

N72-25967

**THE PRACTICAL APPLICATION OF MISHAP
DATA IN ARMY AIRCRAFT SYSTEM
SAFETY PROGRAMS**

**Lt. Colonel James T. Darrah, Jr.
U.S. Army Board of Aviation
Accident Research**

Presented at the

**NASA Government-Industry
System Safety Conference**

May 26-28, 1971

The system safety discipline has existed for several years now as a rather well defined concept. There has been very little argument as to the desirability of the system safety objectives. In fact, among many of those who know what these objectives are, there even has been generated a fair amount of what can only be described as "religious fervor" at the prospect of achieving the goals of system safety. But, with its well-organized, logical and comprehensive approach to accident prevention, the application of the system safety concept in practice has not been as rapid and effective as its attributes would warrant.

The United States Army Board for Aviation Accident Research (USABAAR) is vitally concerned with the application of system safety, particularly with respect to new developmental Army aircraft programs. USABAAR serves as the central agency for the Army Aviation Accident Prevention Program which includes the receipt, processing and analysis of all data and information related to Army aircraft accident experience. This paper discusses the means by which USABAAR now utilizes this vast store of historical accident data in the application of the system safety concept for developmental aircraft. While the methods described here admittedly fall short of realizing the full potential benefits of using our past accident experience, we feel that significant steps have been made in that direction. As more experience is gained in the application of these methods, certainly many refinements and improvements will follow.

The history of an accident can be generalized and simplified as shown in Figure 1. This depiction will be used throughout the remainder of the paper as methods are discussed which pertain to each segment of the diagram.

REQUISITE CLIMATE

Requisite climate, or "hazardous conditions" as it might be called, indicates that the stage for an accident must be properly set. If the proper conditions are not present, no accident will occur. These conditions involve the familiar triad of accident factors: man, machine and environment; plus the overall factors of command, management and supervision.

The command or management influence existing in an operation may play a significant role. Some casual remark by the commander at a morning briefing may quite innocently start a chain of events leading to catastrophe. Such influence most likely will concern the urgency of the mission to be performed, the quality of results desired or the belittling of problems, obstacles and risks. The result may be that the impression of "accomplish the mission whatever the cost" is conveyed which is tantamount to endorsing recklessness.

The condition of the people involved is perhaps the most complex factor present. The physical condition, state of mind, morale, proficiency and a wide variety of physiological and psychological factors all interrelate in a complex way to affect the potential human involvement in an accident. Change one small item and an accident could be averted.

The condition of the machine also involves a highly complex functional relationship of hardware which must exist in just the right way before an accident can occur. This relationship includes maintenance practices, worn pieces/parts, age of the equipment, design deficiencies, operating limitations and others, the complexity with newer sophisticated aircraft.

Environmental conditions cover an extremely broad range of phenomena including weather, terrain, operational situation, air traffic control airfield facilities and many more. The true influence these conditions on accidents is most often either not known or ignored.

MANIFESTATION OF HAZARDS

The worst possible combination of all the conditions listed above could conceivably exist and no accident would result unless some hazard manifested itself. Given the requisite climate the manifestation of the proper hazard initiates the accident sequence. This sequence can usually be divided into two or more main occurrences, precipitating and sustaining events.

The sequence will start with some trigger event which can be produced by a staggering variety of causes; again involving man, machine, environment and management or any combination of the four. Until that time, the

factors present in the requisite climate have played a passive role in the accident where the cause-effect relationship is usually not very precise. With the occurrence of the trigger event, however, the sequence of events which follow is usually quite predictable. What was a potentially hazardous condition before will now manifest itself through some event which, in itself, may never be considered hazardous. For example, shutting down one engine in a twin engine aircraft at altitude may present no hazard whatsoever. Shutting down that same engine while on short final approach during an emergency landing because the other one failed earlier could - - - and did - - - have catastrophic consequences.

Rarely does an accident occur as a result of one single event. There is usually a series of several events which follow the trigger event in sequence up to the accident itself. These can be called "sustaining events". If they do not occur, the accident sequence is broken.

Thus, given a requisite climate or potentially hazardous conditions, the accident sequence begins with a trigger event, is carried forward through sustaining events and an accident occurs.

UNDESIRABLE EFFECTS

If all this just described did not produce consequences which we wish to avoid, there would be no safety effort at all. It is really the undesirable effects of accidents themselves which justify our attempts at accident prevention. If this statement seems a trifle too basic and should have gone without saying, consider the possibility that we as safety specialists may have tended to lose sight of these undesirable effects of accidents as our basic motive force. Perhaps we have not concentrated sufficient attention on all the adverse consequences we are trying to preclude. We allow ourselves to become completely absorbed and obsessed with safety techniques, methodology and philosophy for their own sakes without maintaining a clear view of our ultimate objective - minimizing these efforts.

The effects of accidents can be grouped into two general areas with the respect to time. First, the abrupt damage and destruction to materiel plus injury and death to personnel

are the immediate consequences of an accident. Accidents are classified as to the degree of severity of these immediately observable effects. MIL-STD-882, the system safety standard, categorizes hazards in terms of their potential effects on materiel and personnel should an accident result from the hazard. But such categorization is not the end event; in a sense, it should be only the beginning of the analytical process to determine effects of accidents.

The second grouping of consequences from accidents includes the long range effects, those perhaps not immediately observable and which have an impact far beyond the time and geographical location of the accident itself. To the Army, these effects add up to a total cost in terms of lost or degraded mission effectiveness or capability. It is not at all far-fetched to say that each aircraft accident, no matter how insignificant in terms of immediate consequences, has some adverse effect on the capability of the Army to accomplish its mission. It logically follows, then, that if the total number of aircraft accidents is substantial, then the impact on mission effectiveness also will be substantial.

At any given point in time the accomplishment of the Army mission requires that certain aviation resources, people and materiel, be available. The degree of non-availability of these resources logically has a direct bearing on the ability to accomplish the mission . . . mission effectiveness. Since we obviously cannot acquire these resources instantaneously, we must not only project what our missions will be in the future, but also estimate what total aviation resources will be required in light of that future mission. Such estimates and projections are made for as far into the future as practicable and are then refined as time goes on. It is an extremely complex process, not the least part of which involves projecting the status of the current aircraft inventory, aviation personnel and facilities situation. Any shortfall of quantity, quality or capability in our projected inventory, personnel or facilities compared with our estimated requirements gives the basis for planning to acquire these resources. If we err, and underestimate our losses in aircraft and personnel, for instance, or do not adequately provide for quality in new aircraft,

an adverse impact on mission effectiveness is the result.

The main thrust of USABAAR's use of accident data for future aircraft programs is to estimate the long range impact on mission effectiveness through the proper analysis of this data. Unless we fully consider the far-reaching effects of accidents on people and materiel, we are not fulfilling the objectives of the system safety discipline.

ACCIDENT DATA

Accident prevention programs have traditionally operated on the basic premise that if the causes of accidents could be determined, preventive measures could then be developed to eliminate the causes. Following this premise, the primary task has been the acquisition of data and information through an accident investigation and reporting system. This task is performed exceptionally well today. Several years of diligent sleuthing, exhaustive interviewing of witnesses, and even precise laboratory analysis by both highly skilled and amateur investigators have produced an immense store of data and information on the causes of aircraft accidents. A significant portion of the safety effort of all military services, the Federal Aviation Agency, the National Transportation Safety Board and civilian aircraft manufacturers and operators is devoted to merely processing this wealth of data and information.

The results of accident investigations have usually been recorded in the form of a description of the accident sequence of events; the confirmed or suspected cause factors; recommendations to prevent recurrence and general factual data such as date, time, place, type aircraft, crews members, injuries, fatalities, etc. In general, the immediate consequences of the accident are recorded along with the events which led up to the accident. Quite often, but not always, it is possible for a thorough investigator to delve far enough into the past to well define the hazardous conditions which existed some time prior to the accident thereby enabling the accident to occur.

Until fairly recently, the primary use of all this data was to provide a source for various totals and rates reflecting only the most

general accident information. The key parameter for safety has been the periodic accident rate, the number of accidents divided by the number of hours flown. Accident "costs" have been reported by totalling acquisition "book value" for destroyed aircraft and repair costs for damaged machines. Fatalities have been totalled as have injuries, but with various criteria being used to describe severity of injuries. Cause factors have been lumped into a very few categories which then have been totalled. Among the most usually cited factors are crew error, materiel failure or malfunction, weather and maintenance error. Degrees of severity of accidents have been classified from "total loss" to "incident" depending on the extent of damage and injury.

Certainly, this most general treatment of accident data had a significant impact several years ago when compared with the even earlier situation when nobody even knew how many accidents they had been having. Initially, the concentration of attention on safety supported by only the most superficial analysis of accident data produced dramatic improvements. The magic "accident rate" began to drop rapidly as if to prove conclusively that such measurement of the problem was all that was necessary to solve it.

IMPROVED DATA SYSTEM

These methods which served the cause of accident prevention so well in the past are no longer adequate. There are widespread efforts underway for the development of more sophisticated data systems for safety. These efforts show that traditional parameters used to measure mishap experience cannot be used directly to solve many accident prevention problems today. Only a few deficiencies which have caused accidents in existing aircraft can be pinpointed sufficiently to correct the problem. For the rest of the problems in existing aircraft and for all of the potential hazards in a developmental aircraft, the identification of these old, generalized parameters does little but indicate a broad area of interest in which detailed analysis and specific evaluation is required. The detailed effects on mission capability must be identified to justify corrective action and the cost of such action.

To enable USABAAR to respond in this manner, completely revised accident reporting forms have been developed and put into use recently which greatly expand the scope and detail of information provided as a result of investigation of the accident are recorded along with the events which led up to the accident. Quite often, but not always, it is possible for a thorough investigator to delve far enough into the past to well define the hazardous conditions which existed some time prior to the accident thereby enabling the accident to occur.

Until fairly recently, the primary use of all this data was to provide a source for various totals and rates reflecting only the most general accident information. The key parameter for safety has been the periodic accident rate, the number of accidents divided by the number of hours flown. Accident "costs" have been reported by totalling acquisition "book value" for destroyed aircraft and repair costs for damaged machines. Fatalities have been totalled as have injuries, but with various criteria being used to describe severity of injuries. Cause factors have been lumped into a very few categories which then have been totalled. Among the most usually cited factors are crew error, materiel failure or malfunction, weather and maintenance error. Degrees of severity of accidents have been classified from "total loss" to "incident" depending on the extent of damage and injury.

Certainly, this most general treatment of accident data had a significant impact several years ago when compared with the even earlier situation when nobody even knew how many accidents they had been having. Initially, the concentration of attention on safety supported by only the most superficial analysis of accident data produced dramatic improvements. The magic "accident rate" began to drop rapidly as if to prove conclusively that such measurement of the problem was all that was necessary to solve it.

IMPROVED DATA SYSTEM

These methods which served the cause of accident prevention so well in the past are no longer adequate as evidenced by the comparatively recent development of more sophisticated data systems for safety. The traditional

parameters used to measure mishap experience cannot be used directly to solve many accident prevention problems. Only a few deficiencies which have caused accidents may be able to be pinpointed sufficiently to correct the problem. For the rest of the problems in existing aircraft and for all of the potential hazards in a developmental aircraft, the identification of these old, generalized parameters does little but indicate a broad area of interest in which detailed analysis and specific evaluation is required. The detailed effects on mission capability much be identified to justify coorrective action and cost of such action.

To enable USABAAR to respond in this manner, completely revised accident reporting forms have been developed and put into use recently which greatly expand the scope and detail of information provided as a result of investigation. The new forms were designed to take maximum advantage of a vastly improved data processing capability at USABAAR using a large digital computer. A completely new management information system has been constructed around this computer and is now in use.

It was realized early in the planning stages of the new USABAAR data system that it would not be good enough if all the computer could eventually do was produce the same sort of totals and rates produced previously. One skeptic, early in this planning stage remarked, "We're going to be able to arrive at the same, old general conclusions . . . only faster!" It has not worked out that way for one basic reason. The speed of the computer has enabled the efficient processing of timely data in far greater detail than ever before. This is the key to the success of a modern accident data system.

The production of this much more definitive data already has significantly improved our capability to do the following:

- a. Conduct in-depth studies and analyses to determine the long-range effects of accidents.

- b. Clearly define the sequence of events and the mechanism by which hazards manifest themselves.

- c. Comprehensively define the hazardous conditions which must exist prior to initiation of an accident sequence.

d. Pinpoint areas for specific corrective action, specify the action required and establish priorities for action.

e. Forecast measures to limit the requisite climate and inhibit hazard manifestation while at the same time placing such actions in context with their influence on the long-range undesirable effects of accidents.

DEVELOPMENTAL AIRCRAFT

We have recently developed methods by which this expanded capability can be applied "before-the-fact" to developmental aircraft systems. It is here that the most fertile application of our management information system is to be realized. These methods have shown that the gap can be successfully bridged between historical accident data on a fleet of existing aircraft in various stages of obsolescence and potential hazards in future aircraft which now exist perhaps in concept only.

The system safety discipline furnishes us with the overall management tool by which we can optimize the conservation of resources through the prevention of accidents before they happen, that is, to design safety into our aircraft systems. The heart of this process is hazard analysis in which the system is examined in a methodical, comprehensive way at each stage in its development to isolate hazards present. At some point in time, however, the moment of truth arrives when decisions have to be made as to what to do about hazards identified through analysis. Sometimes there is no penalty to correct or eliminate a hazard. Sometimes the hazard is so great that its elimination is mandatory regardless of the penalty. But the vast majority of hazards which are identified through system safety analysis fall somewhere in between. The question then becomes, "How bad do we want to eliminate these hazards?" Heretofore, the system safety engineer could only fall back on the MIL STD 882 category he has assigned the hazard. He has not been able to relate this hazard to future adverse long range consequences. His categorization has only addressed the immediate effects.

History has shown that new operational aircraft systems rarely incorporate a very large number of advanced technological features. Rather, new aircraft represent rational

growth versions of previous aircraft with improvements being made where practical and high technical risk features being held to a minimum consistent with performance requirements. The point is, in dealing with new systems, there is usually not that much really "new" about them. Those features of a developmental aircraft which are not new provide the place where accident data on previous systems is most directly applicable.

It is logical to expect that previous accident experience will be used in the design and operation of new aircraft so that cause factors noted in the past will not recur. To a disturbing degree, this has not been the case. There are several instances of the same feature which caused accidents in earlier aircraft being duplicated in newer models. One good example is the use of "redundant" systems in critical areas. Acknowledging that loss of hydraulics for flight controls would be catastrophic, one fairly recent design provided for two hydraulic systems, including two pumps - both driven by a single shaft of inadequate strength. Another design approached the same problem by also providing two hydraulic systems, but with all the hardware and plumbing co-located greatly increasing the chance of double failure from one event.

Such deficiencies as these were not negligently designed into the new system. Perhaps such designs were the result of ignorance - designers just didn't know we had supposedly already learned that lesson. More likely, however, it was probably felt that previous accident experience of one type of aircraft just did not apply to the "new" aircraft on the drawing boards.

This applicability of accident data is a real problem when trying to justify certain safety features in a yet unborn aircraft. USABAAR came face to face with this problem a few years ago when we attempted to prove, through accident statistics, that the Utility Tactical Transport Aircraft System (UTTAS) should have two engines. Since we had no twin engine utility helicopters in the inventory, we used accident data from the CH-47 Chinook, a twin engine light cargo helicopter and compared that data with the single engine UH-1 Iroquois data. As it turned out, one model of the UH-1 actually had a better accident rate than the CH-47. Obviously, this did our argument no

good. Other comparisons, using available accident data, showed some advantage for two engines, but not in the clear cut manner we thought it should. When the case was presented for decision, our arguments were unconvincing. We were told our reasoning was essentially faulty since a CH-47 differs so greatly from a UH-1 that they just could not be directly compared. They are of different size, have different missions, and do not even appear in the inventory in comparable quantities. In short, we had attempted to compare "apples and oranges to justify peaches."

This setback caused us to seriously ponder the factors which would make a difference in decisions such as for the twin-engine UTTAS. Our conclusion was that accident statistics just do not speak for themselves. The development of improved analytical techniques for processing accident data could not stop short of assessing the long range impact of accidental losses. Whereas, for the UTTAS question, we had compared single vs. twin engine accident rates, materiel failures, injuries, and deaths, degrees of damage and costs; we could not estimate, for example, the number of single engine UTTAS aircraft that would be lost due to engine failure and how those losses would affect the number we had to procure initially. This kind of estimate would have had a direct bearing on the decisions being made.

Today, USABAAR is carrying its analytical work several steps farther than before and doing it in much greater detail. While there is much work yet to do, progress has been made in several significant areas.

One area much in need of improvement is the design of future aircraft systems for the specific environment in which they are intended to operate. This consideration is not new, in itself, but the detail to which the operating environment must be specified is new. A major effort is now underway to clearly define the environment in which Army aircraft are expected to operate in the future. Given this definition, USABAAR is now in a better position to identify the specific environmental conditions which favor accidents and to specify detailed design criteria to counter these conditions.

Besides the greater detail now reported from accident investigation, there is another significant improvement which has been

made in our data system. A uniform method has been developed to translate the complex details of each mishap into data which can be stored and retrieved by the computer without losing the essential ability to differentiate between the details of each accident. Called "ABACUS", which stands for Aircraft Basic Accident Causes, U.S. Army, this method prescribes a vocabulary and syntax for encoding cause factors of aircraft accidents using a key word concept. Coding of accident information used to be a matter of fitting each set of circumstances to one of a limited number of rigid preconceived statements which seemed to best describe the event. Obviously, this procedure did not allow for distinction between similar situations where the differences were highly significant when it came to specifying corrective action. ABACUS, on the other hand, allows for nearly complete freedom to record the specific circumstances surrounding each individual mishap.

Statements concerning accidents are constructed using approximately 650 key words and phrases. They are combined in a prescribed sequence to describe phase of operation, subject, action verb, subject manner, subject position and/or condition, main object, object qualifier and reason. In addition, to these key words and phrases, aircraft nomenclature is also included using an abbreviated version of the aircraft parts catalog system. While the number of data elements available for use is still somewhat limited, the system allows for an extremely large number of possible combinations.

Probably most important is the fact that retrieval of data in a usable form is greatly facilitated through the use of ABACUS. Depending on the purpose of the analysis to be performed, any combination of ABACUS words, phrases or aircraft descriptors can be used as an argument with which to query the data bank. This exceptional flexibility in output means that the entire data base can be focused rapidly on virtually any conceivable accident prevention problem. We are no longer limited by inadequate or unusual data but only by our imagination in how to use the available data.

Using the matrix generating capability of the computer, we have greatly expanded our ability to compare the more detailed elements of information now acquired through accident

investigation. From the large number of possible combinations, relationship, between the most significant data elements have been established as indexes for various areas of interest.

One such area is fire in aircraft. A "Fire-worthiness Index" has been developed which measures all detailed factors relating to the incidence of aircraft fires and the immediate and long range effects. This index is established for each type, model and series aircraft in the inventory so that rankings between aircraft can be obtained. All the known elements in Fig. 1 are included. Given the detailed insight into past fire experience specific operations and aircraft configurations are then evaluated to determine those conditions which affect the index. The specification of fire-worthiness criteria for future aircraft, then, follows this evaluation directly. Furthermore, a relative priority can be attached to these criteria based on the fireworthiness index. For design criteria, the "index" approach is being used to make recommendations in terms of alternatives expressed as functions of the long term impact on mission effectiveness. At present, these recommendations are mostly general in nature, but as our analytical studies are completed, more specific criteria will be

developed. For developmental specifications, in addition to the estimate of long range impact, we will make recommendations in terms of alternatives expressed as functions of program costs, schedule and system performance. Such estimates will be of maximum benefit to the project manager and as such, maximize the effectiveness of system safety efforts in a program.

This has been a very general discussion of how USABAAR has begun to solve the difficult problem of using historical accident data in new developmental aircraft programs. By this discussion we do not wish to minimize the importance of continuing to develop improved analytical methodologies. More sophisticated techniques employing better predictive and quantitative procedures are sure to find widespread use in the future. We feel that the surface has only been scratched and that we have embarked on a course that will lead us eventually to the most effective attainment of the system safety objectives.

REFERENCE

Spezia, Emil, "ABACUS", U.S. Army Aviation Digest, October 1970, p. 50.

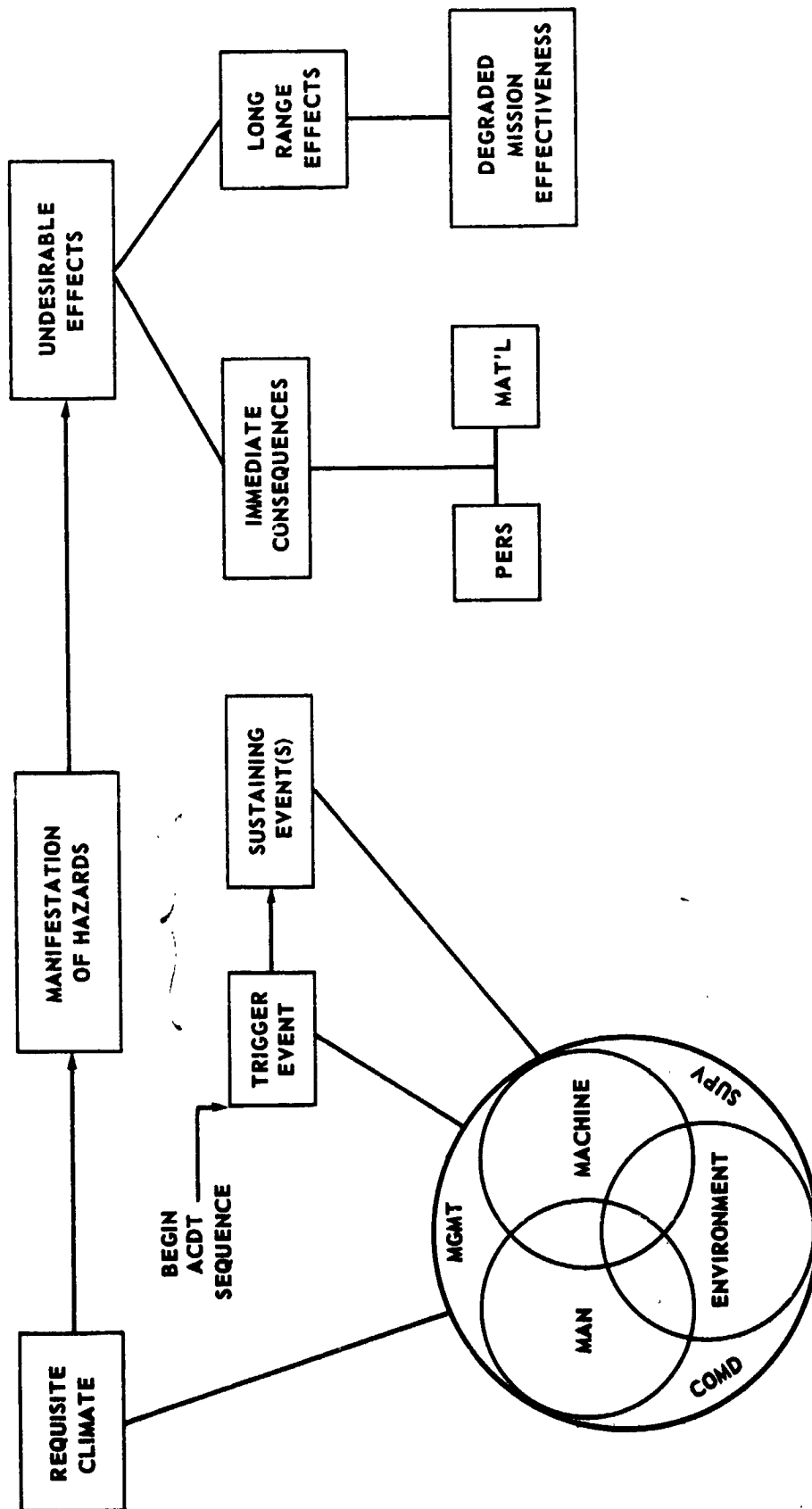


FIGURE 1