes well beyond safety for safety's sake in the personal or traditional sense of the word. Assembled into one sentence, the foregoing components have been merged into the following definition:

> 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.

"Conservation" denotes, in a highly descriptive manner, the relative freedom from the danger of loss or damage; and suggests the importance of mission attainment. "Within the (necessary) operational and economic requirements" further identifies mission orientation. The other parts of the sentence structure are taken directly from the precepts as stated.

In recent years, the terms system(s) safety and system safety engineering have been heard, but not well understood. This is a classic case where the principles related to a given subject have been generated and a philosophy developed by practitioners in the field, but it took development of a concept in a related discipline (in this case, systems management) to lend substance to the original thoughts. The concepts and influence of systems management on safety will be discussed later.

As an activity, system safety has been defined as "the integration of skills and resources specifically organized to achieve safety over the entire life cycle of a system".

As a condition, system safety has been defined as "the highest possible degree of safety within constraints of time, cost and operational effectiveness, attained through specific application of management, scientific and engineering criteria, techniques, and procedures throughout all phases of system life". (47:9)

Similarly, system safety engineering has been defined by the U.S. Air Force (USAF) as "the specific application of management, scientific and engineering criteria, principles and techniques throughout all aspects of system development, to assure optimum safety". (40:1) Note here the qualification of "system development" which would not cover the entire life cycle of a system. Also,

"engineering" in this sense is a far cry from the parochial meaning of the term as may be used in the engineering department of a university or in industry. It reflects USAF systems management terminology. It is shown here because the USAF has led the world in customer identification of system safety as a separate and important discipline.

Now the semantics exercise indeed becomes a morass of sticky inflections. For example, if system safety includes the entire life cycle, and system safety engineering covers only the conceptual, definition, and acquisition phases of system programming,* it follows that there is another part of the whole .... operational safety .... that is not included in system safety engineering. The above system safety engineering definition should be paraphrased to include system operational safety as "the specific application of supervision, maintenance and crew requirements, standards and skills throughout all aspects of system operation to assure optimum safety".

Since the current state-of-the-art confines system safety engineering to the conceptual, definition and acquisition phases of the system programming, it follows that something falls between the cracks between the acquisition phase and the operational phase. Even though optimal safety for the hardware has been incorporated in the first three phases of the system programming within the constraints of cost, schedule (time) and performance, other necessary safety inputs must be made if the system is to achieve optimal safety in the operational phase.

A breakdown occurs because the software (personnel skill and training requirements, maintenance requirements, facilities requirements, operational procedures, etc.) is either non-existent or is couched in the language of the designer. Since the language of the designer is quite different from those who will operate the system, we might expect failures to occur in the operational phase. This is particularly true in the more complex systems.

Another fine point in safety and semantics involves the use of the term system. The literature reveals many definitions of a system. Two of the more representative definitions are:

1. A group of things (man-machine-environment) which are related to one another in some dependent manner, so that collectively they represent a whole and accomplish a task.

---

* As differentiated from the total life cycle of a system which would include the operational phase.

2. An orderly arrangement of components that are interrelated and act and interact with one another to perform a task or function in a particular environment. (37)

Thus, the bounds of system safety application are best described in terms of input and outputs at any level in the total hierarchy of system description (i.e. systems, system, subsystem, assemblies, component, element, etc.).

This means system safety could be applicable to the environs of the president of a company or a line maintenance man; a vice-president for engineering or a draftsman at a third tier level. It follows, then, that principles of system safety are a process and should remain the same. Only the details of the particular task at hand determine the precise effort. They also have their functional meaning, as will be shown later.

Most management definitions show a close relation to that devised for system safety. For example, "Management .... the control, coordination, and direction of personnel and resources to effect a useful product or service". (12:325) The pattern is the same; using personnel, skills and resources to achieve something. But the "something" in the management sense in the industrial environment is a concrete product or service (hardware or software). The tasks of system safety are utilized to effect a "product" of accident prevention within the prescribed objective of management.

The useful product or service of system safety is accident prevention in a specialized technology sense. This is simply a further division of knowledge and application .... that brings up one further distinction about the safety discipline. It involves the relationship between science, engineering, and the professional approach to safety.

System safety today is not a science. The distinction between a scientist and an engineer is perhaps best described by the following quote:

> ".... a scientist differs from an engineer in that both, working from a given set of facts or data, apply logical analysis and hopefully reach conclusions; but the engineer proceeds to do something about it, and the scientist is inclined to put his information away in storage for some future use. To the extent that a scientist takes action, he is functioning as an engineer. And when an engineer fails to act, he is reverting to the role of a scientist." (22:1)

Certainly when one thinks of system safety as an act in preventing accidents, it would entail doing something. This argues for safety as a division of the engineering discipline.

But logical thinking, application of facts and lessons learned by experience, and a defined methodology including experimentation and analysis are by no means unique to the engineer. They are perhaps more descriptive of the acts of a professional regardless of his specific area of training.

Since the practitioners in the system safety field are truly inter-disciplinary; since there are specialized schools for safety education and training, as well as the hard "school" of experience that comes with every major accident; and since skills exercised to prevent accidents are primarily aimed at other than the safety man himself, it would seem system safety personnel should strive towards the professional concept as opposed to subgrouping within a particular field of learning.

One final thought is necessary to describe the scope and meaning of system safety in the industrial community. It involves the relation of system safety to older forms of accident prevention such as industrial safety, traffic or farm safety. In theory, system safety would be a parent discipline with subgroupings such as industrial, traffic, farm, etc. This may come to pass for, once again, the truly fundamental principles and techniques of accident prevention are not restricted by the system to which they are applied.

System safety is now virtually confined to aviation, missile, and space vehicle applications wherein accident prevention measures are aimed at the vehicles themselves, their immediate equipment and facilities, and the people who operate, maintain or service them. There is little reason to limit the system safety concept to the aerospace industry. The concepts are applicable to any industry, to any product produced by industry, or any of the other safety disciplines.

CHAPTER III

EVOLUTION OF SYSTEM SAFETY

Key Historical Events

The recognition of the need to take specific accident prevention measures in our society occurred first during the industrial revolution. In the United States the first organized safety movement took place when the National Safety Council was founded in 1913. The next milestone was laws governing the safety of explosives and did not appear until the post World War I era. (7:12)

A landmark paper in system safety principles was given by Amos L. Wood of the Boeing Company in 1946 at the Institute of Aeronautical Sciences (IAS). (51) Wood emphasized "continuous focus of safety in design", "advance analysis and post accident analysis", "safety work .... most effective when it is not fettered by administrative organizational pitfalls", "importance of incident or near accident reporting", "safety education programs", "accident preventive design minimize personnel errors", "statistical control of post accident analysis", and many more principles and techniques used in accident prevention today. Mr. Wood's paper is considered to be the first formal presentation about system safety.

Another landmark publication by William Stieglitz titled "Engineering for Safety" appeared in 1948. Stieglitz's views were far sighted relative to system safety as evidenced by a few quotations.

> "Safety must be designed and built into airplanes, just as are performance, stability and structural integrity. A safety group must be just as important a part of a manufacturer's organization as a stress, aerodynamics, or a weights group ...."
>
> "A safety program can be organized in numerous ways and there is probably no one best way."
>
> "Safety is a specialized subject just as are aerodynamics and structures. Every engineer cannot be expected to be thoroughly familiar with all developments in the field of safety any more than he can be expected to be an expert aerodynamicist."
>
> "The evaluation of safety work in positive terms is extremely difficult. When an accident does not occur, it is impossible to prove that some particular design feature prevented it."

Here, then, we see the professional approach to safety through the medium of technical society presentations.

Key events in the 1950's marked the accelerated understanding and growth of the system safety discipline. Widespread formal recognition of the specialty was not in evidence, especially in customer procurement areas, but major advances in safety relative to management occurred. For example:

1950 . . . USAF Directorate of Flight Safety Research (DFSR) was formed. This was followed by the establishment of safety centres by the Navy in 1955 and Army in 1957. Safety officers became an integral segment of military operational organizations throughout this period.

1951 . . . The USAF negotiated with a number of major aircraft manufacturers to have representatives of their engineering staffs serve with the DFSR on a temporary basis. (6:33) These later became permanent liaison positions for all USAF contractors.

1953 . . . Courses introduced at the University of Southern California to train aviation safety officers.

1953 . . . First Missile Safety Branch formed at DFSR.

1954 . . . Start of joint Air Force-Industry conferences sponsored by DFSR wherein safety considerations of various sub-systems would be considered by sub-system and safety specialists.

1954-5 . . First known use of the term "system safety" in a technical publication. Although numerous system safety principles were in evidence, the classification of prevention data was limited to sub-systems of aircraft. (24, 25)

1957 . . . First known paper relating flight safety engineering to reliability and effectiveness in weapon system design and operations. (26)

1958 . . . First quantitative system safety analysis effort; performed in connection with the Dyna-Soar, manned space glider. (4, 36) This was a critical analysis of mission accident potential and contained much of the safety "allotment of probability shares".

1958-9 . . Missile safety activities greatly enhanced by the Air Force with formation of the Missile Safety Division.

Entry into the 1960's for system safety discipline was highlighted by initiation of customer contract requirements for system safety effort. To be sure, the entire history of aviation has stressed means for life protection at least on a sub-system or component basis. However, a by-product of the

transition into the space age was the system-wide approach to safety through contract requirements.

A new order of magnitude in man-vehicle hazard prevention was required because of the unique emergency, rescue, and survival problems attendant to the X-20 mission. (14:2) This generated a "Fire Prevention and Safety Section of the Dyna-Soar (Project) Engineering Office" at Wright-Patterson Air Force Base and comparable activity at the prime contractor's facility (the Boeing Company). In July 1960, a System Safety Office was established at the United States Air Force Missile Division for the Dyna-Soar system development as well as for many other unmanned systems. (41:1) Obviously, the qualitative and quantitative safety requirements established during the entire Dyna-Soar program were milestone events in safety related to management.

Progress accelerated when in June 1962 the Ballistic Systems Division (BSD) of the USAF released BSD Exhibit 62.41, "System Safety Engineering: Military Specification for the development of Air Force Ballistic Missiles." (41:3) This was, in effect, the first specification applicable on a systems wide basis in the interest of safety although it was confined to ballistic missile systems.

The soundness of the 62-41 document is illustrated by the fact it became the pattern for the military specification applied to all types of Air Force systems. (13) MIL-S-38130 (USAF) covering missiles and aircraft was released in September 1963, entitled "General Requirements for Safety Engineering of Systems and Equipment". (45) MIL-S-58077 (MO) was released by the U.S. Army in June 1964 entitled "Safety Engineering of Aircraft Systems, Associated Subsystems, and Equipment; General Requirements for". (48)

The Navy adoption of the system safety principle hit a snag. The Navy had become so completely system effectiveness oriented that they were reluctant to encourage any separate specification for safety. They preferred to wait for a broader program which would encompass safety, relaibility, maintainability, and other similar requirements under one heading. (49)

The 1964-65 time period continued to see more significant developments in safety relative to management. The Air Force System Command (AFSC) continued USAF leadership in system safety by establishing a task force to accomplish two projects: (a) Prepare a System Safety Management Manual to be used by Air Force System Project Officers, (b) Revise MIL-S-38130 and other appropriate regulations relative to system safety. A third closely related project was

undertaken at the Systems Engineering Group of AFSC, namely to prepare the comprehensive safety criteria handbook.

Late in 1965, the Department of Defense (DOD) instituted development of an interservice system safety specification. This achieved Army-Navy-Air Force approval in March 1966, was circulated to industry shortly thereafter, and was released as MIL-S-38130A in 1966.

While this safety requirements activity was underway, the 1960-65 period also saw the introduction of system safety papers on a large scale by numerous technical societies such as the American Institute of Aeronautics and Astronautics (AIAA), the Society of Automotive Engineers (SAE), and the American Society of Mechanical Engineers (ASME). A system Safety Symposium was conducted in Seattle co-sponsored by the Boeing Company and the University of Washington in June 1965. Also, an Aerospace System Safety Society was formed in the Los Angeles area in late 1963, and quickly expanded to all parts of the country. Its purpose is to:

"1. Facilitate the interchange of ideas and information among management and engineering personnel who have an interest in the area of System Safety.

2. Encourage the further recognition of System Safety as a management and technical responsibility in the development of aerospace systems.

3. Promote the principles and techniques of System Safety as a valuable tool in system development efforts outside the aerospace industry.

4. Promote professionalism and recognition of professionalism among persons working in the System Safety area". (17:1)

One final chronological note involves the educational process for system safety. In 1964, the Aerospace Safety Division of the University of Southern California began conducting a masters degree program in Aerospace Operations Management for the USAF in Europe. This program had as it origin the same interdisciplinary approach used for safety officer training and intensive course work (ten weeks and two weeks duration respectively) conducted since 1953. (12:326) Then, starting in the Spring of 1966, a specific set of System Safety graduate courses were initiated to provide a system safety area of emphasis within this aerospace management graduate program. Also, a short course had been initiated in system safety analysis at the University of Washington in 1965, and can be expected to be repeated periodically.

The Known Precedent Concept

No discussion of the evolution of system safety would be complete without reference to a principle referred to as the "known precedent" concept. It is important because it ties together the history of accidents with the evolution of accident prevention effort. It can be explained as follows:

> "The known precedent is the basis for recognizing accident cause factors and potentials, in that once a factor has been demonstrated as being capable of accident causation, it can be expected to recur with a given frequency and in much the same manner as errors tend to perpetuate themselves .... A .... cause factor, like history, tends to repeat itself." (15:4)

The known precedent concept has permitted growth of system safety on one hand, yet it provides a tremendous challenge on the other. As more and more accidents occur, the resultant data reflected as prevention information becomes immense. Therefore, as part of the total expanding industrial technology, specialists are required in safety to keep abreast of information developments.

As observed numerous times in tracing the literature pertaining to what is now known as system safety, countless examples were observed regarding people not being familiar with what was accomplished, written or spoken earlier. This was particularly true of many of the missile safety personnel, some of whom still feel system safety work started in 1962. This is not a criticism of them any more than it is a criticism of all safety personnel to date who have not purposefully chosen to document their ideas and made them available to the industrial community at large. This is a requirement of the known precedent concept.

CHAPTER IV

SAFETY RELATED TO MANAGEMENT

Whither Management

In industry, there are managers and safety specialists of one form or another. In both cases they represent a relationship that has evolved within recent times. The dynamics related thereto, however, have not been influenced solely by a maturing approach to accident prevention by safety specialists. It is also true that management, as its own art and science, has certainly not been static. Thus, before further relating safety to management, it is necessary to note certain past developments and current trends in management. The following are fundamental to understanding safety's role in the broad management structure.

1. The exploding technology .... This is perhaps most acute in industry. Technological information is doubling every five years. It has produced not only almost unbelievable complexities of tasks, but also has required expenditure of great personal energies as well as high dollar costs. This has required that the line managers, the decision makers, solicit technical assistance from outside their classic chain of command.

The "doers", the line function people, simply do not have the mental capacity and/or the time to acquire and assimilate all the available knowledge that can be used to optimize their actions. The result has been increased specialization and the so-called matrix organizations, or staff activities which go well beyond the traditional advisory nature of staff work. (21) Management people are relying more on the specialist to watch a given discipline for them, e.g., system safety people to provide for safety inputs into the system.

2. The behavioural approach to resource management .... Today, one might chuckle over the manager in the old days who placed an order on the bulletin board which read:

"By Order of the Management:
There will be no more
accidents".

However, analysis of the management discipline will reveal the human side of enterprise has been accepted only relatively recently as a more effective

avenue towards goal accomplishment. (20:77) Authoritative directives such as the above were quite serious in their intent, and perhaps even more effective in the culture of the time than one might suspect by today's standards. The point here is that today, effective management is accomplished by people through people more than ever before. This carries with it the requirement for more "selling" of ideas, more interactions and participation on a person to person basis. This is especially so if those ideas are relatively new and appear to encroach upon some pre-established "sacred cow" function within the organization. Remember that functions are identified with people in the real world.

3. The rise of system management .... Two main points about system management have vitally affected safety efforts.

(a) The entirety of the life cycle approach: Table 2 discloses the items considered as part of a system for management purposes. (46:1) It means that when someone or an industrial firm buys or contracts for a "system", they will buy a single package of hardware plus software to achieve optimum system performance. Prior to the system management, these elements were approached on a piecemeal basis both in contract administration and technical effort.

(b) Centralized visibility and control: Fundamental to the system management concept is a centralized program office and various reference baselines for relatively rigid management control. These are applied by both the buyer and seller throughout the entire contract spectrum. This means that requirements are established very early in the process (conceptual and definition phases). Funds are rarely made available for items not planned or established as part of some system baseline.

4. The system effectiveness concept .... This was mentioned briefly earlier. It is of such importance, however, that it merits full discussion as a separate topic including a more detailed return into history to understand its meaning.

System Effectiveness

During the late 1950's and early 1960's it became quite obvious that air vehicle systems were being delivered that were not reliable in the broad sense of the term. A system may have had its advertised performance if it

TABLE 2

ELEMENTS INCLUDED IN A SYSTEMS CONCEPT

- Prime mission equipment (e.g., the machines)
- Equipment for training
- Checkout, test, and maintenance equipment
- Facilities required to operate and maintain the equipment
- Selection and training of personnel
- Operational and maintenance procedures
- Instrumentation and data reduction for test and evaluation
- Special activation (test) and acceptance programs
- Product support for all aspects of the system
- Computer programs pertaining to system functions

could ever be put in the air. Component unreliability, poor maintainability, hazardous flight characteristics, incompatibility with personnel available for the task were but a few of the problems experienced. All of these resulted in program slippages and huge cost overruns for required "fixes". (34) By the time the system was "shaken down", the original operational requirements may well have been outmoded. In other words, the complex system had arrived, but advances in system management had not.

System effectiveness then became a term that tried to describe what the customer found missing in their system. It took two forms when finally defined. First, the general approach which would look something like:

> "The ability of a system to do the job for which it is intended". (2:I-1)

Then there is the specific approach which follows the current trend to attempt to quantify everything in the management process.

> "The PROBABILITY that a system can successfully meet an operational demand within a given time when operated under specified conditions". (2:I-1)

System effectiveness can be clarified by stating, "It is a function of availability, dependability, and capability". Availability answers the question, "Can I get it on demand?" Having it available, dependability answers the question, "Will it work right?" And finally, having it dependable, capability answers the question, "Will it carry out the mission I want it to carry out?"

Other technical areas which contribute to system effectiveness are:

- Reliability
- Maintainability
- Quality
- Operability
- Safety
- Compatibility
- Design Simplicity
- Human Factors

The above "ilities" must be recognized in the policy statement reference framework in which they were given. They are criteria or items that a customer wants within constraints of the three prime tools of management; namely, cost, schedule, and performance. A company must be alert for new operating concepts to achieve more emphasis on and integration with the criteria emphasized by the customer.

Therefore, besides the traditional disciplines which bear on system effectiveness, such as the basic design skills, various organization/people

complexes have evolved and have become identified in the following categories:

- Human Factors
- Product Support
- Maintainability
- Quality Assurance
- Reliability
- Systems Engineering
- System Safety
- Value Engineering

If the "wants" listed earlier could be referred to as the "ilities", then these responses by industry would be called "ility disciplines". Note, especially, that system safety as it pertains to the industry environment is listed as one of the "ility" disciplines.

There is no doubt that considerable confusion (bordering on antagonism) exists in the minds of some managers over these "ility" disciplines. The fact remains, however, the "ilities" have evolved because of a deficiency in previous methods of management which failed to provide adequate system effectiveness in the broad sense. (38)

There are many common features among the "ilities".

- They all base their work on some similar, if not identical system, subsystem, component classification hierarchy when approaching the analysis task surrounding a given system.
- They all use analytical techniques involving statistical probability and evaluation methods.
- Interdisciplinary approaches are the required rules rather than the exception if full effectiveness of the discipline is to be realized.
- All must place close reliance upon task analysis to identify the human element in the system.
- Reports of system performance (or lack thereof) by data feedback are essential for upgrading not only the system involved but also the discipline itself. Much of this feedback data is from common sources.
- They all aim at a form of technical direction by providing information and operational guidelines to design.
- They all take the unbiased and independent look at design through design review and other reviews (drawings, test procedures, test plans, specification, and supplier documentations).
- They all must develop overall program plans that must be implemented during the entire product cycle. (23)

It is the marked differences between the "ility" disciplines, however, that provide insight to how they each, individually and collectively, contribute to system effectiveness. These differences consist of the viewpoint of the people involved; their particular background, training, and experience; and the information they generate and/or apply. These differences are examined in subsequent paragraphs. The principle viewpoints of the "ility" disciplines are shown in Table 3.

This does not mean elements of one area cannot exhibit interest in or share viewpoints which are similar to those of other activities. However, as practised today at the working level, the principal viewpoints of the disciplines shown are clearly evident. They are different from each other. They also logically represent principal technical capabilities which is really the important point. Unless all are applied to a high degree of professionalism, a less than optimized system effectiveness job will be accomplished.

As an illustration of this precept of different viewpoints, consider a failure mode effect analysis -- a process where attempts are made to outguess future problems based on experience from the past. Shown in Table 4 is an abbreviated outline approach to such an analysis. It contains many items (marked by the asterisk) which highlight the safety or accident prevention significance of the failure being considered.

Some of these items, e.g., "how to inspect...for an impending failure" have different meanings to different people. To the quality assurance man, this probably means how does he do it and to what standards. To the maintainability man, it probably means when does he do it and with what people/procedures. To the safety man, it would solicit the question as to whether the procedure is sufficient in recognition of an impending failure to prevent an accident (usually in combinations with other failures) or, is there a better way to be explored to effect prevention involving this failure?

This application of safety logic comes before the failure although chronologically in the design process it may be accomplished concurrently or after a preliminary failure mode and effect analysis is made. That is, the ability to detect an impending failure will considerably modify one's "judgment" in how to treat a given failure, and how to classify it as being either marginal or critical, or perhaps even catastrophic. To not intelligently ask all types of questions in a failure analysis is to go to perhaps one extreme or the other. It could result in being too safe, as well as being not safe enough.

TABLE 3

PRINCIPAL VIEWPOINTS OF THE "ILITY" DISCIPLINES

Human Factors . . . optimum matching of man and machine.

Product Support . . . material and personnel readiness.

Maintainability . . . the system can be worked on conveniently.

Quality Assurance . . . verification of product characteristics.

Reliability . . . minimum failure within predetermined goals.

Systems Engineering . . . Technical data integration.

System Safety . . . accident prevention.

Value Engineering . . . cost saving.

TABLE 4

TYPICAL ELEMENTS TO BE EXAMINED DURING

FAILURE ANALYSIS

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 and incorrect action by operator(s))*
- Of subsequent additional failures within same system*
- Interfaces/potential effects on other systems*

* Items emphasize the prevention viewpoint

This questioning viewpoint or attitude -- playing the WHI game (what happens if) -- is considered the prime ingredient of the accident prevention discipline. It applies in virtually every task assigned to the safety specialist.

The discussion of attitude leads logically to the next major difference between safety and the related system effectiveness disciplines. It involves the background, experience, and training of personnel being considered since it is difficult to isolate an attitude from a person's exposure to past events.

The accident prevention attitude (looking for potential failure) is not something one is born with; although, he soon learns how to practise it to one degree or another. It is something that is learned by the bitter lessons of experience, be it by a designer or an operator. It is learned by retrieving and studying pieces of wrecked equipment and/or people. It is learned by some specific safety educational process which attempts to short-cut the other methods time-wise, and accident-wise.

Contrast this with the background of the types of people used in the failure analysis illustration. The quality assurance man most likely spent most of his years as an inspector -- someone who judges adherence to well defined requirements. His contact with the human element is minimal from the standpoint of why an error is made. His educational process for advancement encompasses specialization areas in his field of verification of product characteristics, not accident prevention per se (e.g., non-destructive testing).

Similarly, the maintainability man can usually be recognized from the bruised knuckles he received trying to put a wrench on some hidden hydraulic fitting. He understands how to assign manpower or otherwise attend to malfunctioning equipment. Like the qualify assurance man, he may also be active in attempting to prevent individual malfunctions. However, his concern for malfunction prevention usually does not permit separation of the wheat from the chaff in the sense of spotlighting hazards. Again, maintenance including its required training is an involved, time consuming, and specialized process.

From the experience factor comes the third area of difference ... the safety information legacy. Though not organized as best as it could be, the body of specific accident prevention knowledge is immense. It is growing. Properly applied, it can prevent accidents. (30, 31, 44) This subject will be discussed more in Chapter V.

Organization for Safety

The four characteristics of industrial management evolution (exploding technology, humanized approach, the system management trend, and concern for system effectiveness) combined with safety's emerging role have produced challenges relative to organization for safety. For example, some people feel what safety purports to do is "just good management, I don't need a safety group", or "safety is the prime responsibility of every man, you can't give the job to someone else". There is also a tendency to fully equate safety to management because of the undeniable fact that a "job well done is inherently safe". These views represent extremes which, most often, reveal a lack of understanding of a fundamental precept about delegation of work. (1, 18, 43:2)

Where the confusion has arisen is in "responsibility" for safety. It is clear that the manager bears prime "responsibility" for accident prevention under his control; but no more so than a corporate president would have "responsibility" for fiscal solvency. When a manager delegates work to subordinates, he does not delegate his responsibility. He will assign duties, he grants authority, and he creates (not transfers) an obligation or accountability in the subordinate. He cannot abandon his own obligation. To do so would mean he would have tremendous influence and yet not be accountable for the results wherein the entire chain of command would deteriorate.

Misunderstanding arises because people indiscriminately confuse "responsibility" with both an assigned duty and an obligation created in a subordinate. (33:60) And it must be emphasized that an obligation (or accountability) simply can never be delegated. Thus, the creation of a safety position does not transfer management's responsibility for safety; it simply assigns certain duties, grants certain authorities, and creates more obligation for safety .... i.e., a further breakdown and emphasis of safety within the expanding technology.

An area for concern relative to safety organization within engineering, is a particularly difficult communication problem. System safety must introduce lessons of the past which have occurred in an operational environment and communicate them to non-operationally oriented people, the design engineers. Similarly, the output of engineers, either in publications or hardware, often has to be "translated" before it can be understood and/or applied in the field in a practical accident prevention manner.

Thus, the system safety man must be in a position, organizationally, to have direct access to communications between the engineering and the operational environments. Whether he is in an engineering department per se, a test organization, a field service group or other location is secondary to this vital requirement.

The Law - Safety Interface

Another facet of safety's relationship with management requiring understanding involves its legal aspects. An event of relatively recent origin, it stems from the sociological trends toward absolute liability relative to a product's performance. (27-29, 32, 39) That is, if person or property is injured/damaged, someone must pay. The legal principles involve both tort (negligence) law and those statutes and interpretations relative to warranties.

The problem from the safety point of view is that "objective/unprejudiced comment on accidents, incidents, or malfunctions (are) threatened by the prospect that information related thereto may be subpoenaed in courts of law". (27:174) From the general management point of view, it becomes not only a threat to an aggresive accident prevention program, but also a very serious economic consideration, because of the absolute part of the liability trend.

An aviation insurance executive indicated a 150 passenger jet airliner crash could readily incur damages amounting to over $40,000,000. (8:15) It takes little imagination and mathematics to realize the impact of just a few losses of this order of magnitude. Coincidentally, Life magazine reported the property damage during the infamous Watts riot to be $40,000,000. (11:34)

The total law/safety subject is far too involved to explore in depth in this study. Suffice to say here, the liaison between safety personnel, management, and the legal staff of any organization must be extensive. Any organization that cannot demonstrate -- in fact and in name -- the modern techniques of accident prevention, could indeed be vulnerable in liability litigation. (40:5)

CHAPTER V

ACCIDENT PREVENTION TASKS

Framework for Application

The traditional approach to accident prevention has been the three E's -- Engineering, Education and Enforcement. Some have added "Environment" and "Example". All of these factors are recognizable when considered as the results of a decision process facing management. Assume an accident occurs. Now a decision must be made regarding what should be done to preclude its happening again. Assuming a machine is involved, one can engineer the machine differently or change the job procedure; the personnel who are involved can be retrained; certain rules or laws can be enforced (which is probably doing it the hard way); the environment contributing to the accident could be modified or avoided; and the manager can personally set an example in the safety attitude.

However, two vital ingredients have been lacking in these traditional approaches -- productive as they are. These absent items are the total life cycle system concept and management's delegation of additional obligation for safety to an accident prevention specialist. This means specific prevention tasks for some time-line framework.

In general, a product passes through the following phases -- by whatever name they are called:

1. Customer requirements
2. Conceptual design
3. Prototype development
4. Product design
5. Test and Qualification
6. Manufacturing
7. Use
8. Ultimate disposal

These are not necessarily sequential since they may well overlap. Also, depending upon the particular product, the life cycle could vary from days to decades. In any event, accident prevention inefficiency arose in the past because of the manner the E's were applied. They were applied only at various steps in the process without attention being paid to where the problem had been

or where it was going. This is tantamount to trying to conduct a business without a planning function. In general terms it results in depletion of personnel energies by continually "putting out fires" at the expense of the total basic job. In safety, it results in after the fact thinking rather than accident prevention.

It is necessary, therefore, to establish some framework in which the total safety job can be efficiently accomplished. In today's technology, this logically becomes some form of a system life cycle in which tasks would be planned, organized, staffed and controlled; i.e., managed. Implementation then involves a fundamental premise relative to system safety; one which is either accepted or rejected by management. The premise is that system safety is a necessary further breakdown of the increasingly complex technology facing management; and by assigning specific safety tasks to a safety specialist within the systems framework, more accident prevention (and better mission accomplishment) can be achieved than by previous management techniques.

The Safety Task Checklist

Prior to the advent of the system safety concept, there was little formalizing of safety tasks in the specialized sense. Hence, it was not surprising that management was reluctant to delegate work to a safety specialist. Unless a task can be clearly identified and shown to contribute productively towards a given objective as part of scientific management, it has no meaningful function.

System safety specification implies certain tasks to be performed in the name of safety. Common sense implies others. Listed below are fundamental system safety tasks that were derived empirically, but these have stood the test of time.

1. Establishment of accident prevention requirements as early as possible in system development, especially through inputs in system specifications. These would emanate from design safety checklists or other such sources gathered over the years from bitter experience. This would help eliminate faults carried from one system to the next.

2. Participation in hazard analyses emphasizing the before-the-fact symptom of failures as well as the effects of failures in the system including its human element. A strong argument can also be made for the final intersystem failure analysis integration and coordination task (integration of subsystems) being assigned to safety in view of the relatively broad background usually present in a well qualified safety personnel.

3. Determination of emergency procedures for those conditions where the equipment, personnel or surrounding property are endangered by improper performance of the system.

4. Participation in design mockup reviews. This usually occurs at specific points during system development where the numerous viewpoints of the "ilities" are brought together for objective discussion of the system in question. The unique contribution of safety personnel continues to be the what-happens-if approach described earlier. In the broad sense, this could be interpreted to include mission simulations conducted during development and test operations.

5. Maintenance of accident/safety information files pertinent to system development and operation. Such activity also requires close coordination with the organization's technical information centre to establish an adequate safety information storage and retrieval system. Due to the sensitive nature of some types of accident prevention information, it is essential to have a repository for such material outside the normal library.

6. Liaison with other people and safety organizations such as National Safety Council, American Society of Safety Engineers, Systems Safety Society, etc. The real payoff arising out of such liaison is not usually recognized until two or three years later.

7. Recommendations for and conduct of safety research, study, or testing in potential safety problem areas not fully resolved during scheduled system development.

8. Provision for safety education and training throughout all elements of system development and test. This would include programs oriented towards upgrading safety people themselves in their own technology as well as motivational type training for others in the development process.

9. Utilization of standards, safety inspections and surveys as prevention techniques where applicable.

10. Preparation of accident/incident investigation plans. This is another accident prevention technique to insure not only rapid and comprehensive information about any mishap, but also to keep safety in its proper perspectives in the emotionally charged environment following an accident. Future accident prevention efforts, as well as mission accomplishment, suffer from any inaccurate and/or premature actions taken under a condition marked by lack of investigation planning.

11. Participation in accident investigation. This is part of the essential information feedback loop. It follows that the people most involved with the specialized prevention efforts would be valuable additions to the accident investigation and analysis team. Since accident investigation requires a skill and technique, a properly qualified safety specialist should participate in the fact finding portion of the investigation.

12. Follow-up all action resulting from accident/incident investigations and maintain a record thereof. It may seem superfluous on the surface to cite this as a separate required safety task. Unfortunately, history has shown that normal follow-up procedures rarely accomplish the intended purpose within a reasonable time span between recommended action and accomplished fact.

13. Communication of accident prevention information through written material and by personal contact (face to face), not only with design engineers, but also with other personnel through briefings and safety conferences.

14. Provision for objective response to safety inquiry ... an area to which problems of a safety nature can be addressed. This especially includes the need for a place for people to present an anonymous report of an incident which would be too embarrassing to report otherwise. This might be called the "Chaplain" requirement in safety.

15. Development of a system safety plan and management thereof. The previously described tasks constitute work that must be collectively coordinated and implemented throughout the life cycle of the system.

These tasks would be presumably the assigned duties of a system safety function with the necessary delegated authority from management to carry them out successfully. Note the difficulty that would be experienced in attempting to classify these tasks collectively as either staff or line functions.

Note also that these tasks could be described in the safety engineering framework and mean one thing, or be described in the operational safety framework and mean something else. Yet, they are fundamental system safety activities in which accident prevention action principles can be recognized.

The concepts of system safety and the system safety checklist are much broader in scope than those encompassed by the traditional occupational safety engineer. Organizationally, the occupational safety engineer is frequently a segment of industrial relations. The system safety concept would suggest that the system safety function would assume an organizational position parallel with the other "ilities" involved in system effectiveness, such as reliability, quality assurance etc.

CHAPTER VI

COMMUNICATION OF SAFETY INFORMATION

Safety Information Flow

The flow of information is vital to the system management process. (16:73-88) It must, therefore, be considered vital to the accident prevention process. This can be best understood by recalling the known precedent concept described previously. Known precedent is the cumulative accident prevention knowledge provided by history. It has also been described in a very practical vein as learn from the mistakes of others since you might not live long enough to make them all yourself.

When viewed in a communicative safety information flow process, Figure 1., known precedent becomes a significant reference point. Initially it determines hardware safety characteristics and procedures for a given system under development. These characteristics and procedures are then refined, tested, and put into operation. Should they result in an accident free function, the assumption is justified that the known precedent and the application thereof was adequate.

In practice, however, accidents, mishaps, incidents, and hazards do occur from which prevention lessons are learned. They become part of a feedback loop which must be applied to the system in which the event occurred, and to the more generalized data bank of "known precedent".

Observed from the management point of view (see Figure 2), the safety information logic is quite similar to that shown in the previous figure. In the management framework, however, specific actions are suggested rather than merely mental observation of information flow characteristics. If adequate safety requirements are specified within constraints of cost, schedule and performance, and if other management steps are effectively taken through the implementation phase, then, theoretically, no safety problems will occur.

When the accidents, mishaps, incidents and hazards do occur, there is once again a feedback process to the management task. If circumstances (especially time) permit, the original requirements might be changed. Interim solutions might be necessary. Interim solutions are not permanent, but merely buy time and keep the system functioning until a permanent solution is found. In other cases, new solutions might be required. Finally, the case might reveal

FIGURE 1

COMMUNICATIVE SAFETY INFORMATION FLOW PROCESS

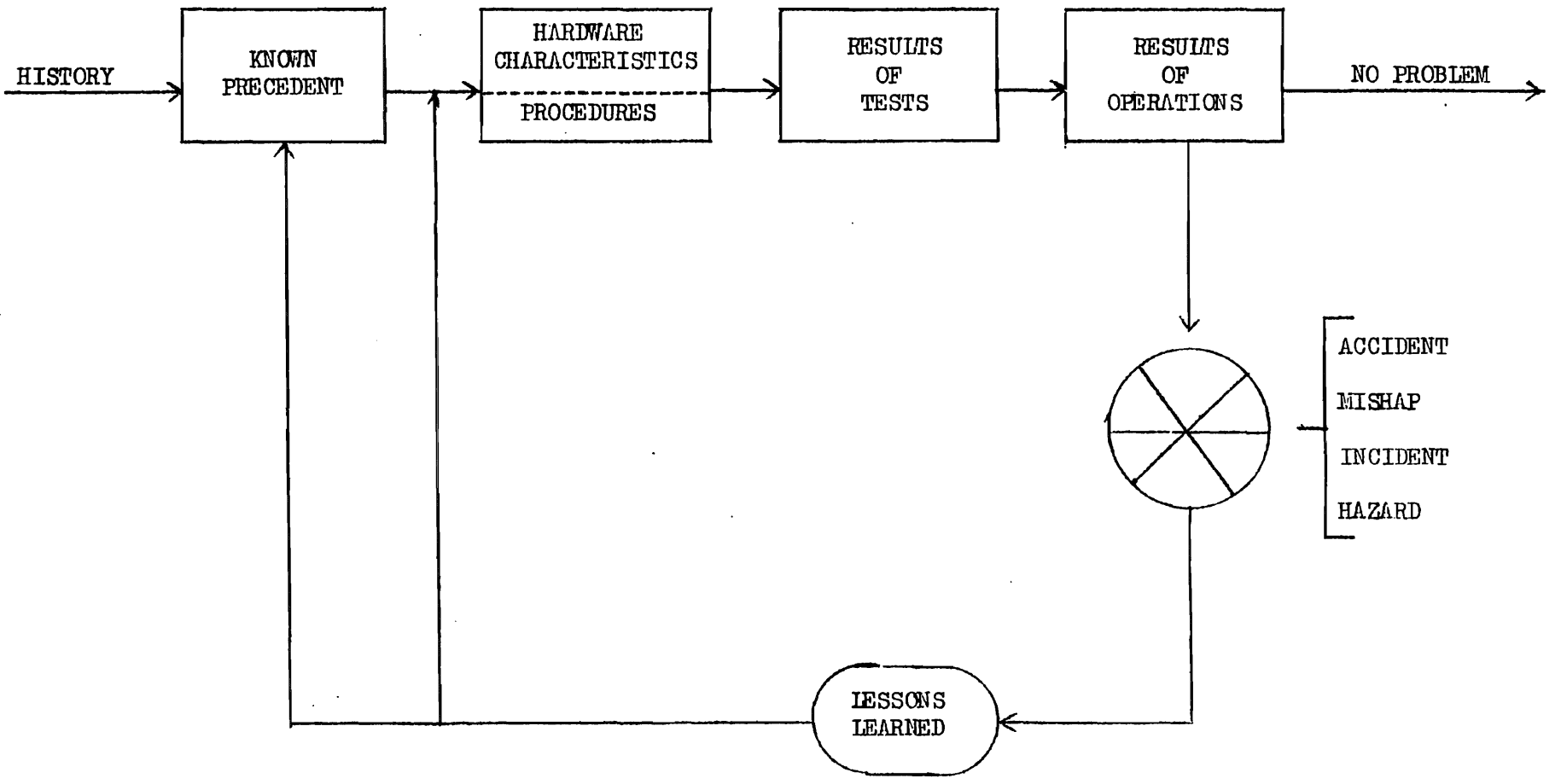
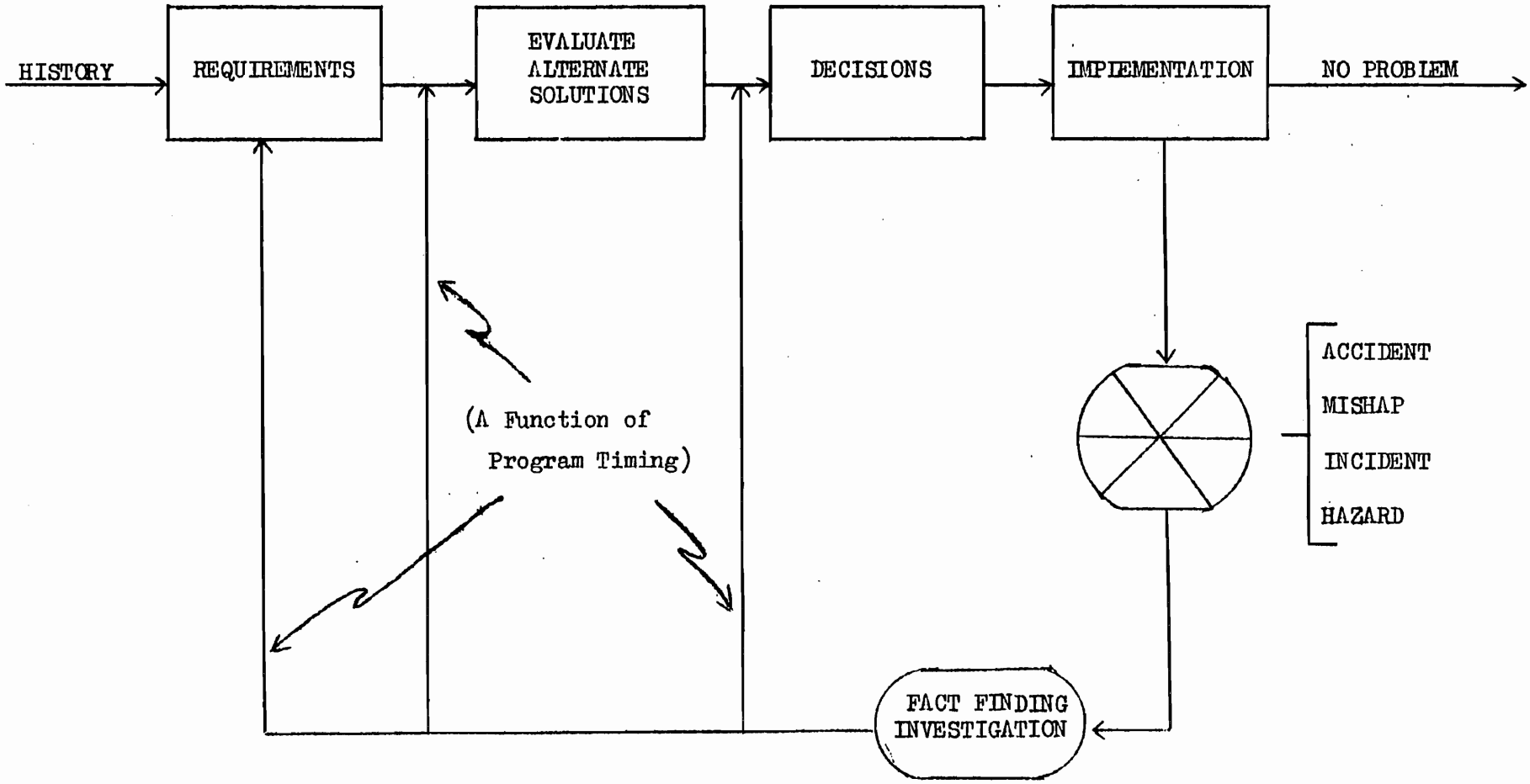


FIGURE 2

MANAGEMENT UTILIZATION OF SAFETY INFORMATION



factors which have already been evaluated as much as is practical and the decision process essentially results immediately. The task is to know which path to take.

The foregoing discussion emphasizes the dynamics and importance of safety information flow. An analysis of why an accident occurred can often be better highlighted by reference to such a flow diagram, rather than an unstructured review of investigation findings.

Types of Safety Information

In the general sense, safety information is any communication of knowledge of value in the accident prevention field. More specifically, it takes the form of:

1. Management data reports .... the increasing volume of documentation pertaining to the system development not necessarily under the heading of safety per se. (31:9-13)

2. Accident/hazard information .... actual investigation reports and summaries, or analyses thereof. This could also be part of (1) since accidents or hazard reports could be considered a status report on management's effectiveness.

3. Procedural/directive information .... those ways which have demonstrated good accident prevention results in the past. (Manuals, job procedures, technical orders, etc.).

4. Technology information .... those published documents (books, reports, journal articles) and grossly overlooked unpublished material (bulletins, films, committee minutes, letter reports, etc.).

5. Personal knowledge .... information in the minds of men.

Safety information is indeed voluminous. This can be appreciated only when the interdisciplinary nature of accident prevention is recognized. The safety practitioner finds it necessary to know the language of many fields. He must do this to be able to apply knowledge not otherwise recognized as potentially contributory to accident prevention.

In relation to safety information, the safety specialist becomes, in a sense, a generalist. He will search many fields, retaining his specialist classification only because he is trying to spotlight unique bits of information that have specific accident prevention meaning.

Safety Information Sources

If a given discipline chooses to organize its knowledge for advancement of their phase of the total state of the art, the members of that discipline must personally participate in the storage and retrieval process. This is not something that can be delegated to a documentation centre or a secretary. Although documentation concepts are best understood and implemented by documentation trained personnel, subject classification of documents is the key to user oriented information retrieval. It must be accomplished by those in the particular discipline to be effective. (31)

A significant amount of data is stored as a direct result of accidents. Thousands, perhaps millions of IBM cards are in existence to tell what happened during a given period of accident exposure. Examination of the accident code books reflects a continuing effort to include material on why the accident happened, although much of this gets lost on the way from the investigation to the key punch operator.

What is known, however, of the prevention activity resulting from accident? Does anyone really know where the accident lessons go after the pieces were picked up? The answers are negative. An entire new aspect of accident data recording is needed in the future if the loop is ever to be tightened between accidents and prevention.

It can be concluded that the system safety discipline has been trying to mature in a period of an information explosion. Such an environment could be helpful since resultant technologies have now become available to economically classify, store, and retrieve information. Thus, as a young activity, the safety discipline heritage can be efficiently built if those in the field realize the requirement and were able to do something about it. This is where management must help by recognizing the value of safety information and provide funds accordingly.

CHAPTER VII

ANATOMY OF SYSTEM SAFETY

Anatomy of An Accident

> "A man has a protracted argument with his wife. He stamps out of the house to the nearest bar and drinks four highballs. He then decides to go for a ride. It is night-time; there is a skim of snow on the ground, and the tyres on our victim's car are smooth. In rounding a poorly banked curve at excessive speed, the right front tyre blows out, the car leaves the road and is demolished". (10)

The question becomes "What caused the accident?" Was it the liquor, the poor visibility, the snow, the tyre condition, the highway engineering, the wife -- or a combination of all these factors? More importantly, what should be done to prevent this type of accident in the future?

Accidents today are classified personnel error, material factor, weather, facilities, and the like. All were present in the above case as they often are in many accidents. Arguments sometimes ensue as to which factor should be applied in the finding. Principally, these findings remain descriptive man-made judgments about what happened in an accident.

To have an accident prevention effect on future operations, findings must proceed through intermediate steps to implemented action or the information generated during the investigation is virtually wasted. This involves decisions on what should be done and who should do it; and finally the decision implementation process itself. What should be done is often indicated in the accident report through the usual recommendations. However, classifications or analyses are rarely made of recommendations regarding what should be done.

Pursuing this line of reasoning further, a recommended action presumably becomes the responsibility of some organization or person to make a decision -- including possibly to do nothing about it. In any case, rarely, if ever, are classifications or analyses of decisions made on accident investigation recommendations. (i.e., who was to make a decision, who actually made the decision, and what that decision was).

Finally, some specific action would presumably be taken if a recommendation is approved by the appropriate party. Again, few if any classifications or analyses of implemented action are made based on decisions made following accident investigation recommendations. (i.e., what was done?)

It should be remembered that a given accident cause factor labelled by the investigation as material failure, may well be treated in several ways. The hardware may be changed through redesign. The problem may be treated by a modification in procedure, be it during manufacture, maintenance, or operation. The solution may be a change in people through training or replacement, the decision might be to live with the problem. These choices are not the prerogative of an investigating group since they may not have all facts available on the sonsequences of implementing a recommendation. The investigating group should not be discouraged from pointing the way to corrective action as they see it. However, a summary of findings, or even recommendations, becomes a limited one.

Current methods for analysis of safety information gained from accident investigations do not go far enough to really establish where the breakdowns occur between the acquisition of prevention information and actual prevention of accidents. This might appropriately be called action failure. (42) On occasion, an individual accident is treated in depth, but little is done to document all accidents completely from occurrence to actual implementation of corrective action. Unless this is accomplished, how does one efficiently use the efforts of the accident investigators? How does one assure that the accident will not reoccur while time was being consumed in protracted decision and implementation processing?

This is indeed a challenge to management and safety personnel alike. It means a required thorough understanding of factors involved in system safety as well as the total safety and management information flow described earlier.

Factors in System Safety

Traditionally in system safety, the man, the machine and the media (environment) have been described as factors in accident causation and consequently, factors in accident prevention. It would seem management is an identifiable fourth element in accident prevention of equal or superior importance to the other M's.

Management's role is difficult to distinguish since current analysis methods used to assess accident causation do not adequately evaluate the management process. Other factors in the system safety model are the aforementioned information factor, cost and time (schedules). It is logical to assume that management is in the best position to create an environment in which all of these factors can be examined in the most efficient manner.

The Implementation Process

Professional engineers subscribe to Canons of Ethics which includes their safety responsibility in clear terms. (19) The question is asked, however, as to what happens to a safety problem handed up the line to a decision making executive? To phrase it another way, if someone is in the decision making stream without a specific set of guidelines established on the point in question, what action will be taken? The answer, of course, is human judgment based on the knowledge he has or can attain within the time available for decision. Thus the implementation role of system safety is to provide the manager objective data with which his conscience can be exercised. This is accomplished through well defined tasks concerning accident prevention.

System safety, as a relatively new discipline, faces a two-pronged problem today. On one hand is the diminishing safety improvement rate in most areas. This means improvements in our increasingly complex society will continue to be technically more difficult. (9)

The other problem for safety is neither new nor unique. It concerns innovation. By system safety's very definition as a further breakdown of the expanding technology, it will continue to encounter cries of "cult", "preachers", and "pitchmen". This is a well established and predictable behavioural reaction on the part of a manager or anyone else to whom something must be "sold".

Safety operates with other strikes against it as an innovator. First in the relatively rare nature of accidents, expensive though they may be. Second is the previously mentioned inability to prove conclusively why something -- an accident -- did not happen.

There is a need to create the atmosphere for change, which in turn leads to the requirement for a specific strategy to implement change. Thirteen steps of innovation that should be followed by any innovator are shown in Table 5.

Anyone who ever tried to sell a new idea and failed, will undoubtedly recognize some of these admonitions as possibly being the reason for that failure.

TABLE 5

THIRTEEN STEPS FOR INNOVATION

1. Become accepted by your associates as a respected responsible individual before attempting to win confidence for a new idea.

2. Realize the time to start preparing is well in advance of the initial proposal.

3. Avoid proprietary jealousies . . . try to create conditions that will build an "ownership" interest that will make others as interested as the innovator in putting over new ideas.

4. At a preliminary stage, participation should be spread through several levels of organization.

5. Recognize the "what's in it for me" reaction, and use such personal interests of associates in soliciting their support and approval.

6. Rigid thinking of the either - or, black or white variety should be avoided . . . be "political" in the approach.

7. Maintain an open minded interest in the ideas of others . . . it will encourage reciprocity.

8. Take particular care when faced with a resultant change in the power structure of the organization because of the innovation . . . plan the desired change with the minimum upset of the status quo.

9. Recognize timing as an important part of strategy . . . be sensitive to the particular climate of the existing state of affairs . . . decide when to advance the idea or keep it in a temporary deep freeze.

10. Avoid filing proposal upon proposal in rapid succession which will encourage resistance.

11. Use organizational channels for the purpose they were designed to serve . . . short cuts are only a last resort.

12. Never attack resistance head on . . . or with public criticism . . . Its intensity will mount in proportion to the volume of criticism raised against it.

13. Provide clear and persuasive presentation of ideas . . . good ideas deserve good presentations.

NATIONAL SAFETY COUNCIL October 12, 1967

CHANGE DOCKET

NAME Mike TITLE Foreman, Dept. 22

JOB Manufacture widget boxes from sheet metal -- mostly a punch press operation.

DATE	CHANGES	COUNTER-CHANGES
10/5	New 707 press delivered.	Check Engr. specs & see if press conforms? Check set-up? Reroute trucks during set-up? Review JSA for possible change. Who to assign?
10/6	Engr. says new material for #603 box will come in 10/15.	Burrs? Can Dept 23 handle? Speed up 1st day? or hold till later? Explain whole change to everybody?
10/7	Joe Zilch Badge #62,706, reported. Two yrs experience at Acme.	Interim clearance & papers. ✓ JSA on bee press. Observe OK Assigned to Jerry as buddy (Jerry said ISA should be revised.)
10/8	We'll need about 100 hours of overtime this week to get out Fcd. order.	Who? when? Supervise?
10/10	West parking lot closed on Saturday. Jim mad as h—	Buy him a coffee to cool off. (Jim could be Asst if we double?)
10/12	Six 1st aid cases last week — all slight	Review for potential & recheck last 6 weeks.
10/13	8% rejects from #602 box, & in phase out??	?
10/14	Leave at 3:30 to take Sue to Dr.	

ATIONAL SAFETY COUNCIL

October 12, 1967

CHANGE DOCKET

NAME Joe TITLE President

OB Plans to be the low-cost producer of high-quality products, and market them.

DATE	1967 CHANGES	COUNTER-CHANGES
July	Product liability suits are eroding profits. (Legal say Walter's claim may cost $300,000. 1966 claims were $45,000 vs $22,000 in 1960. Looks like '67 will be a million. In 1968?)	Have Marketing study use criteria now, 5 years & 10 years ahead? Have Legal publish their criteria? Augment R&D staff? Establish strong safety policy? Redesign products? Give better dealer & customer service?
Aug.	Marketing VP killed in traffic accident. (Were the 3rd outfit in town to get hit this way — wonder if there were others & what their acc. cost.)	Promote Asst. V.P. & coach him well? Start an OTJ safety program? Ask Medical to get info. on alcoholism programs?
Sep.	Competent, responsible people are not available in needed numbers & turnover is high. (as of yesterday we have 265 vacancies & turnover is 25% for hourly group)	Restructure jobs to isolate unskilled components? Develop special programs for under-qualified? Drastically improve training? Revise salary & other benefits to build pride? (Rept due 11/1)
Oct.	Supervision is deteriorating & here too turnover is rising. (If we lose supervisory control, we're dead.) Why did Joe, a good man, resign?	Keep salaries competitive? Increase pride building elements? Provide more training — general & special? Start JSA & JII next week? (Make it a point to visit at least one Dept. every day.)

Get new input who can help

NATIONAL SAFETY COUNCIL

October 12, 1967

CHANGE DOCKET

NAME _____ TITLE _____

JOB _____

DATE	CHANGES	COUNTER-CHANGES

Whither Safety

System Safety has approached a series of intersections. There is significant progress in having safety as a special entity in systems management. On the other hand, there is an air of "put up or shut up" to this picture. Funding for safety tasks will continue only as long as they contribute to mission success in the form intended. Hence, system safety specialists must not falter in responding to the challenge which they, to a large measure, brought about themselves. They would be wise to review the market fluctuations in the reliability field over the past decade to avoid the mistakes made therein. These mistakes have included a super-dependency on statistical analysis techniques and a neglect to appreciate the contributions to reliability objectives available from other disciplines.

The industrial safety field continues to function primarily in the operational phase of the system life. It too, however, is feeling the impact of the system approach to safety. (37, 50) It should only be a matter of time before all of the safeties will be more closely aligned professionally than they are today.

Many of the problem areas described in this document will continue -- some diminishing such as the misunderstood meaning of system safety -- some increasing such as the law-safety interface problem. Staff-line and related organizational conflicts will continue. Similarly, management faces continuing problems in evaluation and measurement of accident prevention performance and in safety information communications.

The extent to which this safety integration process is carried out by managers and by safety specialists remains to be seen. Hopefully, this document will contribute knowledge towards improved mutual understanding between safety and management.

As a special message for those in the safety business, consider this recessional hymn:

> "Every industry is obliged to improve its safety record where it can. Those who insist on ignoring the smaller safety problems about which something can be done, pointing to the larger problems about which nothing can be done yet, are mostly evading the issue. Most safety measures adopted by an industry deal with small portions of the total hazard. Over the years the steady improvement that results is significant. If each step is discouraged because it doesn't solve the whole problem, then nothing is accomplished". (35)

REFERENCES

1. Alford, L.P. and Beatty, H.R., Principles of Industrial Management, Revised Edition (New York: Ronald Press, 1951).

2. ARINC Research Corporation, "System Effectiveness Training Course Notebook". Washington, D.C., 1965.

3. Barnhart, C.L. et al, The World Book Encyclopedia Dictionary (Chicago: Doubleday and Co., 1963).

4. Barton, J.A., "Dyna Soar I Failure and Escape Analysis" Report E8R 11774, Chance Vought Corporation, Dallas, Texas, December 1958.

5. Barton, J.A., "Operational Safety Analysis Techniques". Annals of Reliability and Maintainability, Vol.4 (Washington: Spartan Books, 1965).

6. Bertrandias, Maj. Gen. V.E., "Flight Safety Research". IAS Aeronautical Engineering Review, April 1951.

7. Blake, R.P., Industrial Safety, Third Edition (Englewood, N.J.: Prentice Hall, 1964).

8. Bush, P.S., Jr., "Aircraft Products Liability". Johnson & Higgins, New York (Speech given at the Aviation Distributors and Manufacturers Convention, Grand Bahama Island, November 1965).

9. Caldara, Maj. Gen. (Ret) Joseph D., "The Diminishing Safety Improvement Rate". Alumni Review, Aerospace Safety Division, University of Southern California, Fall 1964.

10. Chapannis, A., "The Design & Conduct of Human Engineering Studies". Technical Report No. 14, San Diego State College Foundation, San Diego, Calif. (No date)

11. Cohen, Jerry and Murphy, W.S., "Burn, Baby, Burn". Life Magazine, July 15, 1966.

12. Hancey, Carl, "Safety Education and the Management Process." Annals of Reliability and Maintainability, Vol.4 (Washington, D.C.: Spartan Books, July 1965).

13. Hensley, Col. H.S., "System Safety - The Development of a New Program for Defense". Safety Division Headquarters, Air Force Systems Command, Andrews AFB, July 1966.

14. Hodapp, E.J., Jr., "Dyna Soar Safety Program". Aerospace Safety, December 1960.

15. Holladay, David H., "What Constitutes a Safety Program". Aerospace Safety Division, University of Southern California, March 1961.

16. Johnson, R.A., Kast, F.E., and Rosenzweig, J.E., The Theory and Management of Systems (New York: McGraw-Hill, 1963).

17. Kohlheyer, Richard, "Purpose and Progress: 1966 Report". Hazard Prevention, Vol. 3, No. 5, April 1966. (Bulletin of the Aerospace System Safety Society).

18. Koontz, H. and O'Donnel, C., Principles of Management, Third Edition (New York: McGraw-Hill, 1964).

19. Lederer, J., "Reduction of Aircraft Accidents". Flight Safety Foundation, New York (Delivered to the Air Research and Development Command Safety Conference, Baltimore, Md., September 1954).

20. Likert, Rensis, New Patterns of Management (New York: McGraw-Hill, 1961).

21. Longnecker, J.G., Principles of Management & Organizational Behaviour (Columbus: Merrill Books, 1964).

22. McCourt, Francis P., "Safety is a Commodity". U.S. Army Transportation Research Command, Spring 1965.

23. Medford, J.F., "1970 ... ?" Hazard Prevention, February 1966. (Bulletin of the Aerospace System Safety Society).

24. Miller, C.O., "Applying Lessons Learned from Accident Investigations to Design Through a System Safety Concept". Chance Vought Aircraft, Inc., Dallas, Texas. (Presented at the Flight Safety Foundation Seminar, Santa Fe, New Mexico, November 1954).

25. Miller, C.O., "Design Systems Safety in Operation". Chance Vought Aircraft, Inc., Dallas, Texas. (Presented at the Flight Safety Foundation Seminar, Taxco, Mexico, November 1955).

26. Miller, C.O., "The Role of Flight Safety Engineering in Aircraft Reliability and Effectiveness". Chance Vought Aircraft, Inc., Dallas, Texas. (Presented at the first IAS Naval Aviation Meeting, San Diego, Calif., August 1957.)

27. Miller, C.O., "Legal Ramifications of Aircraft Accident/Malfunction Data". Proceedings of the IAS National Aerospace Systems Reliability Symposium, Vol. 1, Salt Lake City, Utah, April 1962.

28. Miller, C.O., "The Engineer, Lawyer and Flight Safety". Flight Safety Foundation, New York, N.Y. (Presented at the SAE-ASNE National Aero-Nautical Meeting, Washington, D.C., April 1963).

29. Miller, C.O., "Aviation Law-Air Safety (A Symposium Report)". Alumni Review, Aerospace Safety Division, University of Southern California, Fall 1964.

30. Miller, C.O., "The Safety Information Challenge". ASSE Journal, September, 1966. (Originally presented at the 17th Annual Flight Safety Foundation Seminar, New York, October 1964).

31. Miller, C.O., "Current Safety Information Classification, Storage and Retrieval". Aerospace Safety Division, University of Southern California. (Presented at the Systems Safety Symposium, Seattle, Wash., June 1965).

32. Miller, C.O., "The Influence of Systems Engineering and Management on Aviation Products Liability". Aerospace Safety Division, University of Southern California, January 1966.

33. Newman, W.H., and Summer, C.E., The Process of Management (Englewood, N.J.: Prentice-Hall, 1961).

34. Peck, M.J., and Scherer, F.M., The Weapon Acquisition Process (Boston: Harvard Business School, 1962).

35. Pinkle, I. Irving, Personal Communication with C.O. Miller, Institute of Aerospace Safety and Management, University of Southern California, October 1962.

36. Pitts, W.C., "Summary Report of Reliability-Safety Analysis Methodology for Manned Space Vehicles". Report AST/EOR-13030, Chance Vought Corporation, Dallas, Texas, July 1960.

37. Recht, J.L., "Systems Safety Analysis". Reprint, National Safety News, National Safety Council, Chicago, Illinois, June 1966.

38. Riordan, J.J., "The Problem of Cultism in Logistics, Management". Department of Defense. (Presented at the Eighth Navy-Industry Conference on Material Reliability, Washington, D.C., May 1965).

39. Robb, D.A., "Safety Is Not Just Common Sense - A Trial Lawyer's View". ASSE Journal, December 1965.

40. Robbins, Jay T., "System Safety Implementation Problems". Directorate of Aerospace Safety, Norton AFB, California. (Presented at Systems Safety Symposium, Seattle, Wash., June 1965).

41. Ruff, Lt. Col. George F., (Ret) and Haviland, Maj. George P., "Early USAF Efforts to Develop System Safety". (Presented at the Systems Safety Symposium, Seattle, Wash., June 1965).

42. Stevenson, Maj. Gen. John D., "Ideas and Realities". (Presented at the First Annual USAF Safety Congress, Riverside, Calif., September 1960).

43. Taylor, F.W., Scientific Management (New York: Harper & Row, 1947).

44. Theleman, D.R., "Industry Safety Information Interchange System, Part I Need and Ramification". Northrop NORAIR, Hawthorne, Calif. (Presented at the Systems Safety Symposium, Seattle, Wash., January 1965).

45. U.S. Air Force, "General Requirements for Safety Engineering of Systems and Equipment". MIL-S-38130. Headquarters, U.S. Air Force Systems Command, Washington, D.C., September 1963.

46. U.S. Air Force, "Systems Engineering Management Procedures". AFSCM 375-5, Air Force Systems Command, Washington, D.C., December, 1964.

47. U.S. Air Force, Systems Engineering Group, Wright-Patterson AFB, Ohio. Request for Proposal No. 01071 dated 7 January 1966.

48. U.S. Army, "Safety Engineering of Aircraft Systems, Associated Sub-systems, and Equipment; General Requirements for". MIL-S-58077 (MO), June, 1964.

49. U.S. Navy, Letter to the Assistant Chief for Research, Development, Test and Evaluation from the Intra-Bureau Systems Effectiveness Policy Committee, RAAV 02/39, Washington, D.C., 9 April 1964.

50. Wissner, I.E., "How System Safety Relates to Industrial Safety". National Safety News, National Safety Council, Chicago, Illinois, May 1966.

51. Wood, Amos L., "The Organization and Utilization of An Aircraft Manufacturer's Air Safety Program". The Boeing Company, Seattle, Wash. (Presented at the Institute of the Aeronautical Sciences Meeting, New York, January, 1946).