THE ROLE OF SYSTEM SAFETY

IN

AEROSPACE MANAGEMENT

by

Charles Otto Miller III

A Thesis Presented to the

FACULTY OF THE GRADUATE SCHOOL

UNIVERSITY OF SOUTHERN CALIFORNIA

In Partial Fulfillment of the

Requirements for the Degree

MASTER OF AEROSPACE OPERATIONS MANAGEMENT

January 1967

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

UNIVERSITY OF SOUTHERN CALIFORNIA
THE GRADUATE SCHOOL
UNIVERSITY PARK
LOS ANGELES, CALIFORNIA 90007

This thesis, written by

Charles Otto Miller

under the direction of his Thesis Committee, and approved by all its members, has been presented to and accepted by the Dean of The Graduate School, in partial fulfillment of the requirements for the degree of

Master of Aerospace Operations Management

Milton C. Kloetzel
Dean

Date February, 1967

THESIS COMMITTEE

Harold Sherman
Chairman

Louis A. Lesoine

R. E. Roland

PREFACE

"The best man in my belief is he who lays his plans warily, with an eye for every disaster which might occur, and then when the time for action comes, acts boldly."

HERODOTUS

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ILLUSTRATIONS

INTRODUCTION

Safety and management can be written many ways: safety as a function of management, management as a function of safety, safety equals management, or safety versus management. In examining each, an investigator would undoubtedly encounter component relationships of even more complexity.

Still in today's world - and in today's aerospace world in particular - these relationships must become better understood. United States missiles are poised on launching sites which could literally destroy Los Angeles rather than Vladivostok, if an inadvertent, unguided launch were to occur. Aircraft are on the drawing boards which can singly carry over 500 passengers by the early 1970's. Some preliminary versions of these aircraft observed by the author could carry over 1000 people! Unfortunately, if they can fly, they can fall. No one has devised a way to repeal the law of gravity. The question is not "will missiles detonate inadvertently" or "will aircraft fall accidently." The real question is what can be done to prevent accidents; prevent them in an evermore efficient manner.

It is suggested that safety has become an effective and an increasingly integral part of aerospace management -

especially systems management. Yet this role is by no means complete nor is it fully recognized. Hence, this thesis examines problem areas faced by the aerospace safety discipline within the aerospace management environment. These problems include:

1) Incomplete understanding of the meaning of safety environment. (Chapter I & II)
2) Organizational and philosophical conflicts between safety and other disciplines within the engineering and management hierarchy. (Chapters III through V)
3) Difficulties inherent in evaluating, that is, measuring, effectiveness of accident prevention effort. (Chapter VI)
4) Inefficiencies in communications flow pertaining to accident prevention. (Chapter VII)

The last chapter then describes factors of system accident causation/prevention in model form. Such an approach is necessary if the expensive lessons of the past are to be <u>applied</u> intelligently to preclude even more expensive lessons of the future. Conclusions are presented thereafter not only to summarize the preceding discussion but also to indicate required areas of further inquiry.

CHAPTER I

SAFETY AND SEMANTICS

The Problem Defined

In 1962, a number of representative definitions of "safety" were collected by the author and quoted to show the extreme variability in general understanding of the term "safety" (45:3).* These are reproduced as Table 1. Subsequently, informal safety definition quizzes have been given routinely to scores of students 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.

Thus, the semantics aspects of safety represents a fundamental problem in the role of safety and management; indeed, in safety as related to most activities. It should not, however, be unexpected. The aerospace discipline is young and dynamic. When this is coupled with the complexity and the explosion of aerospace technology, it is obvious that definition of terms is of major significance. Nor is

*Numbers in parenthesis represent references and detailed location of information if appropriate; in this case Reference 45, 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 aviation 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 aviation 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. A feeling of being safe in flight engendered by confidence in those who are responsible for:
   a) Airworthiness of the aircraft
   b) Proficiency of flight crews
   c) Integrity of management

9. 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.

TABLE 1----Continued

10. 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.

11. Action taken toward the prevention of loss in manpower, material and time during aviation activities.

12. A specialized form of over-all reliability which involves actual or potential loss of life; actual or potential loss of the vehicle and/or a high level of emotion.

13. The professional way to do things.

14. Conservation of combat capability.

the situation new or unique. For example, in 1789 the great French chemist, Lavoisier, wrote:

> As ideas are preserved and communicated by means of words, it necessarily follows that we cannot improve the language without at the same time improving the science itself; neither can we, on the other hand, improve a science without improving the language or nomenclature which belongs to it.

While safety is not a science today, Lavoisier's thoughts are still relevant. He might have added, however, not to expect unanimity in acceptance of specific terminology. Nor should one expect zero modifications with time to the language of aerospace safety because of its dynamic status.

Safety Defined

To the passenger or crewmen of an air vehicle, 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 (2). 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 behavior involving preservation of life involves both his conscious and subconscious mind.

To members of the aerospace engineering and management complex, safety has evolved to further meaning, beyond the

innate abstraction common to all men. To aerospace 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.

To the practitioner of the aerospace 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 aerospace safety field several commonly accepted precepts appear. These include:

1) Relative freedom from danger: One may have a goal of zero accidents, but he will choose to function with less than perfect safety. 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 com-

promises 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 equally as important as cases involving only injury to personnel. Fundamental categories in the safety process are hazards to equipment operated on, tools and machines, operators, property in the environments, and contiguous personnel (149). 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 simply air transportation. This is, however, the least recognized precept among non professionals in aerospace safety. It conflicts with personal exposures to dangerous situations and does not necessarily agree with precepts followed by most safety practitioners in other areas, for example, automobile or industrial safety.

4) Progressive activity: With either military or civilian aerospace endeavors, there is a dynamic activity involved; an interaction of people and resources which must develop to exist in the future. If it is not healthy, that is 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, accident prevention feature. In the military, especially with missile operations, there is a corollary meaning, namely the necessity to react to a catastrophe prior to losing further combat capability.

Thus it should be obvious that aerospace 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:

> Aerospace safety is the objective conservation of men and equipment in a timely manner, and within the operational and economic requirements necessary in a progressive aerospace community. (45:3)

"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.

System Safety Defined

In recent years, the terms system(s) safety and system safety engineering have been heard if 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 an air

vehicle system." (46)

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." (106:9)

Similarly, system safety engineering has been defined by Air Force Major General Robbins as "the specific application of management, scientific and engineering criteria, principles and techniques throughout all aspects of system development, to assure optimum safety." (86:1) Note here the qualification of "system development" which would not cover the entire life cycle of a system, and the implied meaning of a single weapon system as opposed to a discipline oriented approach. 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 an aerospace contractor. It reflects USAF systems management terminology. It is shown here because the USAF has led the world in identification of aerospace 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 of an air vehicle, and system safety engineering covers only the concept, definition, and acquisition phases of system programming,* does it not follow there is another part of the whole . . . system safety-operational, or simply operational safety. Could not General Robbins' safety engineering definition be paraphrased by describing 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?"

Operational safety terminology was used by Barton but has yet to gain widespread acceptance; perhaps because this has been virtually the entire meaning of aerospace safety to most people in the field (3:299-302). People tend to resent new names for things they have been doing all along.

Another fine point in safety and semantics involves the use of the term system or systems to modify safety. It has been argued that systems is the more generalized discipline oriented approach as contrasted to the single system

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

application (46:5). However, Ruff provides an excellent interpretation of "system" based on an original description in USAF Manual AFSCM 375-5. He states:

> A system is the unification of all component parts of a whole, necessary for the production of a single set of purposive outputs based on proper transformation of inputs, in obedience to effective control . . . It is, therefore, encumbent upon the person using the word 'system' to precisely define or bound the limits in which the system operates. As an example, the earth may be a system when limited to the earth's bounds, however, when viewed in relation to the solar system, the earth becomes a subsystem. (53:8)

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

This means system safety could be applicable to the environs of an airline president or a line maintenance man; a multi-star general, or an airman; a Vice-President of Engineering at a prime manufacturer or a draftsman at a third tier subcontractor. It follows, then, that applying principles of system safety constitute a process and should remain the same during decision-making at any level. Only the details of the particular task at hand determine the precise effort. Actions relative to system safety 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." (11:325) The pattern is the same; using personnel, skills and resources to achieve something. But the "something" in the management sense in aerospace environment is a specific 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 search 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. It was mentioned earlier that aerospace safety today is not a science. This was based on the author's agreement with McCourt who stated:

> By my definition, 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 (131:1).

Certainly when one thinks of system safety an an act in preventing accidents, it would entail <u>doing</u> something. This argues for safety as a sub-division of the engineering discipline. This premise is reinforced when noting a description of modern engineering by G. R. Harrison, Dean Emeritus of the Massachusetts Institute of Technology School of Science. He wrote:

> Modern engineering is distinguished by systematic experimentation and analysis and requires a combined mastery of facts (science), experience (technology), and method (experimentation and analysis) . . . . The engineer must choose the most effective way of accomplishing a desired result and his analysis must involve matters of cost as well as feasibility - a matter of indifference to the prideful scientist (35:16).

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 <u>professional</u> regardless of his specific area of training.

Tarrants cites a profession as "a self-selected, self disciplined group of individuals who hold themselves out to the public as possessing a special skill derived from

education and training and who are prepared to exercise that skill primarily in the interests of others." (56:6) Since the practitioners in the aerospace safety field are truly interdisciplinary; 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 aerospace community. It involves the relation of system safety to older forms of accident prevention such as industrial safety, traffic or highway safety, or other forms of ground safety. In theory, system safety would be a parent discipline with subfunctions such as aviation, missile, nuclear, space vehicle, ground vehicle, undersea vehicle, and industrial. Indeed, some day, this may come to pass for, once again, the truly fundamental principles and techniques of accident injury prevention are not restricted by the system to which

they are applied.*

Aerospace system safety usually is confined to aviation, missile, and space vehicle applications wherein the accident prevention measures are aimed at the vehicles themselves, their immediate equipment and facilities, and the people who operate, maintain or service them. Aerospace safety and system safety will be used synonymously throughout the remainder of this paper and will be limited to the applications just noted. To do otherwise would rapidly expand this thesis beyond practical bounds.

This chapter has thus revealed the varied interpretions of safety as it exists in the aerospace community. There is no single, simple definition, but rather a listing of components or combinations thereof that have achieved varying degrees of understanding and acceptance. Safety can be approached as a condition, a process, or a function. Specialists knowledgeable in all areas will also tend to classify safety as a professional discipline. To the extent this is justified, will become more apparent throughout subsequent chapters.

---

*Note articles concerning system safety appearing recently in the National Safety Council News, a non aerospace publication, references 48, 49, 50, 51, and 60.

CHAPTER II

EVOLUTION OF AEROSPACE SYSTEM SAFETY

Key Historical Events

The recognition of the need to take specific accident prevention measures in our society most likely occurred first during the industrial revolution throughout the world. In the United States, however, National Safety Council was not formed until 1913. Laws governing the safety of explosives did not appear until the post World War I era (4:12).

The Civil Aeronautics Act of 1938 established a Bureau of Safety. This was perhaps the first organization with specific aerospace safety activities of the kind recognized as integral to todays aerospace safety group operations - particularly in the field of accident investigation. According to Major General Griffith, USAF, flight safety became an organizational segment of the Army Air Corps in 1940 (34:15).

It was not until World War II and the demobilization thereafter that the full impact of air accidents was recognized and aviation safety started to grow. For example, in 1943, there were 3,847 Air Corps aircraft destroyed

ascribed to combat conditions compared to 5,000 due to "pure" accidents (150). Similarly, during seven months in 1943, there were 2,932 combat fatalities compared to 3,426 stateside accident victims.

These were highly conservative accident estimates too, since combat losses did not make the distinction between casualties as a direct result of enemy action and those accidents incidental to combat missions. Obviously the flight hours exposure ratio was not comparable to the above. But this did not distract from the loss of mission capability due to accidents as compared to enemy action.

In the immediate post World War II era some far sighted personnel in the commercial aviation field saw the need for full time devotion to accident prevention by a group of specialists. Under the banner of human factors education and safety information dissemination, the Flight Safety Foundation was chartered in 1945. This organization continues today as one of the handful of civilian groups in the world whose exclusive mission is the prevention of aerospace accidents.

A truly landmark paper in aerospace safety was given by Amos L. Wood of the Boeing Company at the Fourteenth Annual Meeting of the Institute of Aeronautical Sciences

(IAS) in New York in January 1946 (91). It was titled: "The Organization of An Aircraft Manufacturer's Air Safety Program." 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 to 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 reasonably formal presentation about system safety. Unfortunately, it was never specifically published by the IAS except as a preprint and was essentially lost to specialists in the field until quite recently. It was referenced in another landmark publication two years later by William I. Stieglitz entitled "Engineering for Safety" which was printed in the IAS Aeronautical Engineering Review in February, 1948 (55:18-23).

This paper was actually presented at a special IAS meeting on safety in September, 1947, which resulted from a conversation among a group of safety specialists at a Civil

Aeronautics Board (CAB) accident hearing in June 1947 (148).

That Mr. Stieglitz's views were far sighted indeed, relative to system safety, are evidenced by a few quotations from his paper:

> 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.
>
> The rate of improvement (in accident prevention) will have to be greatly accelerated if a rapid increase in the total number of accidents and fatalities is to be prevented.*

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

Key events in the 1950's marked the accelerated under-

---

*Lundberg provided a similar admonition about the supersonic transport program in 1963 (119:13).

standing and growth of the aerospace 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) formed at Norton Air Force Base. This was followed by the establishment of safety centers by the Navy in 1955* and Army in 1957 at Norfolk and Fort Rucker respectively. Safety officers became an integral segment of military operational organizations throughout this period.

1951 . . . Major General V. E. Bertrandias, Deputy Inspector General USAF, negotiated with a number of major aircraft manufacturers to have representatives of their engineering staffs serve with the DFSR on a temporary basis (27:33). These later became permanent liaison positions for all USAF contractors.

1953 . . . Courses introduced at the University of Southern California to specially train aviation safety officers. Over 5,000 personnel representing nearly 50 countries have graduated in various accident prevention programs.

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

*Actually, the Navy had the Flight Safety Branch of the Office of the Chief of Naval operations located in Norfolk since 1951. It was, however, "oriented primarily to record keeping and statistics." (125)

considered by sub-system and safety specialists. Fifty-five had been accomplished through 1965.

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 (74, 75).

1957 . . . First known paper relating flight safety engineering to reliability and effectiveness in weapon system design and operations (76). It also commented upon the staff-line relationships which have formed a fundamental point of controversy in safety management philosophy over the years.

1957 . . . Naval Aviation Safety Center sponsorship of the first Conference on Aeronautical Material, Safety and Reliability (1). This resulted in the formation of the Bureau of Weapons - Industry Material Reliability Board, (BIMRAB); a significant policy influencing board relative to system safety in the Navy (79:1).

1958 . . . Federal Aviation Act of 1958. This delineated safety responsibility between the FAA, CAB, and the military services, particularly in connection with air traffic control and accident investigation involving civil aircraft. The Act also generated specific accident prevention functions to be performed by the Civil Aeronautics Board (CAB) and the Federal Aviation Agency (FAA).

1958 . . . First quantitative system safety analysis effort; performed in connection with the Dyna-Soar, (X-20) manned space glider (114, 120). This was a critical analysis of mission accident potential and contained much of the safety "allotment of probability shares" thinking later expressed by Lundberg relative to supersonic air transportation (119:21-23).

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

Entry into the 1960's for the aerospace 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 subsystem or component basis. However, a by-product of the transition into the space age was the system-wide approach to safety through contract requirements.

As reported by Hodapp in 1960, 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 (36:2). 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 in Inglewood, California, for the Dyna-Soar system development, as well as for many other unmanned systems (87:1). Obviously, the qualitative and quantitative safety requirements

established during the entire Dyna-Soar program were milestone events in safety related to management.

However, the ball really picked up speed in June 1962, when 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." (87:3) 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. A lesser known document encompassing some of the 62-41 safety philosophy, but applied to air launched guided missiles, was released by the Navy the previous fall (110).

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 (117). MIL-S-38130 (USAF) covering missiles and aircraft was released 30 September 1963 entitled "General Requirements for Safety Engineering of Systems and Equipment." (102) MIL-S-58077 (MO) was released by the U.S. Army on 30 June 1964 entitled "Safety Engineering of Aircraft Systems, Associated Subsystems, and Equipment; General Requirements for." (108)

The United States Navy's position during this specification development gave rise to an interesting paradox. Personnel at the Naval Aviation Safety Center were among the first to recognize the applicability of the BSD Exhibit 62-41 to aircraft. Indeed, they were very active in promoting an interservice system safety specification for aircraft as well as missiles, including considerable liaison work with the aerospace industry (39:12). However, Navy adoption of the system safety principle hit a snag. Their BIMRAB committee (supra p 23) 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, reliability, maintainability, and other similar requirements under one heading (147).

As will become more apparent in Chapter IV, there was considerable merit in such an approach. However, over three years of possible specification application were lost because of this decision. There resulted a degradation of the safety program for at least one large Navy procurement program, the A7A attack aircraft. The paradox is in evidence when one realizes the Navy safety people gave birth to BIMRAB. Yet it was the same committee that deferred and

nearly destroyed the most important specification development ever to potentially aid the Navy Safety Center's objectives.

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. This culminated in a request for proposals from various organizations in January 1966, and award of an approximate one year contract in June 1966 to the Martin Company of Denver.

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 scheduled for release as MIL-S-38130A by the fall of 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 . . . formerly IAS and the American Rocket Society), 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. It had approximately 200 members at the beginning of 1966. Its purpose is to:

1) Facilitate the interchange of ideas and information 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 (38:1).

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 highly successful program had as its origin the same interdisciplinary approach used for safety officer training and intensive course work (ten weeks and two weeks duration respectively) conducted since 1953 (11:326). 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 aerospace 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 per se with the evolution of accident prevention effort. D. H. Holladay, long time accident prevention instructor

at the University of Southern California, explained it this way:

> 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 . . . . An aircraft cause factor, like history, tends to repeat itself (129:4).

Examples of known precedent are multitudinous. In reviewing the aircraft accidents experienced by the United States Army Signal Corps prior to 1914, a number of interesting cases were observed (28:14-17, 141). For example, in accidents No. 4 (28 September 1912), No. 8 (4 September 1913) and No. 10 (24 November 1913), the pattern was identical: the aircraft was at a relatively low altitude; the engine was heard to go to high power; and the aircraft would dive into the ground. The pilot was unable to control the aircraft because of the excessive pitching moment developed by the thrust vector.

This could be considered known precedent in two ways. First, it is obvious someone did not pass the "word" between accidents 4, 8, and 10, and aircraft are lost today for similar failures to communicate known problem areas. Second, on the technical side, is there any real difference between excessive misaligned thrust in a Wright Biplane or

that which may be produced by an outboard engine in a current vehicle when an engine on the other side suddenly stops? Certainly there is no difference in causal factor principle.

Accident No. 8 also produced the precedent of a manufacturer perhaps not accepting responsibility for his share of the problem. Indeed, Mr. Wright replied to a wire telling him of the accident as follows:

> (The accident) was due to a light gust when descending at too great speed and too small angle of incidence.

Here, apparently was another form of known precedent becoming established, namely, the contractor claiming "pilot error!"

The truism of known precedent 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 aerospace technology, specialists are required in safety to keep reasonably abreast of information developments if nothing else.

As observed numerous times in tracing the literature pertaining to what is now known as system safety, countless

examples were seen of 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 aerospace community at large. This would seem to be a continuing requirement in the presence of the known precedent concept.

CHAPTER III

AEROSPACE SAFETY REQUIREMENTS

Socioeconomic

Requirements form the basis for any function related to management. Socioeconomic requirements for aerospace safety involve factors in one or more of four areas: moral, mission, economic and prestige (76:1). They are implemented either by man's conscience or some regulatory method, with only the latter being reflected in systems specifications.

1) The moral requirement: This has been expressed in several eloquent ways. There was the response to the very American cry of "I got a right!" by an Air Force Chaplain who wrote:

> Yes, we have a right to 'life, liberty and the pursuit of happiness.' Every time someone cuts corners in safety procedures he infringes upon my natural and constitutional rights. Every right has a correlative duty. So when we are tempted to cry out 'I got a right,' remember the rest of it too: 'I got a duty' -- a duty to respect my fellow citizen's rights because we are our brothers keepers (54:12).

Jerome Lederer, founder and Technical Director of the internationally recognized Flight Safety Foundation, pointed out:

> The Judaeo-Christian and other civilizations center

> around the dignity of the individual. Society must conduct itself so as to preserve his rights, protect his person against the harm that might be done to him consciously or in ignorance. Each individual has a spirit, family, friends, and deserves to be respected as an individual (71:13).

Then a most significant statement was issued by President Johnson early in 1965 - a statement which preceded the current high level of executive and legislative interest in safety matters. In "A Safety Policy for the Federal Service," President Johnson said:

> Americans have always placed the highest value on human life, in accord with the worth of every individual. As the public repository of our social ideals, government has a direct obligation to express our regard for human life in every measure necessary to safeguard and protect it (99).

It would seem very little could be added to these statements.

2) The mission requirement: This was discussed when defining safety and describing the aerospace system safety discipline. (Supra p 8) It may also be emphasized by citing the FAA's policy statement of April 1965 which states: "A major factor in the demand for air transportation is its reputation for dependability and safety. Thus, enhanced safety is needed, not only for its own sake but also for the continued growth of our transportation." (98:10) Safety, not only for its own sake . . . that is

the key. Safety is required for mission success.

3) The economic requirement: This factor, especially in consonance with the moral factor, is particularly apparent from a continuation of the previously cited statement by President Johnson:

> Americans also place a high value on efficiency and economy. As this country's largest single employer, the Federal Government has a continuing duty to prevent needless waste . . . . The policy of this Government, then, is both humanitarian and practical . . . . It safeguards and conserves manpower, it reduces the cost of injuries and eliminates the waste of materials . . . . It is a basic element in sound and prudent management (99).

Strangely enough, economics and aerospace safety have been referenced to one another countless times in general terms. Yet, the ability to become definitive in safety economics remains the subject for much needed research (40:14, 58, 70, 118). In the one planning study made in this regard it became obvious why the task is so large, - although not impossible (118). Lederer et al began by classifying safety economics factors in three areas; investment, losses, and returns. Investment was considered that expenditure of funds in direct support of accident/injury prevention. It included the items shown under "Investment" in Table 2.

The problem is that such investment terms are subject to considerable judgment as to what constitutes a pure

TABLE 2

ECONOMIC FACTORS IN SAFETY

Investment	Losses
Design Configuration	Accident Investigation
Quality Control	Mission Disruption
Testing	Crew Considerations
Ground Safety Installations	Insurance/Basic Vehicle Cost
Rescue Services	Legal Fees and Damage Claims
Government Supervision	Deficiency Corrections
Education and Training	Unnecessary Regulations
Medical Programs	National Image
Safety Organizations	Productivity of People

safety investment compared to something that is necessary for the basic function of the air vehicle within its mission definition. For example, in the design configuration area, what portion of the development and production costs of a triple redundant flight control system should be considered a safety investment? Actually, there is no simple answer. After all, the aircraft could probably complete its mission with one or perhaps even two of the systems inoperative. An easier design configuration investment assessment would be the costs of life rafts or other "pure" safety equipment. Also relatively easy to compute would be the man-hours expended by safety organization personnel.

For example, Barton has estimated the total cost of a safety program by a manufacturer at $750,000 over a ten year life cycle for an aircraft which would sell for about one million dollars. Basic arithmetic shows a 33 1/3 per cent profit on investment of such a program assuming only one aircraft saved in ten years due to the system safety efforts (61:9-10). Barton concluded his discussion by saying:

> A new proverb might well be coined to summarize System Safety's place in the new aerospace age . . . 'A penny of prevention is worth a dollar of correction.'

Collins has shown an interesting cost analysis of two major

missile weapon systems; one with a system safety program; one without. Although one and one-third million dollars were expended each year (USAF and industry personnel combined), a cumulative ten million dollar saving was cited. (24:18-20).

Losses are more dramatic and somewhat easier to visualize and record statistically. Yet they too contain items not always considered at first glance and have their own ambiguities. Losses are the operating expense for non-safety and are also listed in Table 2. Usually all that is ever tabulated is "book" value costs of the aircraft or missile itself. Such values in the military amount to over $750,000,000 annually . . . three quarters of a billion dollars! (124, 125)

Not easily described at all are the returns from the investment which could be considered the increased profit in the absence of accidents. Basically, these are the antithesis of the "loss" items plus the benefits to be derived from the complete acceptance of moral responsibilities.

4) The prestige requirement: This factor was given formal recognition by Farish of the NASA Marshall Space Flight Center in describing safety parameters for manned space flight (116:7). He pointed out that a ten million

dollar rocket launching failure was bad enough, but the potential effects on the image of the United States suggests prestige as another "safety to" requirement. The U. S. A., of course, is particularly vulnerable in this area due to our cherished freedom of communications to the public at large.

Another example of this requirement was in evidence following the mid-air collision over Spain in January, 1966 in which a nuclear bomb was lost for several weeks at sea, and another landed in a Spanish field. The millions of dollars expended in retrieval of the weapons involved one thing (economic loss), but the impact on U. S. prestige was ever present throughout the entire operation.

Once again, it is difficult to treat this type of requirement with any real degree of specificity. However, none can deny its existence and the challenge such socio-economic requirements represent to the students of safety and management.

Regulatory Requirements

Safety requirements are implemented in either one of two regulatory forms; statutory laws or contractual documents. There is a point not generally understood about

statutory regulations and civil aviation that eminates from the earliest Anglo-Saxon law. The point involves a differing level of concern for persons riding as fare-paying passengers and people who travel in private aircraft. In essence, those offering their services to the public will be held to a higher standard of care. Indeed, the FAA Act of 1958 requires air carriers to operate with the highest degree of safety in the public interest (95).

Constrast this with the statement made by the FAA relative to General Aviation (non carrier aviation) as follows:

> The agency should pursue a regulatory policy which: (1) recognize the primary right of the individual to accept personal risk but balances this right against society's interest in the safety of the individual; (2) limits the individual's right to incur risk when the exercise of that right creates a risk for others; and (3) regulates in a manner which recognizes both the limited resources of the individual and the need for efficient allocation of public resources (98:15).

No wonder FAA safety rules and regulations will seem inconsistent at times and open to considerable judgment. Like all laws, FAA regulations are statutory in every legal sense of the word and are made to provide the greatest good for the greatest number of people. Where differences of opinion exist, they are resolved in a court of law.

In private enterprise, in the military, and within

other departments and agencies of the government, internal regulatory "statutes" are found. These are better known perhaps, as policy statements, regulations, manuals, specifications, standards, standard operating procedures, etc.

In the USAF alone, there are over a hundred documents which directly concern the Air Force wide safety program (134). Of particular note within the scope of this text is Air Force Regulation (AFR) 127-1, "Responsibilities for United States Air Force Aerospace Accident Prevention Programs." (105) AFR 127-1 is particularly interesting because this was the first system safety regulation (as differentiated from a specification) ever prepared in the sense of system safety as defined in this text. It was released in this form on 20 April 65. It went well beyond previous versions of this regulation or similar exhibits and provided cradle to grave direction to Air Force safety efforts.

Whereas regulations are considered in-house rules, specifications often impose requirements on both the military and their contractors. For example, the stated objective of the original MIL-S-38130 was "to achieve a comprehensive system safety engineering effort, integrated with the system design, development, manufacture, test, checkout, and, as applicable, construction/installation

activation/operational efforts." (102) To accomplish this objective, contractors were directed to: "establish and pursue an active system safety engineering plan." The plan would entail:

1) The contractor's organization for safety, including its function, authorities and interrelationships with other departments.

2) Detailed description of the program sequence including milestones for planning, design, test, and operation.

3) Safety requirements and design safety criteria to be used in system development.

4) Subsystem safety analysis (37:17).

Once the safety engineering plan became part of the contractual agreement, however, it imposed requirements on Air Force personnel. Many parts of the planned program sequence indicated above would require USAF support.

The revision to MIL-S-38130 accomplished in June 1966 did not change any of the original requirements. Rather, they were clarified and broadened where necessary to provide better guidance in the specification's potential application to any air vehicle system.*

*For a comprehensive discussion of implementation considerations for MIL-S-38130 and related documents, see Reference 22, pp. 281-289.

A specification is just one way to implement a series of requirements between the customer and contractor (5:329-332). There can be various guides or handbooks issued, such as the USAF AFSCM 80 - series of instructions to designers (100). Still another way in the software area is through the data requirements/management complex.

In the Air Force Systems Management concept, control of required data has been achieved through reference to the AFSC/AFLC 310 manual, "Management of Contractor Data and Reports." (103) Unless a specific data item is called out in request for proposals and contract negotiations, the contractor will not be reimbursed for submittal of such information. Data items so referenced become essentially segments of a statement of work. They have very high priority compared to any software effort not so requested.

Examples of data items would be hazard analyses, accident/incident reports and the System Safety Engineering Plan itself. Indeed, the safety data items in today's 310 manual are more definitive in many ways than the 38130 specification. It should be recognized, however, that the 310 manual is essentially a recipe book from which the Air Force can choose to apply certain data requirements on a large scale program. The specification on the other hand,

is targeted for relatively small scale projects as well as possible reference in the multi-million dollar efforts.

Other aerospace customer agencies are implementing system safety requirements in various forms. The FAA introduced several system safety tasks in the flight standards requirements for the supersonic transport (96). Subsequently, the FAA instituted a Supersonic Transport (SST) Safety Office within its project structure in July 1965.

Throughout NASA's program management documents, including publications issued by their laboratories, an increased awareness for system safety thinking can be seen (116). Furthermore, in March 1966, NASA solicited sources of technical competence to perform a safety survey of the entire NASA organization and create a NASA Safety and Standards manual (32).

As noted earlier, the Army has released their system safety specification MIL-S-58077 (MO). As the timing of programs would have it, they were the first Service to apply such a specification to a new aircraft development program, the Armed Aerial Fire Support System (AAFSS) (10:157). Since then, MIL-S-38130 has been applied to the Manned Orbiting Laboratory (MOL) project, to the C-5 heavy transport program, to follow-on procurement of the C-141, and several

classified projects. Since 1963, the Navy has applied MIL-S-23069 (WEP) to many of its guided missile programs.

Thus all government procurement agencies for aerospace vehicles have exhibited system safety interest to one degree or another. This is further evidence of safety's growing role in management.

No discussion of safety requirements would be complete without reference to "Mission SAFETY - 70," instituted by President Johnson in February 1965 (99, 123). This was an intradepartmental program of the Labor Department when initially prepared. Upon submission to the White House, however, it was recognized as applicable to all government agencies. It was so instituted (143).

In essence, Mission SAFETY - 70 is a challenge by the President for all government agencies to reduce injuries and costs due to accidents 30% by 1970. It involves military and civilian personnel, on-duty and off-duty. It is not restricted to accidents in any particular medium. Therefore, it includes areas defined earlier as the aerospace field. Mission SAFETY - 70 resulted in specific and far reaching programs in fifty-four agencies by September 1965 (109). It is a program to be monitored closely since a challenge has really been offered to safety management

experts to collectively produce measureable results.

Safety requirements, therefore, serve as do any requirements imposed upon management. They provide as a baseline from which all functions of management must operate. Because of their socioeconomic nature, however, safety requirements are often difficult to assess in convenient, numerical terms. This, in turn, makes the imposition of regulations or specifications for safety a delicate task.

CHAPTER IV

SAFETY RELATED TO MANAGEMENT

Whither Management

In the military, there are commanders and safety officers. In civilian life they would be called managers and safety specialists of one form or another. In both cases they represent a relationship that has evolved within recent times. The dynamics allied 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 author chooses four developments as being fundamental in understanding safety's role in the broad management structure.

1) The exploding technology: This is perhaps more acute in the aerospace industry than any other business short of the government operation itself. 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" 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 (18).

2) The behavioral approach to resource management: Today, one might chuckle over the commander in the old Air Corps days who placed an order on the bulletin board which read:

> By Order of the Commanding Officer:
> There will be no more aircraft
> accidents.

However, analysis of management philosophy will reveal the human side of enterprise has been accepted only relatively recently as a more effective avenue towards goal accomplishment (17:77). 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 systems management: Two main points about systems management have vitally affected safety efforts.*

a) The entirety of the "system" scope: Table 3 discloses the items considered by the USAF as part of a system for management purposes (104:1). It means that when the USAF contracts for a "system," they will buy a single package of hardware plus software to achieve optimum system performance. Prior to the systems management concept, these elements were approached on a piecemeal basis both in contract administration and technical effort.

*Reference to USAF terminology will be utilized in this discussion although all DOD agencies, the Federal Aviation Agency (FAA), and the National Aeronautics and Space Administration (NASA) have developed some form of the systems management process.

TABLE 3

ELEMENTS INCLUDED IN A SYSTEMS CONCEPT

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

b) Centralized visibility and control over a total life cycle: Fundamental to the systems 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 and design or configuration "frozen" very early in the process (conceptual and definition phases). Funds are rarely made available in later acquisition or operations phases for items not planned or established as part of some system baseline.

4) The impact of the complexity barrier: This was mentioned briefly earlier in the name of system effectiveness. 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 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 poor performance, program slippages and huge cost overruns for required "fixes." (21) By the time the system was "shaken down," the original operational requirement may well have been outmoded. In other words, the complex system had arrived but advances in system management had not.

System Effectiveness Defined

System effectiveness then became a term that tried to describe what the customer found missing in their weapon 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." (142: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." (142:I-1) Or,

"A measure of the extent to which a system may be expected to achieve a set of specific mission requirements." (122:3) The Air Force attempted to clarify what it meant by system effectiveness by stating, "It is a function of availability, dependability, and capability." (122:3) The Navy listed technical areas which contribute to Systems Effectiveness as:

- Reliability
- Maintainability
- Operability
- Supportability
- Compatibility
- Design Simplicity
- Human Factors
- Dependability
- Availability (112:1)

However, such areas must be recognized in the policy statement reference framework in which they were given. They are criteria that a customer wants optimized within constraints of cost, schedule and performance. These criteria should not be confused with the management approaches used by a contractor to satisfy those wants. In other words, a contractor will establish his own policies, organizations, people, and tasks to give the customer what he wants. Sometimes the words describing these two viewpoints are the same; sometimes they are different. Suffice to say, a contractor 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
- Logistics/Product Support
- Maintainability
- Quality Assurance
- Reliability
- Systems Engineering
- System Safety
- Value Engineering

If the wants listed earlier as technical areas may be referred to as the "ilities," then these responses by the aerospace 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.

Delineation of the "Ilities"

There is no doubt that considerable confusion (bordering on antagonism) exists in the minds of some managers over these "ility" disciplines; so much so, the disciplines have been branded as "cults" on occasion. Of course, this situation is not unlike the traditional conflict in role

between staff and line. Only in this case, there is the added complication of matrix organization as an attempted solution. Matrix organization will be discussed more in the next chapter.

Those who really mean "cult" in a derogatory sense subscribe to the antithesis of the point made by Stieglitz (Supra p 21) pertaining to the limited total expertise that can be expected in a single individual. In any event, the fact remains, the "cults" have evolved because of a deficiency in previous methods of management which failed to provide adequate system effectiveness in the broad sense (85).

Confusion between the "cults" exists primarily because there are so many common features among them.

- They all base their work on some similar, if not identical system or subsystem, component classification hierarchy when approaching the functional analysis of a given vehicle.
- They all use analytical techniques involving statistical probability and evaluation methods.
- Interdisciplinary approaches are the rule 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 initial design and changes thereto.
- 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 (43).

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 principal viewpoints of the "ility" disciplines are shown in Table 4 (79).

This does not mean elements of one area cannot exhibit interest in or share viewpoints that are similar to those of other activities. However, as practiced 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 effects analysis - a process where attempts are made to outguess future problems based on experience from the past. Shown in Table 5 is an abbreviated outline approach to such an analysis (79). 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

TABLE 4

PRINCIPAL VIEWPOINTS OF THE 'ILITY' DISCIPLINES

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

Logistic/Product Support . . . material and personnel readiness.

Maintainability . . . the vehicle 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 5

TYPICAL ELEMENTS TO BE EXAMINED DURING

FAILURE ANALYSIS

Operating Condition
- Failure most likely
- Failure most important*

Impending Failure
- Symtoms/Recognition*
- How to inspect for it*

Actual Failure Mode
- Symtoms/Recognition*
- Troubleshooting to isolate failure source

Action by crew
- Recommended Procedure
- Possible Alternatives
- Possible Errors*

Effects
- On immediate flight conditions (correct action and incorrect action by crew)*
- On continued flight operations (correct action and incorrect action by crew)*
- Of subsequent additional failures within same system*
- Interfaces/potential effects on other systems*

*Items emphasize the prevention viewpoint

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 exists prior to the failure in a sense although chronologically in the design process it may be accomplished concurrently or after the preliminary failure mode and effects study is made. That is to say, the ability to detect an impending failure will considerably modify one's "judgment" in how to treat a given failure, indeed, 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.

---

*See MIL-S-38130 for clarification of these classification which while not universally adapted, illustrate the judgment factor necessary in doing failure analyses (102).

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 is not something one is born with; although, he soon learns how to practice it in one degree or another. It is something that is learned by the bitter lessons of experience, be it by a designer or a pilot (although the latter would rarely live long enough to get much experience this way). It is learned by retrieving and studying pieces of wrecked vehicles and/or people. It is learned by some specific safety educational process which really only 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 based on personal experiences of the author during many years in the

aerospace industry. 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 Quality 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 well organized, the data concerning specific accident prevention knowledge is immense. It is growing rapidly. Pro-

perly applied, it can prevent accidents (45, 80, 90). This subject will be discussed more in Chapter VII.

Safety vs Reliability

Before leaving the general area of system effectiveness, there is one relationship that requires special delineation. It entails the normally found gross misunderstandings about safety in its relation to reliability; particularly with respect to the reliability analysis process (72, 76, 79, 88, 133). Too often the human limitations in performing a reliability analysis are forgotten. No man or group of men, operating individually or collectively, are going to be able to forecast every conceivable failure or combination thereof which will produce a catastrophic accident. Thus, without this extensive intelligence approaching the infinite in technical ability, just what part of the absolute whole does a given probability number present? Also, even if the technical ability for analysis existed, would the financial resources to apply it be there?

Furthermore, no one to the author's knowledge has been able to quantify the human variable sufficiently to statistically handle human error in an acceptable and/or prac-

tical manner. There have been noble attempts, such as that by Peters and Hall (136); but there is a tremendous way to go if, indeed, it can be done. Woodson has stated "Quantification of human reliability is an extremely difficult, if not impossible task." (25:1-24)

Finally, in respect to reliability versus safety, the Chief of the Navy's Safety Center, Admiral Outlaw, provided a memorable presentation in the fall of 1963. He described the "non-failure" and "failure" modes of reliability with which one must contend (84:4-6). The non-failure made "alludes to the part or system which has no unpredicted failures yet is an accident causal factor. This mode involves human factors, under design, and faults of omission (or commission)." Cockpit layout problems were examples cited in this respect along with many others.

The "failure" mode problem of reliability was "even more insidious" according to Admiral Outlaw. This was "a situation where malfunction is anticipated and perhaps even predicted, but since the failure cycle occurs only once every ten thousand flight hours or only once every two million cycles, the system is considered reliable from a statistical standpoint." He goes on to say, "if this statistically reliable system has its 'once in a million'

failure, and this malfunction results in a catastrophe (that could be reasonably prevented), the system is irrevocably unsatisfactory."

Admiral Outlaw also cited the perfect cartoon to illustrate his point. It showed a military officer looking at an airplane and saying (presumably to a manufacturer) "I know it's reliable, but would you fly in it?"

The Admiral's "once in a million" failure ratio may be open to debate in a systems effectiveness discussion. However, the safety discipline does not permit inhibition of thought process towards accident prevention based on assessment of any one variable such as design reliability. In some respects, safety takes up where reliability leaves off; but this should not be contrued as a simple extension of reliability functions. This is illogical based upon the differences in the system effectiveness disciplines noted earlier. Unquestionably, understanding the relationships between the "ility" disciplines is essential to grasp the unique role of system safety in aerospace management.

Organization For Safety

The four characteristics of aerospace management evolution (exploding technology, humanized approach, the sys-

tems management trend, and concern for systems effectiveness) combined with safety's emerging role have produced interesting challenges akin 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, 16, 24:2).

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 <u>not</u> delegate his responsibility. He will assign duties, grant authority, and create (not transfer) an obligation or accountability in the sub-

*Col. John F. Sharp USAF, former Chief of Safety for the U. S. Air Defense Command has treated this point particularly well in references 138 through 140.

ordinate. 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.

As Newman and Summer point out, the misunderstanding arises because people indiscriminantly confuse "responsibility" with both an assigned duty and an obligation created in a subordinate (19:60). 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.

Undoubtedly, this rationale might well displease the behaviorists. They would prefer that each man have his share of responsibility in the general meaning of the term, which would better satisfy ego needs. However, the same effect could be achieved by stressing job enlargement in safety matters for every man, concurrent with the instituting of safety specialist positions. The need to effect some such delineation during safety program implementation

cannot be emphasized too strongly. Unless both approaches are taken, the risk of complacency will be severe . . . or the attitude developed of "let the other guy do it."

In most aerospace companies familiar to the author, the problem described above has been common to all of the "ility" disciplines at some point in their past. Indeed, it was probably true much earlier when the first stress analysis group was formed outside a basic design group; or the first flutter specialist became something other than an aerodynamicist.

Most of these "mavericks" would begin in a pure staff function and evolve towards line as time progressed. What has confused the picture for safety (and other "ilities"), has been the advent of the matrix system. This might be otherwise called project vs group management, or project vs functional management. It is a byproduct of the systems management concept in which project managers may staff their teams with people from various functional areas for the duration of their need on the project. Figure 1 illustrates the concept as it might apply in an engineering department including the distinction of line and staff as viewed under a project management concept.

The individual so assigned may well be working for two

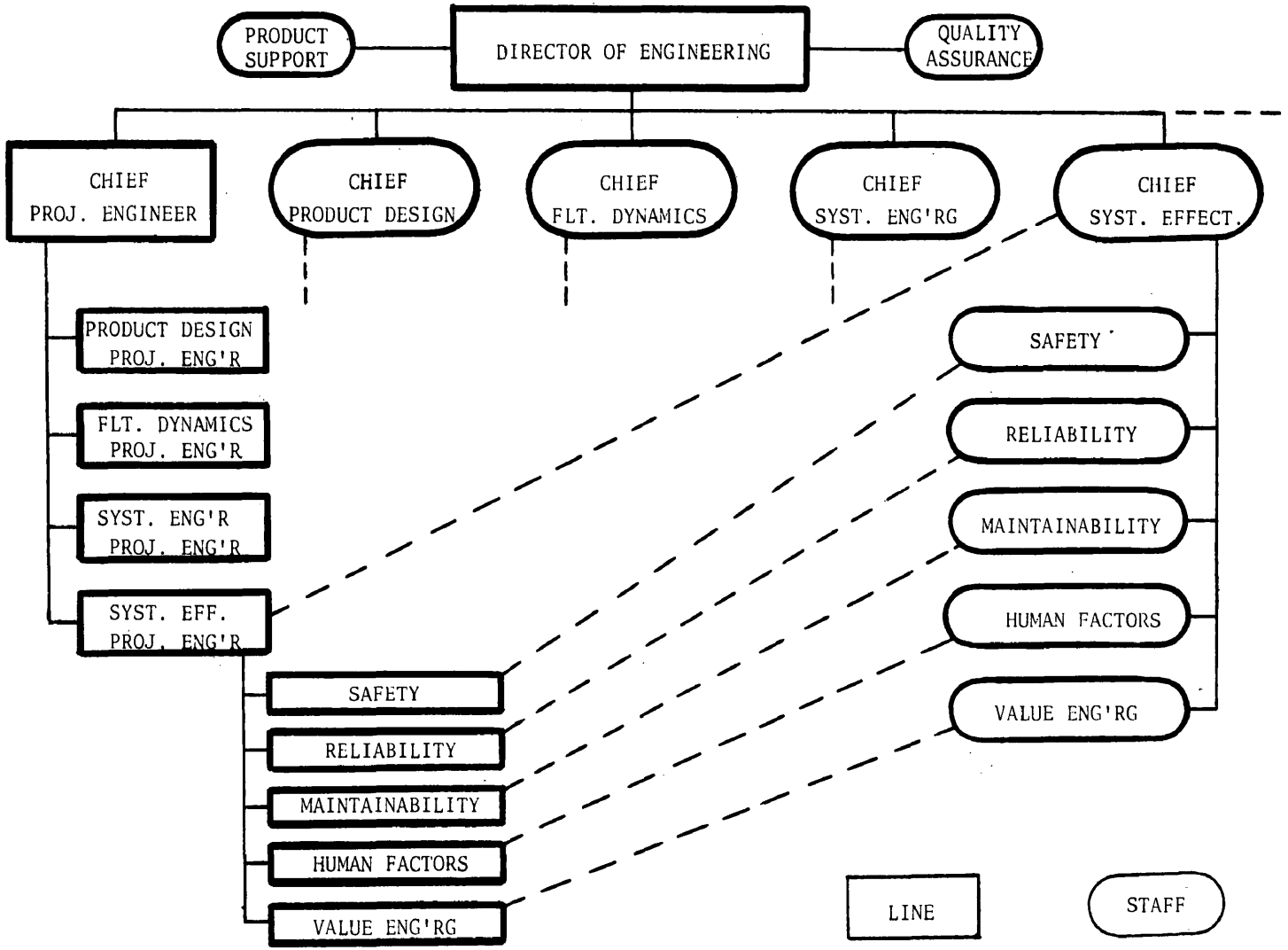

Fig. 1.--MATRIX ORGANIZATION CONCEPT

"bosses" at the same time. By classical management theory, this violates a principle of good management (7:24). However, the project manager will usually have authority and thereby control over what tasks are done and when they are accomplished. The technical group supervisor will usually have authority for how the job will be performed (i.e. technical method), and who of his men will be assigned the task. The conflict occurs over who will rate the man on total job performance.

In any event, the matrix system permits flexibility in assignment of safety as a staff or line function, or both. This depends upon the capabilities of persons in various parts of the total organization and the nature of a given project. For example, if a project has few specific tasks of a safety nature to perform, then the safety group performs as relatively a staff function and no assignment of personnel to the project per se would be accomplished. If, on the other hand, the project requires many specific safety tasks (e.g. response to current USAF requirements) the staff-line matrix concept would be used in its entirety. There would be several full time participants from the safety group on the project staff performing daily jobs. Concurrently, advice and a sense of check and balance would

be effective through the functional safety group. Note in Figure 1 that it reports up a different path to top management.

The establishment of a safety group only within a given project should be avoided. As will be shown in later discussion, several of the tasks to be done in system safety require freedom of communication outside the line authority represented by a project organization. Furthermore, if departmentation is extensive within a total organization, it is conceivable that several levels of the concept illustrated in Figure 1 would be required.

A special note of caution is required in discussing organization and safety when considering the engineering environment - meaning in this case, a design engineering department. A design engineer, by training, visualizes his job as having to produce an economical, efficient, perform-the-mission product. Being as conscientious as his schedules allow, he certainly will not turn out a drawing containing accident inducing features or make an excessively compromising decision involving safety, if he is aware of the total picture (74:1).

On the other hand, and once again because of his training, the engineer may create problems of a safety

nature. As written by Lederer:

> The engineer's technical training creates an extremely literate creature. He falls into the fallacy of thinking that every intelligent person is equally literate and that others, also are inclined to learn by reading handbooks, manuals, or reports . . . Secondly, the places in which the engineers do their laboratory work at college are rarely conducive to teaching the desirability of proper working conditions from the standpoint of human engineers . . . In addition to these handicaps imposed by their college training, many engineers suffer from inexperience . . . (and) when competent designers who have learned their safety lessons by sad experience are moved up to higher administrative posts, they often leave a void in which the upcoming generation must learn again the sad way (69:2-4).

What Lederer described, and what is 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. 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.

An example of this involves the early days of low level ejection seat development. The operators said "Give us a seat which would save personnel during low level emergencies." The designer said, "Fine, here is a zero altitude

seat."* The only problem was that the operators' need for a low level system included vertical descent velocity criteria (i.e. the conditions of a flameout engine approach,) which was not appreciated initially by the engineers. It was the safety specialist's job to better translate these requirements. He then had to ensure that whatever seat performance was available became clearly delineated in operational handbooks in operational language.

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.

Some years ago in a lecture on morale and safety in aviation, Kenneth Andrews emphasized, "Except for Acts of God, every accident, no matter how minor, is a failure in organization." (126) He referred to organization in the broadest sense of the word in management technology, and the fundamental nature of his statement pertaining to safety

*Zero altitude seat . . . one which would recover the pilot above the height at which he ejected, provided the flight path was level with the plane of the earth and the aircraft was upright.

should be recognized.

The Law - Safety Interface

Another facet of safety requiring management 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 (44, 47, 52, 77, 78). That is, if person or property is injured/damaged, someone must pay. The legal principles involves 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." (77:174) From the general management point of view, it becomes not only a threat to an aggressive accident prevention program, but also a very serious economic consideration, because of the absolute part of the liability trend.

As stated by J. P. Coie, General Counsel for the Boeing Company:

> Whether we like it or not, the argument is that social justice and public policy demand that the risk of loss be distributed over the greatest number of those who can best bear it. The argument is further made that there

> are ways and means where the manufacturer or the processor can protect himself. An increase in the price of the product (or) insurance covering product liability are suggested (63:13).

What is the magnitude of the insurance problem? In a recent presentation, P. S. Bush, an aviation insurance executive, indicated a 150 passenger jet airliner crash could readily incur damages amounting to over $40,000,000 (62:15). 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 (31:24).

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 or 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 as well as suffer serious restrictions in accident prevention communications (52:5).

Engineering Compared to Operations

The foregoing discussion of safety and management has been couched in language applicable to the aerospace engineering environment. However, each of the points made has

its counterpart at the operational side. For example, the exploding technology has had its impact on command structures of military operating units. Witness the tremendous communications networks present to control aircraft or weapon availability with their companion system of feedback of failure information. This is not surprising since system effectiveness depends on data from the field as its basic input. In other words, no part of a closed loop function can be independent of developments in another part.

In concept of responsibility for safety, there is absolutely no difference between an operational manager and an engineering manager. There are perhaps some differences in the degree of control each "manager" has over his people, as evidenced by the rank and discipline structure of the military compared to predominently civilian oriented development functions. This is still a matter of degree, however, and not a large one at that. The required communications function is equally strong when comparing a safety engineer with an operational safety man. In the operations field, communications will center primarily between the safety officer and the flight crews. In the development phase, they will primarily center between a safety engineer and a designer - not that other areas will be or should be

overlooked.

Operational personnel have an interesting problem relative to the engineering function at the law-safety interface, especially as it affects a manufacturer. Operational personnel are charged with the fact finding and analysis responsibilities in accident/incident investigations. This is performed from their viewpoint purely in the interest of accident prevention. There are other parties including the public, however, whose interest in investigations is fault determination as a basis for litigation (45:21).

Since the manufacturer is particularly vulnerable in this respect, the availability of evidence from the accident investigations has been the subject of considerable controversy (68, 78, 92). The operational people often need the manufacturer's assistance during investigations. Yet in providing this assistance, the manufacturer increases his vulnerability. Thus the degree of privilege afforded the accident board's findings is a source of concern to management in carrying out its safety responsibilities.*

*Privilege refers to immunity from disclosure or use as courtroom evidence of documents or other forms of communication.

This chapter can be summarized by concluding that aerospace safety and aerospace management are hardly synonymous; but neither can be achieved to a satisfactory degree without the other. Precisely where the safety specialist functions in the system life cycle is a point mainly of academic interest. The words and titles may change, but the principles of such action are fundamentally the same. Similarly, whether safety tasks are accomplished in a line or staff capacity is of little practical concern as long as they are accomplished. The size and mission of the organization, and especially the individual characteristics and capabilities of the people involved, are what determines the most effective organizational alignment for safety personnel.

CHAPTER V

ACCIDENT PREVENTION TASKS

Framework for Application

The traditional approach to accident prevention has been the three E's; Engineering, Education and Enforcement. "Environment" and "Example" were added by McFarland, in discussing accident prevention as a basic management function before an industrial safety audience (42:11-13). All of these factors are recognizable when considered as the results of a decision process facing management.

For example, assume an accident occurs and a decision is faced as to what should be done to preclude its happening again? One can engineer the machine differently, assuming a machine is involved; the personnel who are always involved somewhere can be educated; certain rules or laws can be enforced; 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 were. These absent items were 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 over some time-line framework.

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

1) Evaluation of customer requirements.

2) Conceptual design.

3) Prototype development.

4) Product design.

5) Test and Qualification.

6) Manufacturing.

7) Use.

8) System Retirement.

These are not necessarily sequential; 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. After all, 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 (24:30). It would become an expensive exercising of Parkinson's Law, and no more.*

The military system safety specification and other regulations imply 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 tasks that have stood the test of time and considerable discussion since they were first presented (79).

1) Establishment of accident prevention requirements as early as possible in system development, especially through inputs in system specifications. These could emanate from design safety checklists or other such sources gathered over the years from bitter experience.

2) Participation in hazard condition analyses emphasizing the before-the-fact symtom of failures as well as the effects of failures in the system including its human element. A strong argument can

*Parkinson's Law . . . the concept of self-generation of a need for more people to do a specific job. Based on an analysis originally appearing in The Economist in London on 19 Nov 55 reprinted in full in Fortune, Mar 56.

also be made for the final intersystem failure analysis integration and coordination task 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 vehicle, its crew or surrounding property are endangered by improper functioning of the system.

4) Participation in design mockup reviews. It usually occurs at specific points during system development where numerous viewpoints 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 parent organization's technical infor-

mation center 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 type facilities.

6) Liaison with other aerospace safety organizations such as the United States Directorate of Aerospace Safety, the Naval Aviation Safety Center, the United States Army Board for Aviation Accident Research, the CAB Bureau of Safety, the Flight Safety Foundation, and the Institute of Aerospace Safety and Management of the University of Southern California.

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 standardization, safety councils, 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 emotion charged environment following a catastrophic 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 the essential information feedback loop. It follows that the people most connected with the specialized prevention efforts would be valuable additions to the accident investigation and analysis team. A properly qualified safety specialist should actually direct at least the fact finding portion of the investigation.

12) Follow-up all action resulting from accident/inci-

dent investigations pertaining to the organization represented, and maintaining a current 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 not only through written material but also by personal contact with affected personnel through briefings and safety conferences.

14) Provision for objective response to safety inquiry. A need exists for 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 that would be too embarrassing to report otherwise. This might be called the "Chaplain" task 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 of 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 decribed in the operational safety framework and mean something else. Yet, hopefully, they are fundamental system safety activities in which accident prevention action principles can begin to be recognized regardless of where they are applied. If so, they represent a step towards a science of safety. A description of what is done (or should be done) must precede the hypothesizing of scientific principles which, in turn must be evaluated by experimental means prior to becoming finally established.

Current Safety Functional Assignments

To illustrate safety tasks as they are practiced today an appendix is included in this study that contains representative safety job descriptions or roles played by the

safety function of four different segments of the aerospace community.

First, the U.S. Air Force specialty code descriptions (AFSC's) are quoted for the Safety Staff Officer (AFSC 1916) and the Flying Safety Officer (AFSC 1925). These summarize and describe duties and responsibilities of personnel assigned to direct USAF operational safety programs.

Second is a tabulation of corporate, division, and program safety responsibilities as defined by a major aerospace contracting firm.

Third is a directive type description of the functional role assigned to safety chief of one of the nation's largest civil service astronautical research laboratories.*

Fourth is a discussion of typical airline Flight Safety Officer function, qualities, and duties as presented by the United Kingdom Flight Safety Committee (57). This particular committee is unique in that it represents not only airlines per se, but also the British Air Registration Board, insurance carriers, aerospace companies, and Great Britain's Ministry of Defence.

*The precise identification of this laboratory and the previously described aerospace manufacturing firm is withheld at the request of the personnel providing the data.

Throughout these functional assignments, one can observe some variation in specific tasks as described earlier. There can be no doubt, however, that these tasks comprise a separate function within management. Note also in the appendix, illustrations of the basic organizational philosophies discussed in Chapter IV, especially the staff-line relation so critical to effective accident prevention effort.

CHAPTER VI

EVALUATION OF SAFETY EFFORT

Aerospace Accident Trends

Statistical records of accidents have constituted a way of life in attempting to provide background data for accident prevention. With due care, such records would logically indicate past safety performance and safety status today. For example, Figure 2 shows the comparative accident rates of several segments of aviation. They are plotted on the basis of major accidents per 100,000 flight hours.

As with any statistical summary, these data have their vagaries. First, the definition of a major accident will vary between the activities referenced in Figure 2. Usually, a major accident includes these unplanned events which result in significant injury to personnel or marked property damage. However, the type of flight or the degree of damage can often decide whether a mishap enters the records as a major accident rather than a minor accident or an incident.

Of a more insidious nature in reviewing accident data are the changes in definitions that have occurred over the

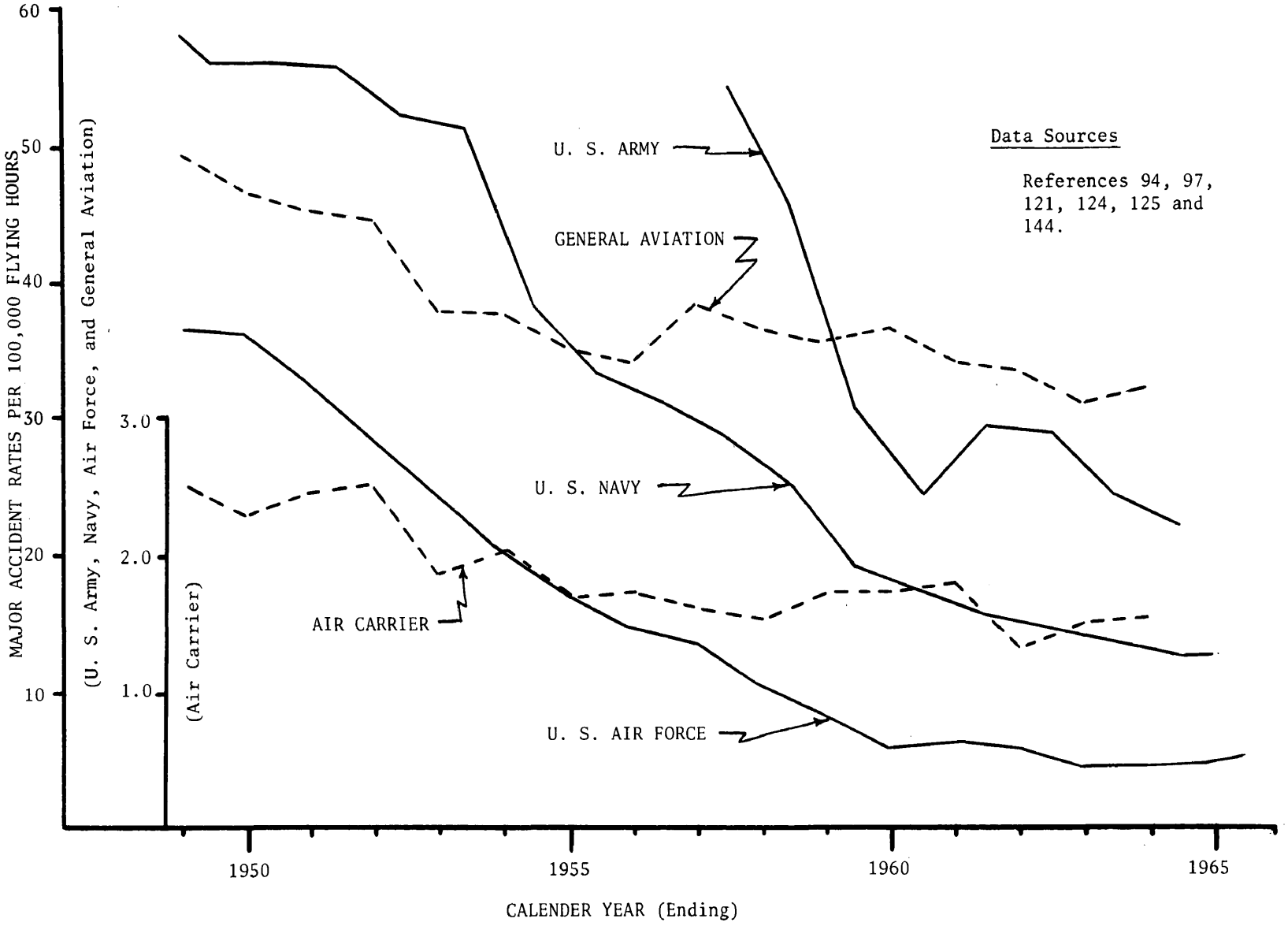

Fig. 2.--MAJOR ACCIDENT RATES-AVIATION

time span depicted in Figure 2. These changes have occurred often enough that analysts have been discouraged from trying to continually replot data to some common accident definition baseline (144).

Nevertheless, at least two major points can be concluded from Figure 2.

1) In the military, a marked decrease in slope in major accident rates occurred in the early to mid 1950's. The phasing of these declines shows the U. S. Air Force (USAF) to lead the Navy by two to three years. The Navy then appears to have led the Army by three to four years; although Army data was not maintained with any reasonable accuracy before 1958.

2) The records of certificated air carriers and general aviation indicate a relatively level accident trend. However, in air carrier aviation, one can observe the extremely rare nature of the events that can markedly cloud any statistical analyses.

It is suggested therefore, that in some segments of aviation, significant improvements have been made towards decreasing major accident rates. As was described in Chapter II, the USAF assumed a distinct, professional, spe-

cialist approach to accident prevention beginning around 1950; to be followed by the Navy and Army in subsequent years. There has been no similar specific approach definable in civil aviation manufacturing or operations area as a whole. Thus the curves in Figure 2, strongly suggest there may be something observable resulting from the specialist approach to safety.

Yet, there are equally strong indicators that these improvements have diminished in slope. This can be seen by direct observation of Figure 2 or by examining what the data means in the sense of an accident prevention learning curve.

As described by Morrison, learning curve theory may be applied to the understanding of aircraft accident prevention (135). In traditional use of learning curve theory pertaining to production costs, the curve may be represented mathematically by equation $y = ax^b$ where y is the cost of the x^{th} unit produced; a is the cost of the first unit produced; and b, a number less than zero (a negative number) is a parameter based on the complexity of the pro-

---

For complete delineation of accident terminology, the reader is advised to review regulations of the military services or the Civil Aeronautics Board, References 93, 101, 107, and 111.

duct.

In the safety sense, y would become the accident rate at the x^{th} unit of time; a is the accident rate at time zero, and b continues to be negative number based not only on system complexity but also the characteristics of the accident prevention programs.

Provided b remains essentially a constant, this equation produces a linear relationship between the logarithms of x and y, given the equation log y = log a + b log x. This means that every time x (the number of time units) doubles, y (the accident rate) decreases by a constant factor. In other words, y is multiplied by a constant number less than 1 (but greater than 0). This multiplier is given the name of the "slope" of the learning curve, although this is not a slope in the pure mathematical sense. For example, a "90% curve" would mean that the accident rate would be 90% of that at the beginning of the period under consideration; the rate at the end of the fourth period would be 90% of that at the end of the second and so forth. This gives the logical result that lacking a major breakthrough, each succeeding improvement in accident rate is a little more difficult to achieve than the last one.

Interestingly enough, Morrison was able to show a marked change in the slope of the learning curve for Naval Aviation safety from a slope of 87% between 1946 and 1955 to 39% between 1954 and 1965. As noted earlier, this was the period of safety specialization in the Navy. He also showed a relatively flat (82%) curve for general aviation between 1946 and 1962. Both of these areas revealed amazingly good correlation with learning curve theory in that the data had minimal scatter when represented on a log log plot. The correlation was not as good for commercial aviation, most likely due to the aforementioned relatively rare nature of their accidents compared to the other fields.

Figure 3 expands on the idea presented by Morrison by plotting Air Force and Army data as well as that from the Navy. Note that dual log scales are used on the ordinate to provide clarity of the log log plot between Air Force data and that of the Army and Navy. Thus the reader is cautioned not to interpret that ordinate as the Air Force accident rates being an order of magnitude above that of the other Services.

Observe in Figure 3 that the Air Force learning curve also reveals a marked improvement in slope, in this case around 1950-51. However, also observe the discontinuities

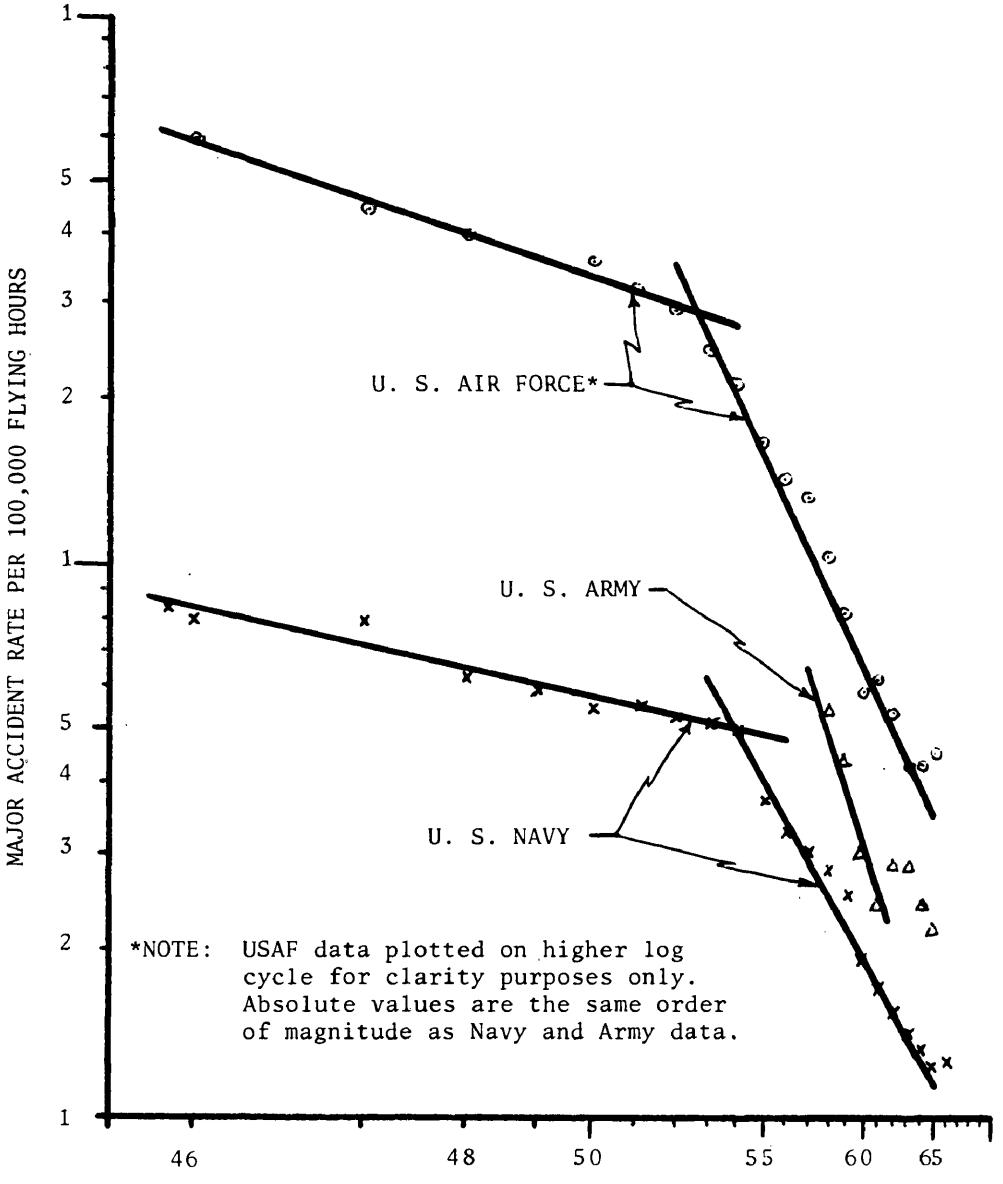

Fig. 3.--ACCIDENT PREVENTION IMPROVEMENT

in the USAF curve beginning in 1960 which correspond to the flattening of the corresponding curve shown in Figure 2. A similar change is seen in the Army curve in 61-64. A hint of a change also appears in Navy data in 65-66.

Therefore, the leveling trend could be accepted as the results of a normal learning curve process or a marked change in the complexity of the aerospace system, or both. The impact of the Vietnam war operations has certainly clouded this picture over the past two to three years, but the USAF leveling trend was certainly seen prior to large scale operations in Southeast Asia.

These data simply reinforce the theory that major improvements in safety have been made, probably through the use of the safety officer concept in military aviation operations. They also emphasize, however, that new breakthroughs will be required to continue a downward trend in accident history. This could conceivably demand more system safety effort at the development end of the life cycle spectrum.

There are no unclassified data comparable to Figure 2 concerning missiles - the other major part of the aerospace safety picture. However, as has been shown missile development and operations have had a major role in shaping

safety policy in the aerospace community. Our space vehicle operations have not been the subject of significant safety statistical analyses to date.

Assessment of Safety Tasks

Independent of the meaning of statistical records just described, a prime management requirement is to be able to measure the current productiveness of its workers (41). Thus, in matters of safety, there is a requirement to measure the results of prevention effort. It is difficult if not impossible to describe a system function for which some standards are not essential. Without them, how is a manager to gauge the effectiveness of his decisions in terms of value received for expenditure of funds or resources?

A problem occurs in safety management because no one has ever devised a method to measure specific accidents that have been prevented due to some specific safety act or group of acts. The author has hypothesized a method in this respect in the past using an information theory approach (45:15). Practically speaking, however, this has not been accomplished to date.

Numerous case histories of incidents could be studied that were prevented from being accidents by some specific

safety action. For example, a young Marine pilot once described to the author an experience over the center of a large metropolitan area, where his airplane (an F8 Crusader) stalled in a vertical climb. By grabbing the thigh portion of his flight suit with both hands, to resist the impulse to move the stick, the pilot recovered from the gyration. He had received a safety briefing along these lines for stall/spin recovery a few days earlier. The first flight of the XB-70 involved only a landing gear incident instead of major accident because a requirement on the gear suggested during a combined designer-safety engineer analysis of the gear's retraction sequencing. It was a matter of including a protective sequence switch that would preclude the main gear retraction until it had rotated to a certain position, thereby ensuring adequate clearance to enter the wheel well (139). Most experienced safety practitioners have a file of such cases in their memory if nowhere else. They could become "measurements" of safety task performance if properly documented.

Fortunately, there are other techniques of task assessment besides numerical evaluation. Most of these find their heritage in management technology. First, there is the method of measurement associated with management by ob-

jectives or goals management (41). This entails simply a set of words established at the initiation of a program describing what the contractor plans to do to accomplish a given objective. At appropriate evaluation intervals, the customer in his own best judgment using whatever similar activity in the past is available to him, "scores" how the contractor performs the task. The customer may secure an outside agency to provide assistance in this judgment if he has reservations about his own capabilities.

A similar approach might be termed the "check list compliance" concept. At the beginning of a program, a specific safety check list can be presented by the customer to the contractor based on the best available knowledge at that time, for example, in design safety. Then as the system drawings are received, they can be literally evaluated and checked off against this list. This is just an expansion of the basic specification or design handbook compliance approach - or is it? Specification type documents tend to be subsystem or single problem area oriented whereas safety is a total system overview approach.

Another form of measurement might involve the safety inspection techniques. It could be used to evaluate compliance with procedures presumably in writing pertaining to

accident prevention. Still a judgment factor, it has a rather well known heritage in both civil and military circles.

Measurement of Safety

Observe that until now, no mention has been made of methods to quantitatively measure the absolute level of safety per se. Consider first the matter of prediction of the level of safety. Someone may choose to investigate and summate the probability of catastrophic failure from a given point of view such as material failure. For reasons previously described in Chapter IV, however, any method of this type has severe limitations. Suffice to say here, one should not confuse a relative measurement, which is all that can be done with probability statistics and safety, with management's plea for an absolute measure of accident prevention efforts.

Nor does the concept of waiting for the final accident statistics to be tallied have practical significance although they can be a measure of safety performance. The five to ten year time element that transpires between system conception, development, test, and operational use precludes establishment of reasonably stable conditions to re-

late results to any specific future prevention effort.

Some authors press the point that:

> The history of science has adequately established that rapid progress is made when concepts being dealt with are reduced to quantitative terms which can be predicted, measured, evaluated, and finally communicated (130).

However, does history indicate what happens when only a part of the whole is reduced to quantitative terms without reasonable recognition thereof? One suspicions that the resultant communications might become garbled and lead to worse decisions than had simply human judgment been used alone. The optimum solution, lies in human judgment plus what the numbers can tell with their limitations fully recognized.

A case in point relative to prediction and measurement of safety/prevention effort rests with the "fault tree" concept. This is a recent failure mode and effects analysis technique so named because of the branch-like appearance of its graphical presentation. It combines the principles of set theory, Boolean algebra, statistical probability, and computer technology with system knowledge and safety lessons of the past (65, 66, 67, 73, 83). The fault tree technique has many good features, the main one being an improved method to visually display intersystem failure ef-

fects. Its shortcomings are highlighted by the inability to treat the human variable quantitatively as described earlier (Supra p 63).

Also, as a model of total system safety, the fault tree requires so many simplifications, including eliminations of so called low probability failures, that the model's predictive ability for the whole is seriously open to question. Add the time dependency of whatever failure rates are known, and the practice of numerology, as Grose put it, could indeed become rampant. Grose wrote:

> Numerology . . . a system occultism (hidden, secret, or beyond human understanding) involving divination (the practice of trying to foretell the future by mysterious means) by numbers (8:119).

In terms of probability theory, accidents are indeed rare events. Therefore, extreme caution must be used in applying fault tree or any statistical analysis technique to the assessment of safety.

If prediction of safety becomes difficult, it becomes virtually impossible to demonstrate safety in the scientific sense. To do so would suggest provision of prevention equipment and techniques to the experimental group and not to the control group. Our society as well as the control group would probably not appreciate this approach. Simu-

lation methods might be attempted involving maintenance mockups, flight simulators, or full scale aircraft to a degree; the difference between training and experimentation often being a matter of planning and instrumentation. However, human stress factors would severely cloud the accuracy of this method to the point of its being highly questionable.

Another way to describe this entire situation is to draw the philosophical distinction between an accident prevention attitude and the desire for safety measurement and control. In accident prevention, the goal is unequivocally zero accidents consistent with cost, schedule and mission performance. Its methodology includes attempted control of all causal factors including those that cannot be precisely forecast because of very practical limitations in knowledge. The safety measurement approach, on the other hand, leans towards the ivory tower environment. Known data is used to describe the potential hazard areas to be covered, hence, yielding presumed control of all problems. In the real world unfortunately, these data are incomplete to a marked degree; and what is available, is distressingly disorganized.

There is a story which illustrates this point particu-

larly well. It involves the man crawling on his hands and knees one night in the street outside a local pub. When asked what he was doing by series of people exiting the bar, he replied, "I'm looking for a quarter I lost." Soon he had a number of fellow inebriates on their hands and knees helping him.

Finally, a more rational soul came along and asked the man what he and his friends were doing. He received the same reply as before, but then asked "Where did you lose the quarter?" The man replied in a rather matter of fact way, "down the street about a half a block."

"For heaven's sake, man, why are you looking here then?" asked the latest inquirer. "Simple," said our hero, "the light is better."

One cannot help but feel that much of today's emphasis on mathematical solutions to problems is a subconscious desire to oversimplify complex situations with exact scientific approaches . . . work only where the light is better. In the final analysis, rigid scientific measurement of safety per se is impossible since safety is an abstract quantity. Like other abstractions, however, its components can be evaluated which, in this case, are the tasks known to produce a safer system. They are judged on the basis of X

people with Y skills performing Z tasks according to an agreed-to plan within a given organizational framework. These components cannot be tallied with any degree of accuracy within today's state of the art because of their extreme complexity. As safety becomes a better defined segment of management, and management technology itself becomes more measureable, perhaps safety's role will then be delineated in more quantitative terms.

CHAPTER VII

COMMUNICATION OF SAFETY INFORMATION

Safety Information Flow

The flow of information is vital to the systems management process (14:73-88). It can thus be considered vital to the accident prevention process. This can be best understood by recalling the known precedent concept described previously in Chapter II. 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, you might not live long enough to make them all yourself."*

When viewed in a communicative safety information flow process, Figure 4, known precedent becomes a significant reference point. Observe that it initially determines hardware safety characteristics and procedures for a given air vehicle under development. These characteristics and procedures are then refined, tested, and put into operation. Should they result in an accident free function, the as-

*This phrase was utilized for many years by the Flight Safety Foundation on its stationery and invoked considerable comment and requoting. The original author-philosopher is unknown.

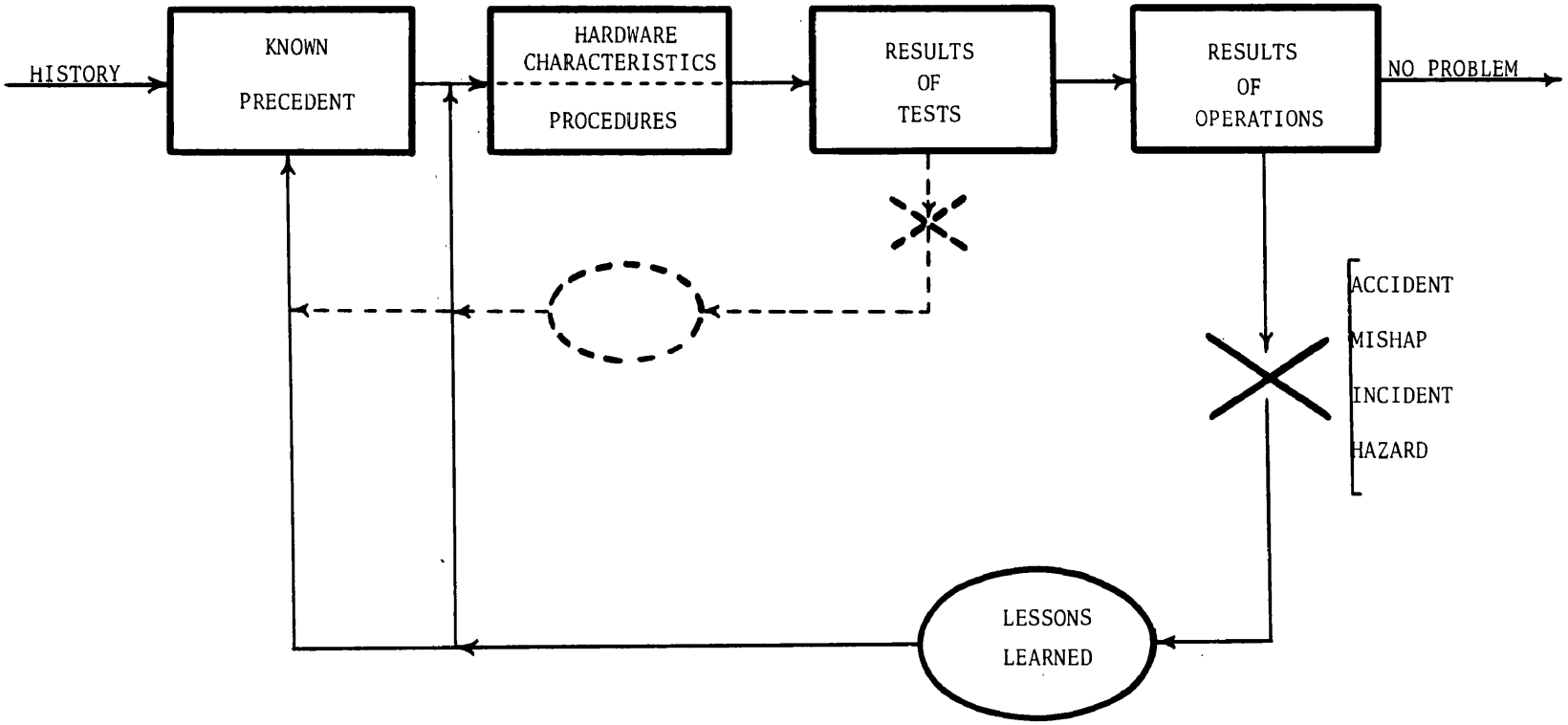

Fig. 4.--COMMUNICATIVE SAFETY INFORMATION FLOW PROCESS

sumption 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 either resulting from tests or operations. 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 5) 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 performance, cost and schedule; 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 timing) permit, the original requirements might be changed. Interim solutions might be necessary as was the case in flight re-

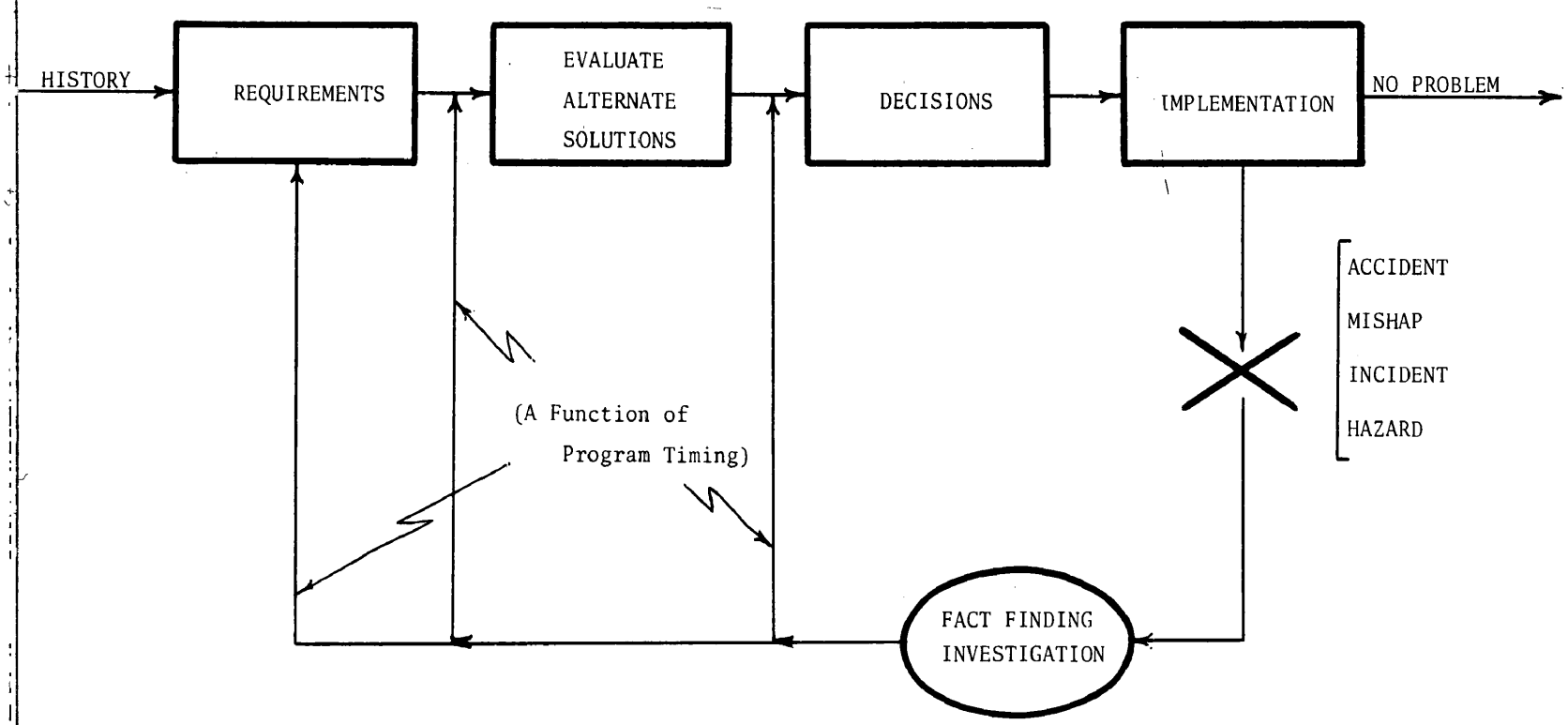

Fig. 5.--MANAGEMENT UTILIZATION OF SAFETY INFORMATION

strictions imposed on the Electra after two fatal accidents early in its career (15:177). In other cases, new solutions might be required. Finally, the case might reveal factors which have already been evaluated as much as is practical and the decision process essentially results immediately. The trick is to know which path to take.

The foregoing discussion emphasizes the dynamics and importance of safety information flow. Indeed, 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 board findings. Unfortunately, figures 4 and 5 are gross oversimplifications of what one might encounter in a specific set of circumstances. This is better understood by examining what comprises safety information and examining the sources thereof.

Types of Safety Information

In the general sense, safety information is any communication of knowledge of value to the worker 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.

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, regulations, 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. Just how much so 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. An example of this would be the need to understand spectrometric oil analysis techniques to provide

a recommendation as to their value in predicting failure of lubricated engine parts (59). For this task, knowledge would have to be present of in maintenance procedures, properties of materials, and power plant design.

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. He, like all men, will have to recognize his limits in storing information in retrievable form and use other people and artificial data retrieval systems as the need arises.

Safety Information Sources

During a three year period, (1962-1964) the author surveyed sources of safety information by interviews and by means of a questionnaire (45, 80, 132). The result was a compilation of data from fifty-nine groups representing thirteen manufacturers, eleven safety centers, ten documentation centers and lesser numbers of airlines, professional societies, and trade associations. Since this was an unfunded independent research project, no attempt was made to follow up the original communications, or perform a compre-

hensive statistical analysis of the results. However, aerospace safety information data sheets were prepared relating each organization, its mission/purpose, the person to whom inquiries should be addressed, and remarks pertaining to the detailed content of the written response and/or oral survey. These sheets were then provided to those organizations who cooperated in the study.

Review of the survey responses individually and collectively revealed a number of interesting points.

Lack of Single Comprehensive Safety Information Source

All organizations, including those designated "safety centers," emphasize their own mission requirements. This occurs to the extent that no single group has a good grasp of the entire aerospace safety information picture. This limited approach applies even within aviation activities. For example, an organization knowledgeable in commercial aviation would rarely have an appreciation for valuable information available, say, for tactical aircraft.

Conversely, there were numerous cases where the military services were not aware of valuable safety information published through civil aviation sources.

There are bona fide reasons for this somewhat re-

stricted attitude towards safety information. Not the least of these reasons is the aforementioned large total volume and scope of data. Particularly unfortunate, however, is the little appreciation exhibited within different facets of the aerospace community for the powerful influence of inter-group safety information monitoring, exchange, or whatever it may be called.

Response to each group's own operational commitment has become the first and in many cases the only priority. This means that if technical files or a library are maintained by a given safety organization, its few personnel occupy virtually all of their time searching in-house answers to in-house problems. This precludes becoming familiar or effecting rapport with outside agencies that may have faced (and already solved) the very problem that set them to the chase.

When one wants to know what goes on outside his own world, he must have time and funds allocated to investigate or research. Very little of this thinking pertaining to information storage and retrieval concepts was observed by the author in the course of the survey referenced earlier.

It is firmly believed that inadequate safety information exchange was contributory to the lack of trans-

mission of existing knowledge in the so-called jet upset problem. It also may have been present in recent accidents encountered by the Boeing 727 (81).

A current and future tragedy in this respect seems to be in the field of general aviation. It is seriously questioned that any general aviation safety source is aware of the tremendous amounts of untapped fundamental prevention knowledge available elsewhere.

It was also apparent from the survey, that the requirement for indexing of data is not fully appreciated. This included an absolute lack of uniformity in indexing - even among safety publications of similar nature (eg various USAF Command Safety magazines.) Furthermore, the depth of indexing left much to be desired. Only a handful of groups chose to go beyond two levels of subject indexing. Without deep indexing, information search is so time consuming as to be impractical.

Although they have elaborate information storage and retrieval systems, documentation centers such as Defense Documentation Center (formerly ASTIA) have serious limitations in solving safety information problems. First of all, they usually store only "published" material which constitutes relatively small part of the total safety in-

formation package. Secondly, and far more important, their scope of operation is so large, that even with thousands of words in their index, they cannot produce the detailed response required in system safety work. Their descriptors become too ambiguous when applied to a specific discipline.

If a given discipline chooses to organize its body of knowledge to accelerate advancement of their phase of the total state of the art, the members of that discipline must personally participate and cooperate in the storage and retrieval process. This is not something that can be delegated to a documentation center or a secretary.

True, documentation concepts are best understood and implemented to a degree by documentation trained personnel; and there are many paper work functions that can be delegated to a clerk-typist. However, 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 (80).

The Nature of the Stored Accident Data

No discussion of safety information would be complete without commenting on the data stored as a direct result of accidents. Millions of IBM cards are in existence to tell

what happened during a given period of accident exposure. Examination of the accident code books reflect a continuing effort to include material on why the accident happened, although much of this gets lost on the way from the investigating board to the key punch operator.

What is known, however, of the prevention activity resulting from accidents? Are the accident board's recommendations analyzed through automatic data processing or other means, except occasionally on a single case? Does anyone really know where the accident lessons go after the vehicle pieces were picked up? The answers to these questions are all negative. Actually, an entire new aspect of accident data recording is needed in the future if the loop is ever to be tightened between accidents and the prevention thereof. This point will be amplified in the last chapter.

It can be concluded that the system safety discipline has been trying to mature in a period of a total 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 VIII

ANATOMY OF SYSTEM SAFETY

Anatomy of An Accident

Several years ago, Chapanis described an automobile accident that provides a most important lesson, even to the layman in safety. He wrote:

> 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 nighttime; there is a skim of snow on the ground, and the tires on our victim's car are smooth. In rounding a poorly banked curve at excessive speed, the right front tire blows out, the car leaves the road and is demolished (115).

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

Of course this entire story could have its counterpart in aviation. Let us assume the domestic scene and the man's immediate actions were the same. Then assume instead of smooth tires, the airplane simply may not have been maintained properly. Instead of rounding a poorly banked turn at excessive speed, it could have been an excessively tight

turning approach to landing on a runway that had a six inch lip between the approach end soil and concrete. The initial physical damage would have been a blown tire once again; but this time due to a premature touchdown. The end result being a demolished vehicle completes the analogy.

Aerospace accident causal factors today are classified personnel error, material factor, weather, facilities, design, maintenance, training, supervision, and administration. Many of these were present in the cases described above.

Arguments sometime ensue as to which factor should be applied in the investigating board finding. These occur because of three conflicting approaches to the recording of accident information.

Approached in the pure accident prevention sense, delineation of all parts of the sequence of event of the accident is important. This is based on the principle that elimination of any one of the parts would break the accident chain. From the viewpoint of practical limits in quantity of data processing, however, providing some semblance of "priority" to causal factors is deemed essential (194). This is accomplished by the determination of "primary" cause as differentiated from contributory cause(s), or by

finding the "most probable" cause.

The finding of the cause is required for social justice in cases where tort litigation is involved. This should not be confused though, with the basic purpose of aerospace accident investigations that is defined by all government agencies as solely for accident prevention purposes (45). In any event, classification of accident findings remain descriptive man-made judgments about what happened in an accident.

To have an accident preventive 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 (82). The what should be done is often indicated in the accident report through the usual recommendations. However, classifications or analyses are rarely made of recommendations from accident boards, that is, 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 labeled by the investigating board 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 education or replacement. Or, as indicated earlier, the decision might be to live with the problem. These choices are not the prerogative of an investigating board since they may not have all facts available on the consequences of implementing a recommendation. A board should not be discouraged from pointing the way to corrective action as

they see it. However, a summary of only board findings, or even their 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 (89).

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 his conscience that some aircraft or some person did not die needlessly while time was being consumed in protracted decision and implementation processing? How does one intelligently establish or evaluate a standard for management decision and implementation if he does not fully know what had happened in the past?

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 aerospace safety, the man, the machine, and the media (environment) have been described as factors in aerospace accident causation and consequently, factors in accident prevention (129). Just why this was emphasized rather than the three E approach (Supra p 79), has never been clearly understood. In any event and based on the discussion immediately preceeding this paragraph, it would seem management is an identifiable fourth element in accident prevention of equal or superior importance to the other M's. Combined they begin to form a model for system safety as illustrated in Figure 6.

As implied before, management's role may be difficult to delineate 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 the other factors can be examined in the most efficient manner.

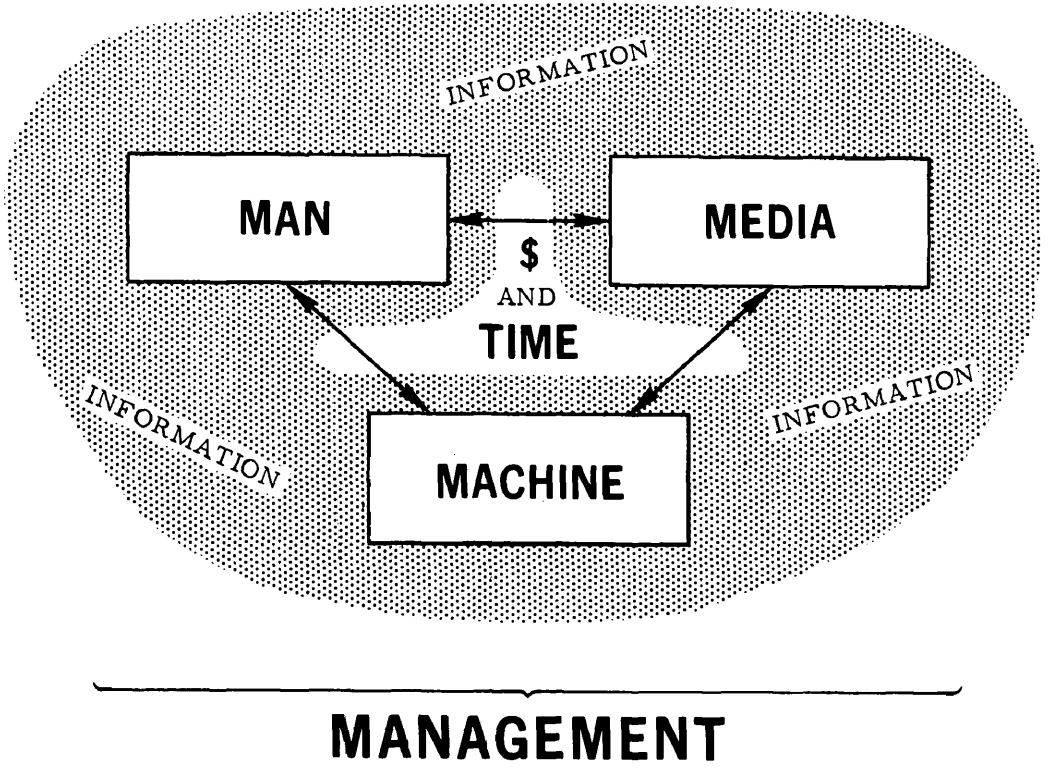

Fig. 6--FACTORS IN SYSTEM SAFETY

Thus, Figure 6 is constructed to show such an overview position for management. It also displays, by means of the arrows, the interrelationships usually found in the traditional accident factors and the bias effects of costs and/or schedules throughout the entire process.

Consider a comprehensive actual case to illustrate this "anatomy" of safety discussion. A commercial jet airliner crashed on approach to an airport under deteriorating weather conditions during hours of darkness. It actually contacted the ground in a relatively level attitude at an altitude below that of the airport it was approaching. The CAB accident report listed the probable cause as failure of the pilot to adequately monitor the altimeters during the approach (33).

The investigation also revealed the following facts:

1) The pilot in the left seat who was flying the aircraft had only 35 hours in the type of aircraft that crashed. His record showed no other jet transport-time although he had been a commercial airline pilot for many years.

2) The pilot in the right seat was also highly experienced in total flying hours, but had only 225 hours in the type of aircraft that crashed. Simi-

larly, his record revealed minimal flight time in other jet aircraft although he was a commercial pilot of long standing. He was functioning as check pilot in accordance with Federal Air Regulations applicable to the other man's qualifications.

3) The enroute planning and courses flown on the ill fated flight were marked by numerous shortcuts aimed at "beating" the approaching weather front to the field.

4) The aircraft was relatively new model with markedly higher sink rate characteristics with reduction in power in the landing configuration compared to other aircraft flown by either pilot.

5) Abnormally high sink rate was present in the subject accident until just a few seconds prior to impact.

6) One accident occurred prior to this one and two within a few months afterwards involving the same type aircraft in which high sink rate in the landing configuration was actually or potentially involved during the final minutes of flight.

7) Sink rate characteristics of this airplane were

not fully appreciated or described as a particular caution area in pilot's flight handbooks prior to the accident.

8) The weather was indeed highly restrictive to landing visibility but in a more or less intermittent manner throughout the approach.

9) The terrain over which the landing pattern was flown was highly conducive to optical illusions.

10) The altimeter was of a type known to have produced interpretation errors in the past although it was the best available instrument.

What, then, were the factors in system safety revealed in this accident?

Man: the questionable although legal proficiency qualifications; also the psychological factors that prompted the pilot's decision to "beat" the weather to the field.

Machine: its high sink rate characteristics as well as the altimeter configuration.

Media: the weather, the darkness, and the terrain features.

Management: the basic schedule decision process in-

volving especially the training program for new aircraft.

Time: the apparent need to maintain particular flight schedules.

Cost: the price paid for training and schedule adherence?

Information: accident potential of the sink rate characteristic.

Also, what steps were taken to preclude this type accident in the future? Unfortunately, these are not chronicled in complete and/or readily available form as of this writing. The accident report noted revised handbook and training procedures and some minor changes in altimeter use. Other than that, one would gather the main lesson was to simply advise pilots to monitor the altimeter on approach more carefully.

Obviously, there were far more significant elements apparent in the anatomy of this accident than those identified by the probable cause. For example, some program should be instituted to better highlight unique flight characteristics of a new model aircraft and assure appropriate safety training related thereto before accidents occur. Unless such elements are searched for, and acted

upon in some improved systematic way, the real lessons of this accident will be lost in the confusion of the future.*

The Implementation Process and Man

In considering implementation of prevention measures, one must also examine the matter of conscience. Lederer's "Perspectives in Air Safety" is considered mandatory reading on this vital point (71:10). He first cites Lord Moulton, a famous British jurist, in an article published in 1912 as follows:

> I ask you to follow me in examining the three great domains of human action. First comes the domain of positive law, where our actions are prescribed by laws . . . which must be obeyed. Next comes the domain of free choice, which includes all those actions to which we claim and enjoy complete freedom.
>
> But between these two there is a third large and important domain in which there rules neither positive law nor absolute freedom. In this domain there is no law which inexorably determines our course of action, and yet we feel that we are not free to choose as we would. This is the domain of obedience to the unenforceable, the obedience of a man to that which he cannot be forced to obey.
>
> And to my mind, the real greatness of a nation, its true civilization, is measured by the extent of this law of obedience to the unenforceable. It measures the extent to which the nation trusts its citizens;

*The author had occasion to present this discussion to an international safety meeting in Oct. 66. It is happily reported the concept was received with high interest (82).

> and its existence and area testify to the way they behave in response to that trust . . . .
>
> The true measure of a nation's greatness is the extent to which the individuals composing the nation can be trusted to obey self-imposing law.

What is fundamental accident prevention but self imposing law as described by Lord Moulton?

Then Lederer posed "The Engineer's Dilemma: Conscience vs. Economics," in which a multitude of variables affecting conscience are indicated. Professional engineers, subscribe to Canons of Ethics which includes their safety responsibility in clear terms (64). 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 in selling safety today. On one hand is the diminishing safety improvement rate in most areas as discussed earlier and illustrated in Figure 2. This means accident rate improvements in our increasingly complex society will continue to be technically more difficult (29).

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 behavioral reaction on the part of a manager or anyone else to whom something must be "sold."

As explained by Anshen:

> Consider the established behavior pattern is A. The would-be innovator says that B is a better way to behave. Those who are behaving in pattern A deny the validity of the innovator's assertion . . . and even given proof that B is better, they may not accept the evidence . . . . What is the reason for this? . . . (most likely) that change carries with it a threat of insecurity . . . successful change might suggest that those who have been running to show in the old way lack either the brains or the initiative to seek improvement (127).

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 some-

thing - an accident - did not happen.

Anshen goes on to explain the need to create the atmosphere for the change which in turn leads to the requirement for a specific strategy. He listed thirteen steps of innovation to be followed by any innovator, as shown in Table 6.

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.

Whither Safety

Aerospace Safety has approached a series of intersections as this document is completed. It is fresh from remarkable progress in having safety become contractually required 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 do 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

TABLE 6

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 other 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 officers . . . 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.

TABLE----Continued

11. Use organization 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.

mistakes have included a super-dependency on statistical analysis techniques and a neglect to appreciate the contributions to reliability objectives available from other disciplines (8).

Another choice ahead rests in the direction in which safety will expand . . . and it most surely will. The USAF, organizationally and through regulations, has shown a strong trend towards integrating flight, missile, ground (traffic), nuclear and explosive safety activities. If history repeats itself here, the other military services will follow suit.

In the civilian side of the aerospace community, there is not only the influence of Mission SAFETY - 70 but also the recent formation of a federal Department of Transportation. This will merge rail, highway, and aviation functions, heretofore found in several Federal departments and agencies. Included is a proposed National Transportation' Safety Board which will function in a staff capacity to the Secretary of Transportation and have reporting to it such objective activities as the current CAB Bureau to Safety (26, 128).

The industrial safety field continues to function somewhat in between the USAF and transportation concepts. It

too, however, is feeling the impact of the system approach to safety (48-51, 60). It should only be a matter of time before all of the safeties will be more closely aligned professionally than they are today.

Conclusions and Recommendations

This thesis has examined the role of system safety in aerospace management. It has identified a relatively young and growing discipline involving accident prevention; a discipline that has been applied in both military and civilian systems effectiveness and systems management concepts. As characteristic of youth in any form however, one finds a number of misunderstandings and conflicts with other activities boasting longer histories. Thus, it is not surprising that:

1) The semantics of safety has led to the development of new meanings for the term.
2) The dynamics of management technology as well as safety has introduced new concepts of system effectiveness. One encounters therein matrix organizations, staff-line relationships and the cost benefit aspects of safety which require careful understanding for efficient use of personnel and

resources.

3) Closely allied with (2) is the recognized difficulty in measuring accident prevention efforts . . . measurements which are needed for scientific management or safety.

4) Accident prevention communications is awakening as a sleeping giant, no longer to be relegated to a simple informal "passing of the word" from one generation to another. It is becoming too expensive to tolerate such luxuries because of both direct accident cost and litigation.

5) Broadening of the depth of inquiry into accident causal factors and the management pathways for effecting corrective action is a sign of times in the evolution from after-the-fact thinking to accident prevention.

There are no "school" solutions to these problems; nor are there single steps that will suddenly transform the aerospace environment to one that is "safe" within the dictionary meaning of the term.

For example, one could provide a good case for the safety specialist to always occupy a specific position within management, performing both staff and line tasks such as

those noted in Chapter V. However, the safety specialist is only one member of the team. His contributions could be accomplished by others if certain types of personnel, organizational structure, training, time and funds were made available. In any reasonable size organization, however, this will become a full time activity.

In the author's opinion, the most profound philosophy ever offered pertaining to safety improvement was presented by I. Irving Pinkel of NASA when he wrote:

> 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 (146).

Within this context, several recommendations for further study and/or action are made based on thoughts developed in this thesis:

1) A need exists to introduce more of today's accident prevention philosophy and methodology into undergraduate degree curricula of many disciplines; indeed, possibly an undergraduate degree program for safety itself.

2) A better understanding is required of the economics of safety to provide better data for management decisions (tradeoffs) relative to accident prevention. A research program is indicated.

3) System effectiveness should be better defined through closer integration of tasks performed by the "ility" disciplines. Within the military or other "customer" areas, this would logically entail a cover specification for existing specifications in safety, reliability, maintainability, human factors, value engineering and quality control.

4) A safety technical information center should be established using modern data storage and retrieval techniques. Basic classification of the information should follow the safety task structure since any good system will be user oriented.

5) A complete safety information flow model should be developed to further examine the variables involved in accident causation/prevention. Basic research should be undertaken to develop some method of quantifying such information.

In conclusion, General "Smokey" Caldara, past Director

of Aerospace Safety in the USAF, and current President of the Flight Safety Foundation seemed to have the right words to express today's realization about safety when he said:

> I think it's mandatory that there is no single, simple key for safety - no grand or magic formula to insure that everyone involved in activity does what he is supposed to do, the way he is supposed to do it. Safety must be the product of many people, dynamic - not static, the sum of many activities (30).

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

BIBLIOGRAPHY

Books

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

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

3) Barton, J. A. Annals of Reliability and Maintainability. "Operational Safety Analysis Techniques." Vol. 4. Washington: Spartan Books, 1965.

4) Blake, R. P. Industrial Safety. 3rd ed. Englewood, New Jersey: Prentice Hall, 1964.

5) Craine, Maj. Robert L. Annals of Reliability and Maintainability. "Safety Management in Aircraft Systems Developments, A Progress Report." Vol. 4. Washington: Spartan Books, July 1965.

6) Drucker, P. F. The Practice of Management. New York: Harper, 1954.

7) Fayol, Henri. General and Industrial Management. London: Pitman, 1965.

8) Grose, Vernon S. Annals of Reliability and Maintainability. "Reliability Can Be Predicted (A Negative Position)." Vol. 4. Washington D. C.: Spartan Books, July 1965.

9) Haddon, W., Suchman, E. A., and Klein, D. Towards a Science of Accident Research. New York: Harper & Row, 1965.

10) Hamilton, Col. R. M., and Newton, Capt. R. W. Annals of Reliability and Maintainability. "The Army Evaluation of MIL-S-58077, and Those Agencies Involved in Its Implementation." Vol. 4. Washington D. C.: Spartan Books, July 1965.

11) Hancey, Carl. Annals of Reliability and Maintainability. "Safety Education and the Management Process." Vol. 4. Washington D. C.: Spartan Books, July 1965.

12) Heinrich, H. W. Industrial Accident Prevention. New York: McGraw-Hill, 1959.

13) Jacobs, H. H., et al. Behavioral Approaches to Accident Research. New York: Gamis & Harris, 1961.

14) Johnson, R. A., Kast, F. E., and Rosenzweig, J. E. The Theory and Management of Systems. New York: McGraw-Hill, 1963.

15) Kepner, C. H. The Rational Manager: A Systematic Approach to Problem Solving and Decision Making. New York: McGraw-Hill, 1965.

16) Koontz, H. and O'Donnel, C. Principles of Management. 3rd ed. New York: McGraw-Hill, 1964.

17) Likert, Rensis. New Patterns of Management. New York: McGraw-Hill, 1961.

18) Longnecker, J. G. Principles of Management & Organizational Behavior. Columbus: Merrill Books, 1964.

19) Newman, W. H. and Summer, C. E. The Process of Management. Englewood, New Jersey: Prentice-Hall, 1961.

20) Odiorne, G. S. How Managers Make Things Happen. Englewood Cliffs, New Jersey: Prentice-Hall, 1961.

21) Peck, M. J. and Scherer, F. M., The Weapon Acquisition Process. Boston: Harvard Business School, 1962.

22) Ruff, George G. Annals of Reliability and Maintainability. "The System Safety Engineering Plan (SSEP), and Integration Considerations in the Implementation Process." Vol. 4. Washington: Spartan Books, July 1965.

23) Simonds, R. H. and Grimaldi, J. V. Safety Management. Homewood, Illinois: R. D. Irwin, Inc., 1948.

24) Taylor, F. W. Scientific Management. New York: Harper & Row 1947.

25) Woodson, W. E. and Conover, D. W. Human Engineering Guide for Equipment Designers. 2nd ed. Berkeley: California Press, 1964.

Articles and Periodicals

26) Anon. "How Will a Department of Transportation Really Work?" Aviation Week and Space Technology, April 4, 1966.

27) Bertrandias, Maj. Gen. V. E. "Flight Safety Research," IAS Aeronautical Engineering Review, April 1951.

28) Borden, Norman E., Jr. "The First Eleven," Aerospace Safety, May 1964.

29) Caldara, Maj. Gen. (Ret) Joseph D. "The Diminishing Safety Improvement Rate," Alumni Review, Aerospace Safety Division, Univ. of So. Calif., Fall 1964.

30) Caldara, Maj. Gen. (Ret) Joseph D. "What's Up Front Still Counts," Flight Safety Foundation, New York, N. Y., SEPT Cockpit, January 1965. (Remarks at the Eleventh ALPA Air Safety Forum, October 1964.)

31) Cohen, Jerry and Murphy, W. S. "Burn, Baby, Burn," Life Magazine, July 15, 1966.

32) Commerce Business Daily. March 25, 1966.

33) "Crew Monitoring Cited in 727 Crash," (CAB Accident Investigation Report), Aviation Week and Space Technology, October 24, 1966.

34) Griffith, Maj. Gen. Perry B. "The Safety of Combat Potential," Air University Quarterly Review, Reprinted by AF SBAMA, October 1962.

35) Harrison, G. R. "The Scientific Origins of Modern Engineering," MIT Technology Review, May 1964.

36) Hodapp, E. J., Jr. "Dyna Soar Safety Program," Aerospace Safety, December 1960.

37) Irvine, W. L. "System Safety," Aerospace Safety, June 1965.

38) Kohlheyer, Richard. "Purpose and Progress: 1966 Report," Hazard Prevention, Vol. 3, No. 5, April 1966. (Bulletin of the Aerospace System Safety Society.)

39) Layton, Cdr. D. M. "System Safety Specifications," Approach, August 1964.

40) Lederer, J. "Air Safety: A Study of Ethics, Economics and Attitudes," Flight Forum, Winter-Spring 1964, Connecticut General Life Insurance Co.

41) McConkey, D. D. "Judging Managerial Performance," Business Horizons, Vol. 7, No. 3, Fall 1964.

42) McFarland, H. S. "The Concept of Accident Prevention as a Basic Management Function," A.S.S.E. Journal, December 1963.

43) Medford, J. F. "1970 . . . ?" Hazard Prevention, February 1966. (Bulletin of the Aerospace System Safety Society.

44) Miller, C. O. "Aviation Law-Air Safety (A Symposium Report)," Alumni Review, Aerospace Safety Division, Univ. of So. Calif., Fall 1964.

45) Miller, C. O. "The Safety Information Challenge," A.S.S.E. Journal, September 1966. Originally presented at the 17th Annual Flight Safety Foundation Seminar, N. Y., October 15, 1964.

46) Miller, C. O. "Safety and Semantics," Alumni Review, Aerospace Safety Division, Univ. of So. Calif., Fall 1965.

47) Miller, C. O. "The Influence of Systems Engineering and Management on Aviation Products Liability," Aerospace Safety Division, Univ. of So. Calif., Astronautics & Aeronautics, September 1966.

48) Recht, J. L. "Systems Safety Analysis: An Introduction," National Safety News, December 1965.

49) Recht, J. L. "Systems Safety Analysis: Failure Mode & Effects," National Safety News, February 1966.

50) Recht, J. L. "Systems Safety Analysis: The Fault Tree," National Safety News, April 1966.

51) Recht, J. L. "Systems Safety Analysis: Error Rates and Costs," National Safety News, June 1966.

52) Robb, D. A. "Safety Is Not Just Common Sense - A Trial Lawyer's View," A.S.S.E. Journal, December 1965.

53) Ruff, George F. "Systems Approach and the Safety Concept," Hazard Prevention, Vol. 3, No. 3, Bulletin of the Aerospace Systems Safety Society, December 1965.

54) St. John, Lt. Col. John D. "I Got A Right," Aerospace Safety, November 1964.

55) Stieglitz, W. I. "Engineering For Safety," Aeronautical Engineering Review, February 1948.

56) Tarrants, W. B. "The Professional Development of the Safety Engineering Field," A.S.S.E. Journal, February 1965.

57) "The Flight Safety Officer," Flight Safety Focus, Flight Safety Committee, London (Heathrow) Airport, Middlesex, England, June 1966.

58) Tye, Walter. "Unresolved Civil Airworthiness Problems," British Air Registration Board, 1959. (IAS Preprint 59-135).

59) Ward, John M. "Spectrometric Oil Analysis," Approach, March 1965.

60) Wissner, I. E. "How System Safety Relates to Industrial Safety," National Safety News, May 1966.

Conference and Symposia Presentations

61) Barton, J. A. "Relationship and Contributions of the System Safety Concept to Cost and System Effectiveness," LTV Vought Aeronautics Div., Dallas, Texas. (Presented at the Fifth Annual Reliability & Maintainability Conference, New York, July 1966.)

62) Bush, P. S., Jr. "Aircraft Products Liability," Johnson & Higgins, New York. Presented at the Aviation Distributors and Manufacturers Convention, Grand Bahama Island, November 17, 1965.

63) Coie, J. Paul. "Systems Safety - Legal Aspects," Holman, Marion, Perkins, Coie & Stone. Presented at the Systems Safety Symposium, Seattle, Washington, June 1965.

64) Collins, Col. J. J. USAF, "Why System Safety and A Discussion of System Safety Standards," Missile Safety Division, Directorate of Aerospace Safety, Norton AFB, Calif. (As presented at the National Safety Congress, October 1965.)

65) Feutz, R. J. and Waldeck, T. A. "The Application of Fault Tree Analysis to Dynamic Systems," The Boeing Co., Presented at the Systems Safety Symposium, Seattle, Washington, 8-9 June 1965.

66) Hassl, D. B. "Advanced Concepts in Fault Tree Analysis," The Boeing Co., Presented at the Systems Safety Symposium, Seattle, Washington, 8-9 June 1965.

67) Kanda, K. "Concept of System Safety Mathematics," The Boeing Co., Presented at the Systems Safety Symposium, Seattle, Washington, 8-9 June 1965.

68) Kreindler, Lee S. "Tort Law & Aviation - for the Plaintiff," Presented at the Law-Safety Symposium, Univ. of So. Calif., Los Angeles, June 1964.

69) Lederer, J. "Reduction of Aircraft Accidents," Flight Safety Foundation, New York. Delivered to the Air Research and Development Command Safety Conference, Baltimore, Md. September 15, 1954.

70) Lederer, J. "Some Economic Factors in Air Transport Loss Prevention," Flight Safety Foundation, New York, N. Y. A Lecture at the International Air Transport Seminar, 27-31 March 1961.

71) Lederer, J. "Perspectives in Air Safety," Flight Safety Foundation, New York (Guggenheim Medal Award Lecture, ASME Aviation and Space Conference Washington, D. C. 1962).

72) Lockwood, Roger A. "Systems Safety Reliability's New Associate," Systems Safety Society, Los Angeles, Calif. Presented at the 3rd Annual Aerospace Reliability and Maintainability Conference, Washington, D. C., June 29, 1964.

73) Mearns, A. B. "Fault Tree Analysis: The Study of Unlikely Events in Complex Systems," Bell Telephone Laboratories. Presented at the Systems Safety Symposium, Seattle, Washington, 8-9 June 1965.

74) Miller, C. O. "Applying Lessons Learned from Accident Investigations to Design Through a Systems Safety Concept," Chance Vought Aircraft, Inc., Dallas. Presented at the Flight Safety Foundation Seminar, Santa Fe, New Mexico, November 1954.

75) Miller, C. O. "Design Systems Safety in Operation," Chance Vought Aircraft, Inc., Dallas. Presented at the Flight Safety Foundation Seminar, Taxco, Mexico, November 1955.

76) Miller, C. O. "The Role of Flight Safety Engineering in Aircraft Reliability and Effectiveness," Chance Vought Aircraft, Inc., Dallas. Presented at the first IAS Naval Aviation Meeting, San Diego, August 1957.

77) 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, 16 April 1962.

78) 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 9, 1963.

79) Miller, C. O. "Safety During System Effectiveness Effort . . . A Management or Engineering Cost Item?" Aerospace Safety Division, Univ. of So. Calif. Presented at the Eighth Navy-Industry Conference on Material Reliability, Washington, D. C., May 11, 1965.

80) Miller, C. O. "Current Safety Information Classification, Storage and Retrieval," Aerospace Safety Division, Univ. of So. Calif. Presented at the Systems Safety Symposium, Seattle, Washington, June 8, 1965.

81) Miller, C. O. "The Application of System Safety and Management to the Civil Air Carrier System," Institute of Aerospace Safety and Management, Univ. of So. Calif., (To be published in the Proceedings of the ALPA Air Safety Forum, October 1966.)

82) Miller, C. O. "The Dynamics of Accident Prevention Information," Institute of Aerospace Safety and Management, Univ. of So. Calif. Presented at the

CASI/AIAA CGASC Aviation Safety Meeting, Toronto, Canada, October 31, 1966.

83) Nagel, P. M. "A Monte Carlo Method to Compute Fault Tree Probabilities," The Boeing Co. Presented at the System Safety Symposium, Seattle, Washington, 8-9 June 1965.

84) Outlaw, E. C. "Design Safety and Material Reliability," Naval Aviation Safety Center, Presented at the Flight Safety Foundation International Seminar, Athens, Greece, November 1963.

85) 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 11, 1965.

86) Robbins, Jay T. "System Safety Implementation Problems," Directorate of Aerospace Safety, Norton AFB, California. Presented at Systems Safety Symposium Seattle, Washington, 8-9 June 1965.

87) 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, Washington, 8-9 June 1965.

88) Ruff, George F. "The Role of System Safety Engineering and Its Relation to Reliability," North American Aviation, Inc. Downey, Calif., August 1965.

89) Stevenson, Maj. Gen. John D. "Ideas and Realities," Presented at the First Annual USAF Safety Congress, Riverside, Calif., September 12, 1960.

90) Theleman, D. R. "Industry Safety Information Interchange System, Part I Need and Ramification," Northrop NORAIR, Hawthorne, Calif. Presented at the Systems Safety Symposium, Seattle, Washington, January 8, 1965.

91) Wood, Amos L. "The Organization and Utilization of An Aircraft Manufacturer's Air Safety Program," The Boeing Company, Seattle, Washington. Presented

at the Institute of the Aeronautical Sciences Meeting, New York, January 1946.

92) Yandalla, Col. G. J. "Use of Privilege to Protect Safety Information," Presented at the Law-Safety Symposium, Univ. of So. Calif., June 1964.

Public Documents

93) Civil Aeronautics Board. Safety Regulations Effective 1 April 1963. Part 320.2 Federal Register, January 23, 1963.

94) Civil Aeronautics Board. U. S. Handbook of Airline Statistics. 1965 Edition.

95) Federal Aviation Agency. Act of 1958. Sect. 601b, (also, Sect. 102b, 103a, 103b.)

96) Federal Aviation Agency. Tentative Airworthiness Objectives and Standards for Supersonic Transport Design Proposals. Flight Standards Service, Washington, D. C., August 15, 1963.

97) Federal Aviation Agency. FAA Statistical Handbook of Aviation, 1965. Washington, D. C.: Gov't. Printing Office, 1965.

98) Federal Aviation Agency. Policy Statement of the FAA. Office of Policy Development, Washington, D. C., April 15, 1965.

99) Johnson, L. B. A Safety Policy for the Federal Service. The White House, Federal Register Doc. 65-2096-7, pp. 2517-8.

100) U. S. Air Force. Handbook for Instructions for Aerospace Systems Design. (A series of manuals carrying the designation AFSCM 80-1 through -9. Available through Systems Engineering Group (SEPS) Wright-Patterson AFB, Ohio.)

101) U. S. Air Force. Investigating and Reporting USAF Accident/Incidents. AFR 127-4, Washington D. C., February 23, 1963.

102) U. S. Air Force. General Requirements for Safety Engineering of Systems and Equipment. MIL-S-38130. Hdq. U. S. Air Force Systems Command, Washington, D. C., September 1963. (Revised as a Department of Defense specification MIL-S-38130A June 6, 1966.)

103) U. S. Air Force. Data Management, Management of Contractor Data and Reports. AFSCM/AFLCM 310-1, 1A, Washington, D. C., August 15, 1964.

104) U. S. Air Force. Systems Engineering Management Procedures. AFSCM 375-5, Air Force Systems Command, Washington, D. C., December 14, 1964.

105) U. S. Air Force. Responsibilities for USAF Aerospace Accident Prevention Programs. AFR 127-1, Hdq. U. S. Air Force, Washington, D. C., April 20, 1965.

106) U. S. Air Force. Systems Engineering Group, Wright-Patterson AFB, Ohio. Request for Proposal No. 01071 dated January 7, 1966.

107) U. S. Army. Accident Reporting and Records. AR 385-40, Washington, D. C., September 23, 1963.

108) U. S. Army. Safety Engineering of Aircraft Systems, Associated Subsystems, and Equipment; General Requirements For. MIL-S-58077 (MO), June 30, 1964.

109) U. S. Department of Labor. Report to the President, Mission SAFETY-70. Washington, D. C., September 1965.

110) U. S. Navy. Safety Requirements, Minimum, for Air Launched Guided Missiles. MIL-S-23069 (WEP), Washington, D. C., October 31, 1961.

111) U. S. Navy. Navy Aircraft Accident, Incident and Ground Accident Reporting Procedures. OPNAV

Instruction P3750.6E, Department of the Navy, Washington, D. C., March 18, 1963.

112) U. S. Navy, Office of Naval Material. NAVMATINST 3960.1, Washington, D. C., January 7, 1965.

Reports

113) Anon. Report of the U. S. Navy-Industry Conference on Aeronautical Material, Safety and Reliability. Sponsored by the Naval Aviation Safety Center at the Naval Air Station, Norfolk, Va., 3-5 December 1957.

114) Barton, J. A. Dyna Soar I Failure and Escape Analysis. Report E8R 11774, Chance Vought Corporation, Dallas, Texas, December 1958.

115) Chapanis, A. The Design & Conduct of Human Engineering Studies. Technical Rept. #14, San Diego State College Foundation, San Diego, Calif. (No Date).

116) Farish, P. T. Launch Vehicle Safety Engineering for Standard Payload Module. TM X-53282, Revised October 20, 1965. NASA Marshall Space Flight Center, Huntsville, Alabama.

117) Hensley, Col. H. S. System Safety - The Development of a New Program for Defense. Safety Division, Hdq. Air Force Systems Command, Andrews AFB, July 1966.

118) Lederer, J., Miller, C. O., and Schmidt, C. Economics of Safety in Civil Aviation, A Planning Study. Flight Safety Foundation, New York, N. Y. December 1963.

119) Lundberg, Bo. Speed and Safety in Civil Aviation: Part II Safety. Report Number 95, The Aeronautical Research Institute of Sweden, Stockholm, 1963.

120) Pitts, W. C. Summary Report of Reliability-Safety Analysis Methodology for Manned Space Vehicles. Report AST/EOR-13030, Chance Vought Corporation, Dallas, Texas, July 6, 1960.

121) Shannon, R. H., et al. Trends in USAF Aircrew Escape, 1 January 1950 - 30 June 1964. Deputy the Inspector General, USAF, Norton AFB, Calif.

122) U. S. Air Force. Requirements Methodology. Final Report of the WSEIAC Task Group i, AFSC - TR-65-1, January 1965 (AD 458453).

123) U. S. Air Force. The President's Safety Challenge, Mission SAFETY-70. Directorate of Aerospace Safety, Norton AFB, Calif., September 1965.

124) U. S. Army. Annual Activity Report, FY65. U. S. Army Board for Aircraft Accident Research, Ft. Rucker, Alabama.

125) U. S. Naval Aviation Center. (Activities Brochure, 1965), Naval Air Station, Norfolk, Virginia.

Unpublished Material

126) Andrews, K. R. "Morale and Safety in Aviation." Harvard Graduate School of Business Administration, 1951. (Mimeographed.)

127) Anshen, Melvin. "Nobody Around this Shop Listens to New Ideas." Carnegie Institute of Technology. (No date; Mimeographed.)

128) Boyd, A. H. "The Department of Transportation." A speech before the Aero Club of Washington, Washington, D. C., April 26, 1966. (Mimeographed.)

129) Holladay, David H. "What Constitutes a Safety Program." Aerospace Safety Division, Univ. of So. Calif., March 24, 1961. (Mimeographed.)

130) Kolodner, H. J. "Correlation of System Safety to System Reliability." General Electric Company, 1964. (Mimeographed.)

131) McCourt, Francis P. "Safety is a Commodity." U. S. Army Transportation Research Command, Spring 1965. (Mimeographed.)

132) Miller, C. O. "Survey of Aerospace Safety Information Sources, Data Sheets as of May 1965." Aerospace Safety Division, Univ. of So. Calif., June 1965. (Mimeographed.)

133) Miller, C. O. "Observations Relative to Fault Tree Analysis." Aerospace Safety Division, Univ. of So. Calif., October 1, 1965. (Mimeographed.)

134) Miller, C. O. "Selected USAF Regulation, Manuals, and Similar Publications Pertinent to System Safety." Aerospace Safety Division, Univ. of So. Calif., Spring 1966. (Mimeographed.)

135) Morrison, F. Robert. "Learning Curve Theory and Its Application to Aircraft Accident Prevention." Aerospace Safety Division, Univ. of So. Calif., Spring 1966. (Mimeographed.)

136) Peters, G. A. and Hall, F. S. "System Safety Engineering as a Technical Discipline." Rocketdyne Division of North American Aviation, Inc., April 1964. (Mimeographed.)

137) Schriever, Gen. G. A. "Charter, System Safety Task Force." Hdq., Air Force Systems Command, Washington D. C., September 3, 1964. (Mimeographed.)

138) Sharp, Col. John F. "The Positive Environment." U. S. Air Defense Command, Ent AFB, Colorado, 1958. (Mimeographed.)

139) Sharp, Col. John F. "A Job Well Done is Inherently Safe." U. S. Air Defense Command, Ent AFB, Colorado, 1958. (Mimeographed.)

140) Sharp, Col. John F. "Supervisor - Know Thyself." U. S. Air Defense Command, Ent AFB, Colorado, August 1963. (Mimeographed.)

141) U. S. War Department. "Mortality in Army Aviation." (Memorandum), Office of the Chief Signal Officer, Washington, D. C., February 28, 1914. (Mimeographed.)

Other Sources

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

143) Interview with R. J. Broderick, Exec. Secretary, Federal Safety Council, Personal, March 1966.

144) Interviews with members of the staff of the Records & Statistics Group, USAF Directorate of Aerospace Safety, Norton AFB, Calif., March 1966.

145) Interview with D. K. Warner, North American Aviation, Los Angeles, Calif., June 1966.

146) Letter from I. Irving Pinkle, NASA, October 1962.

147) 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., April 9, 1964.

148) Letter from W. I. Stieglitz to the Aerospace Systems Safety Society, October 18, 1965.

149) Nolde, George V. "Military Equipment Safety Factors and the Process of Engineering Design," Lecture Notes, Aerospace Safety Division, Univ. of So. Calif., January 6, 1965.

150) Stewart, B./Gen. C. B., USAF Director of Aerospace Safety. Address before the Graduating Class,

Aerospace Safety Division, Univ. of So. Calif.
December 17, 1965.

APPENDIX

SAFETY FUNCTION DESCRIPTIONS

USAF Safety Staff Officer (AFSC 1916)

1. Specialty Summary

Formulates safety policies and programs; coordinates safety matters with appropriate staff activities; and monitors and directs safety activities.

2. Duties and Responsibilities

a. Formulates safety policies and programs: Develops policies, plans, standard operating procedures, and implementing instructions for individual safety programs such as flying, ground, missile, or nuclear; or for integrated safety programs consisting of two or more of the individual programs. Develops policies and procedures for preparation, procurement, and dissemination of educational, promotional, and engineering safety materials. Plans internal training programs for safety officers and airmen. Dtermines personnel and material requirements of integrated or individual safety programs. Determines work loads and work priorities.

b. Coordinates safety matters with appropriate staff activities: Advises commander on the status of the safety programs. Coordinates policies, plans and programs with

appropriate staff agencies, such as armament, personnel, communications, intelligence, maintenance, and operations to insure the application of safety principles and knowledge to the activities of the various organizations. Consults with commanders and other staff officers on matters pertaining to safety. Maintains liaison with Federal, state, municipal, and private agencies to insure the interchange of safety educational materials, accident data, and equipment or facilities design criteria.

c. Monitors and directs safety activities: Reviews reports and compiles staff studies to evaluate operating procedures, to determine accident or incident trends, and to determine requirements for safety studies. Supervises safety activities to insure their effective and efficient operation. Directs or conducts individual or integrated safety activities.

USAF Flying Safety Officer (AFSC 1925)

1. Specialty Summary

Plans, organizes, and supervises aircraft, air-launched missile, and manned space in-flight vehicle safety activities; conducts accident prevention surveys and safety inspections; supervises accident investigations; and con-

ducts or supervises safety programs.

2. Duties and Responsibilities

a. Plans, organizes and supervises aircraft, air-launched missile, and manned space in-flight vehicle safety activities: Reviews and analyzes directives, regulations, accident reports, safety data, and local operating conditions to determine requirements for safety programs. Establishes policies, standards, and procedures designed to promote safe operations and reduction of accident rates. Maintains records, charts, graphs, and files on aircraft safety activities. Compiles statistical data on accident rates and trends. Prepares reports and correspondence on matters pertaining to safety. Distributes safety bulletins, posters, and publications to appropriate activities. Monitors activities concerned to insure compliance with safe practices, accident prevention policies, and standardized training and operations procedures. Reviews reports of alleged flying violations and initiates preventive actions as appropriate. Advises commanders and staff officers on problems pertaining to safety and status of safety programs.

b. Conducts accident prevention surveys and safety inspections: Conducts associated accident prevention and safety surveys. Surveys airdrome facilities and coordinates

with appropriate agencies to insure compliance with safety regulations and programs. Makes periodic inspection of airdrome facilities, such as runways, ground control approach units, taxi strips, light facilities, control tower, fire-fighting and crash equipment, and aircraft parking areas for conditions which would cause accidents. Maintains continuous study of flight operations to correct conditions detrimental to flying safety. Prepares reports on results of surveys and investigations and follows through to assure corrective action.

c. Supervises accident investigations: Establishes local policies and procedures covering accident investigations and insures compliance with higher headquarters and Air Force regulations and directives. Advises commander on designation of best qualified officers as accident investigators. Briefs designated officers prior to the investigation, monitors their progress and assists them as necessary. Reviews accident information, diagrams, statements, photographs, and findings prior to submission to the accident board and to higher headquarters. Participates in aircraft and manned space vehicle board proceedings.

d. Conducts or supervises safety training programs: Plans and schedules classes, lectures, and indoctrination

periods pertaining to safe operations and accident prevention.

Major Aerospace Contractor

Corporate System Safety Responsibilities

1. Provides guidance and coordinates system safety programs throughout the company (covering company products, transport, aircraft, and helicopters).

2. Initiates company policies and directives concerning system safety programs and assures that operating divisions procedures pertinent to these areas are consistent with company policies.

3. Reviews system safety clauses in contracts for the sale of the corporation's products and services in coordination with the Corporate Director--Contracts & Proposals.

4. Maintains liaison with the military organizations, government and civilian agencies, and other aerospace contractors in matters pertaining to system safety.

5. Coordinates company participation and representation on committees, conferences, etc. concerned with system safety when more than one division is involved; and arranges and conducts company-wide system safety meetings.

6. Represents the company in system safety matters with

organizations such as AIA, FSF, etc.

Division System Safety Responsibilities

1. Guide and coordinate the over-all division system safety program.

2. Initiate division policies and procedures concerning system safety programs, which are consistent with Company policy and contractual requirements.

3. Maintain liaison with the corporate Manager - System Safety on over-all system safety matters, and with the customer, and other agencies as necessary, on system safety matters pertaining to division products.

4. Review Requests for Proposals (RFP's) to determine system safety requirements; take the necessary action to include in the division proposals a system safety program consistent with requirements of the RFP, Company policy, and related government regulations.

5. Ensure that system safety requirements, criteria and standards are considered and included in plans, specifications, analyses, data requirements and reports, criteria handbooks, contractor evaluation reports, manuals, technical reports, studies, exhibits, etc., and that they are consistent with the over-all system safety program and Company policy. Establish, as necessary, system safety re-

quirements, criteria and standards where none exists.

6. Determine that system safety analyses and studies are accomplished as required.

7. Coordinate with the other division functions and areas of responsibility such as Design, Reliability, Quality, Life Sciences, Manufacturing, Test, Industrial Hygiene & Safety, Logistics, Contracts, Research, etc., in matters relating to system safety.

8. Participate in design reviews to ensure that proper system safety considerations are applied.

9. Assist, as necessary, in incident/accident/hazard investigations involving Company products.

10. Provide a focal point for the collection, storage and division-wide dissemination of information related to system safety.

11. Monitor and assess the status and effectiveness of division product system safety programs.

Program* System Safety Responsibilities

1. Guide and coordinate the over-all Program System Safety effort.

*Program refers to a given model Aircraft or missile.

2. Insuring that system safety requirements, criteria, and standards are considered and included in program documentation; establishing, as necessary, system safety requirements, criteria, and standards where none exist.

3. Coordinating and integrating system safety efforts with the Division System Safety office, Engineering Department, procuring activity, associate contractors, assigned divisions, and other concerned departments.

4. Determining that system safety analyses and studies are accomplished as required on the programs.

5. Insuring that proper system safety considerations are applied in system engineering, design, development, and design reviews.

6. Insuring that proposed design changes for the programs are reviewed for potential system safety impact.

7. Assisting, as necessary, in incident (accident) hazard investigations involving the program.

8. Coordinating program system safety requirements with functional areas of responsibility such as Design, Reliability, Quality, Human Factors, Manufacturing, Test, Industrial Hygiene and Safety, Logistics, Contracts and Pricing, Research, etc.

9. Reviewing Requests for Proposals (RFP's) to deter-

mine system safety requirements; taking the necessary action to include in proposals a System Safety Program consistent with the requirements of the RFP, company policy, and related government regulations as applied to the program.

10. Monitoring and assessing the status and effectiveness of program system safety activities.

Airline Flight Safety Officer

Safety and Economy

The prosperity and growth of an airline, or an aviation industry, is directly related to safety achievement; but whereas profit or deficit must be accounted for annually, money invested in safety cannot normally bring benefit in a short time scale. It is said that safety costs money. It should be an aim, therefore, that a Flight Safety function should account for its effectiveness by contributing to management efficiency.

Characteristics of a Flight Safety Function

A Flight Safety function should not attempt to replace primary basic organisational responsibility. It should be co-operative, remedial, advisory and non-punitive. Its aim must be to monitor all experience and, through a systematic process of recording, investigation, correlation

and review, to advise upon any changes considered necessary to maintain or improve safety.

The Qualities Desirable in a Flight Safety Officer

He should possess a good background of flying experience. His basic purpose is to communicate efficiently. He should cultivate an atmosphere of confidence which will enable him to establish and maintain continuously good liaison with the operations and engineering divisions of his airline at every level to ensure effective safety coverage of the whole operation.

The Organisational Place of a Flight Safety Officer

In order to maintain the integrity of responsibility in the normal management structure, the function should be advisory only.

The Flight Safety Officer should have direct access and be responsible to the chief executive.

The appointment should, if possible be on a full-time basis to ensure that the officer can work independently of flight operations and engineering divisions.

Where it is not possible to make a full-time appointment and it is combined with other duties, the person appointed should not be financially penalised. In this case the person appointed should be of sufficient seniority to

have access to and be able to discuss problems at every level within his organisation.

In the absence of any other independent investigating body within the organisation, the Flight Safety Officer should conduct any internal investigation into the airline's incident/accidents. (In this context investigation means fact finding only in accordance with the ICAO definition, differentiating between this and an inquiry.)

The Flight Safety Officer should have an office at the main operations base.

The Duties of a Flight Safety Officer

He should be familiar with those procedures and practices of his airline which have a bearing on safety. He should also be as familiar as possible in this respect with the procedures and practices of other airlines to the end that he will suggest consideration of any different procedures to those in use which might benefit safety.

The setting up, within his organisation, of an accurate reporting and recording system for incidents and accidents.

- Incidents/accidents must be reported on a prescribed form designed for the purpose of establishing basic factual and environmental information.

-The record should include all reportable incidents/accidents as defined in the airline operations manual.

-It is essential to encourage the discretionary reporting of incidents which could have led to accidents or which have a bearing on the safety of operations generally.

The survey and analysis of the information recorded from reports to establish trends; and the formulation of any necessary recommendations to management.

The assembly and selective dissemination of flight safety information from all sources within his own organisation and its correlation with that provided by external agencies such as the UK FSC., FSF., ICAO., IATA., ARB., MoA., BOAC., BEA., BIATA., manufacturers, the press, etc.

The provision of Flight Safety information to UK Incident/Accident Exchange Scheme.

The arrangement of periodic meetings with his executive and representatives of operational and engineering management for the purpose of systematically reviewing the overall safety of the airlines operation.

The provision of adequate publicity of flight safety matters within his airline.

Attending those national and international meetings on flight safety at which his airline decides to be represented.

The maintenance of a reference library of flight safety information conveniently accessible to flight crew members and others who will wish to keep up-to-date with current flight safety matters.

Civil Service Astronautical Research Laboratory

Safety Engineer for Lunar and Planetary Projects

Basic Function of Position - The Safety Engineer for Lunar and Planetary Projects is responsible for ensuring that adequate safety standards and procedures exist and are observed during the design, fabrication, testing and launch operation phase of the Laboratory's flight projects. He is concerned with safety not only as it pertains to safeguarding personnel from injury but also from the standpoint of avoiding damage to space vehicle equipment. While he is assigned specific responsibilities as defined below, his functions do not in any way absolve other individuals of their personal responsibility to be familiar with, and follow good safety practices in carrying out the Laboratory's flight project activities.

Specific Responsibilities - The Safety Engineer for Lunar and Planetary Projects is responsible for:

-Advising the Project Managers and their staffs on the safety provisions that should be included in Project Policy and Requirements Documents and in contractual documents.

-Checking at his own discretion, and fostering reviews of, the design of any mission-peculiar or mission-independent equipment, including the procedures for assembling and testing such equipment, to detect safety hazards that may exist to personnel or to equipment; advising cognizant Laboratory personnel, in writing, of actions that should be taken where hazards are apparent.

-Preparing policy statements concerning Project safety matters, including safety standards and procedures pertaining specifically to Project-peculiar equipment and activities, for the approval of the Assistant Laboratory Director, Lunar and Planetary Projects and notifying cognizant Laboratory supervisory personnel, in writing, of admonitions that should be applied as necessary to point up serious violations of safety practices.

-Inspecting at his own discretion, and fostering reviews of, any assembly or test operation at the Laboratory or at the test range, that involves spacecraft and related equipment to detect any safety hazards; advising the cognizant Project personnel in charge, of the need to halt such operation when immediate action appears to be necessary to avoid an imminent hazard to the safety of personnel or equipment.

-Consulting, with the concurrence of the concerned Project Manager, with the safety staff of contractors working under Laboratory Project direction to determine the adequacy of safety practices employed in the fabrication and testing of Laboratory equipment; advising the Project Manager or his designated representative, in writing, of significant changes that should be made by a contractor.

-Representing the Assistant Laboratory Director, Lunar and Planetary Projects, in any accident investigation where Project interests may be concerned.

-Serving as a member of the Laboratory Safety Committee.

-Consulting with the Laboratory Staff Assistant for Safety and the Division and Section Safety Coordinators as necessary to ensure that matters of common

concern are properly coordinated.

Authority - The Safety Engineer for the Lunar and Planetary Projects is accountable to the Assistant Laboratory Director, Lunar and Planetary Projects, for carrying out his assigned responsibilities. He functions in a staff capacity and is expected to provide support and expert advice to the Project Staffs on all matters involving safety. He is delegated authority by the Assistant Laboratory Director as necessary to permit him to carry out his specified responsibilities. A Project Manager or a Deputy Project Manager may override the Safety Engineer's recommendations and may direct waivers to established safety standards as they pertain to Project activities provided such actions or waivers are documented and made known to the Safety Engineer.

The Safety Engineer is authorized to have access to any facility or activity under Laboratory direction which is involved with flight project work. In carrying out his responsibilities he will observe established Laboratory and Project Office policies. In his dealings with a contractor he will observe the role of any Laboratory Resident Office and will be especially mindful of the importance of following established contractual procedures and any under-

standings which may exist between the Project Manager, Spacecraft System Manager and their contractor counterparts.