SYSTEM SAFETY EDUCATION FOCUSED ON FLIGHT SAFETY

Eugene Holt
University of Southern California

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

INTRODUCTION

General John D. Ryan, Chief of Staff, United States Air Force, in his keynote address at the 1969 Air Force Industry System Safety Conference, made a significant statement concerning System Safety. General Ryan stated, "We have encouragement by our competence in the engineering disciplines, but. . .many of our deficiencies in safety can be traced to a prevalent flaw, not in the area of competence, but in attitude." The problem identified by General Ryan is of particular significance in the field of System Safety. Many of our deficiencies in system design could be eliminated with proper attention and early attention to the "demands" of safety. However, the "demands" of safety in many cases are not adequately considered as a result of a negative safety attitude held by non-safety personnel in decision-making positions. This basic attitude toward safety results in the feeling that safety in general and safety programs in particular will inhibit or restrict or otherwise limit operations. The resultant atmosphere finds the system safety engineer in a defensive position attempting to convince personnel who, in the first place, are probably not technically qualified, and secondly, do not understand the system safety concept; in short, ultimately making the "hard sell" to a person who is not buying. Objectivity dictates that these management and non-safety personnel are normally influenced by the pressure of schedule constraints, budget limitations, and performance-oriented design groups. The realization that these personnel are also influenced by a sometimes unconscious bias or negative attitude in reference to the general subject of safety, let alone the lesser understood discipline of System Safety, should serve as a cause for great concern among safety educators. For as we ponder this situation and begin to evaluate proposed solutions to the problem, which incidentally is no unique problem and does not have a unique solution, the answer continues to come up SYSTEM SAFETY EDUCATION. We must educate until management and non-safety personnel recognize where and how utilization of the system safety process can best serve their needs.

The faculty and staff of the Institute of Aerospace Safety and Management, University of Southern California, are dedicated to the proposition that basic safety education is of fundamental importance to the success of accident prevention programs. The Institute, presently in its nineteenth year of operation, consists of two divisions and a Research Center. The Safety Division, founded in 1952, offers a variety of safety education programs designed as short courses which vary from one to twelve weeks in length. More than 9,000 students have attended Safety Division safety courses including personnel from the aerospace industry, commercial aviation, general aviation, the United States Armed Forces, and students from foreign countries. Notable alumni include astronauts Alan Bean, James Lovell, Jr., and Walter Schirra and the 1969 Harmon Trophy winner Major Jerry Gentry. The Graduate Division, founded in 1963, offers a graduate degree program, Master of Science in Systems Management. Operating from 26 graduate study centers located around the world, more than 1,775 master's degrees have been conferred. The recently established Research Center concentrates on research and development in flight safety, highway safety, transportation systems, and human factors.

SYSTEM SAFETY EDUCATION

The Institute of Aerospace Safety and Management has developed and conducted many different types of safety courses. In fact during the last fiscal year, 45 separate courses representing different programs were presented. These courses include Aerospace Engineering, Missile Propulsion Systems, Aircraft Accident Investigation and Prevention, Communicative Skills in Safety Education, Aviation Psychology, Aerospace Physiology, Aerospace Safety Management, etc. Although the major emphasis in all of the courses is safety, four of the courses deserve special attention in this paper due to their relevance to the subjects of Flight Safety and System Safety. These courses are:

I. Flying Safety Officer Course
II. Advanced Safety Program Management Course

III. Fundamentals of System Safety
IV. Quantitative Methods of Safety Analysis

- - - - -

I. The Flying Safety Officer (FSO) Course is presented to rated pilots of the United States Air Force and Air National Guard who are assigned to Flight Safety or Safety Staff Officer duties. The initial FSO course began 16 March 1953 and since that time 90 courses involving some 2,300 students have been completed. The FSO course is designed to develop in the student an understanding of the principles of accident prevention and how to incorporate these principles in an accident prevention program, an understanding of current flight safety educational methods in the Air Force, the ability to recognize hazards involving human performance, equipment performance, physical environment, and the interrelationship of these hazards, knowledge and skill in the supervision of aircraft accident investigation, an understanding of accepted principles of learning and the ability to apply them to instructional situations, etc. No specific reference to the subject of System Safety has been made; in fact, only recently have system safety engineering techniques and a general discussion of the System Safety concept been formally introduced into the FSO course curriculum. Rather the FSO course has been singled out here because of its fundamental importance and great tradition in safety education at the University of Southern California. System safety education at USC has its very roots in flight safety. Flying safety is concerned with the recognition, prevention, and elimination of all hazards to flight and the flying safety officer's job is primarily educational. He must assure that hazards are known and understood with an awareness of required corrective actions. Comparable course are also presented to U.S. Air Force Missile Safety Officers and U.S. Army Aviation Safety Officers.

II. The Advanced Safety Program Management (ASPM) Course provides specialized safety education for officers of the U.S. Air Force and civilians, GS-11 or higher, in order to assist in their further qualification as Safety Staff Officers. The initial ASPM Course began in November, 1964, and since that time 20 courses involving more than 500 students have been completed. The ASPM course is designed to develop in the student an understanding of the principles of management and the relationship of these principles to the management of effective safety programs, the basic principles of safety required for the development of a philosophy of safety, the collection, preparation and analysis of source accident data, the basic principles of motor vehicle safety, and an understanding of communications and industrial relations in safety management. The instructional material on the collection and analysis of accident data has recently been expanded to include not only the traditional methods of post-accident data analysis but also what has been termed pre-accident investigation. The instructional section begins with the graphical presentation of accident data, the derivation of accident rates, basic probability theory, statistical safety measures, confidence and risk, and the utilization of accident data in safety decision-making. System safety education has thus been introduced as a fundamental approach to accident prevention which is more effective, ensures greater leverage in design analysis and decision-making, and also affords the most economical approach to preventing accidents. Graduates of the ASPM course, who receive seven units of graduate credit, usually have a basic understanding of and practical experience in flight safety. Inclusion of system safety education in the curriculum has allowed these students' basic understanding and philosophy of safety to evolve and expand toward more of a total safety concept, including system safety and operational safety as an integrated approach to accident prevention.

III. The course, Fundamentals of System Safety, presents a curriculum of system safety education in its truest sense. The initial System Safety course began in October, 1963, and since that time 18 courses involving over 400 students have been completed. Prerequisite for this course is a bachelor's degree, preferably in an engineering or technical field, or three years of safety, system engineering, or maintenance experience. Three units of graduate level credit are given for satisfactory completion of the three week course.

System Safety as a fundamental approach to accident prevention has been and is continuing to be a rapidly expanding field which requires the best managerial and technical talents available. System safety educational programs have consequently been required to remain flexible in meeting the challenges of this expanding new discipline of System Safety. At the University of Southern California minor System Safety Course modifications have been made with almost every class. In fact, several major curriculum changes have been required during the past five years. It is believed that the experience gained through such a course evolution will prove critically important to the future success of system safety education at U.S.C.

The primary mission of the present System Safety Course is to develop within the student a basic understanding of the total system safety concept. The course is designed to address both the management and the engineering aspects of System Safety. The presentation of management and engineering material in a proper balance is both delicate and critical. Further, while the term System Safety properly defines a program to cover the entire life cycle of a system, the primary interest should be directed to the concept, definition, and development or so-called "design" phase of the system's life. System Safety will thus complement the established traditional safety efforts during the operational phases of a system. A system safety educational program should, therefore, be directed primarily to the earlier design phases of system life, devoting enough attention to the later operational phases to allow the student to understand the total scope of the system safety effort. The system safety engineering methods which may be applied during the design phase to evaluate the relative safety of proposed system designs are not only more technical and penetrating, but more quantitative also. The system safety engineering portion of the course should prepare the student to both perform and evaluate the vital safety analytical function; namely, the identification and control of system hazards. The system safety management portion of the course should familiarize the student with the planning, organizing, directing, and controlling aspects of management.

During the development and presentation of the instructional material of the course, the U.S.C. faculty have reviewed current industry and government system safety technology, adapted basic principles and specific methodology to individual aerospace applications, and genuinely pursued a course which is more than another theoretical discourse. Selected guest lecturers from industry enrich course content with "real world" experience. An extremely effective class group project, recently instituted, has proven successful in preparing the students for necessary System Safety program planning, organizing, job descriptions, and costing. A unique and beneficial aspect of the class group project is the coordination required of military and civilian students as team members. Working together on a team a common goal promotes a better understanding of the problems that each must face respectively.

A similar course is presented to Department of the Navy safety personnel in the Washington, D.C. area, except that separate system safety management and system safety engineering courses are presented, each two weeks in length.

IV. The course, Quantitative Methods of Safety Analysis, is a recent addition to the graduate courses presented by the Institute Safety Division. The basic premise of this course is that system safety analysis should be a process which is fully capable of assuming a leading role in design analysis. The basic purpose of system safety analysis should be, therefore to identify hazards in the system as it is proposed to be designed and operated, evaluate the risk associated with the identified hazards, and eventually to prevent or control the hazards which are considered to be unacceptable. This course provides technical knowledge in the system safety analytical technology and associated quantitative risk assessment methods. Most importantly, effective utilization of the output of the safety analytical program is emphasized in the instructional material. The student is introduced to the philosophy of risk acceptance, the derivation and allocation of risk requirements, and the quantitative risk evaluation methods.

SYSTEM SAFETY IN OPERATIONS

The conventional application of the system safety engineering process to the earlier design phases of the system life cycle has sometimes led to a lack of awareness of the technical safety aspects during operations. Utilization of the modern system safety analytical technology is being restricted almost entirely to the design phases as previously noted. Furthermore, system safety educational programs normally do not include System Safety as a formal, disciplined approach in the operational phase. Recent developments have been made at U.S.C. which should improve safety decision-making during the operational phase. These developments represent new and improved analytical methods for use during operations which were derived from the system safety technology. Accident Logic Diagramming is a good example of the adaptation of a system safety analytical method to assist the accident investigator in identifying accident cause factors. The field of accident investigation has developed into a highly specialized body of technical knowledge. There are files which are literally full of accident cause data, hoping that through knowledge of the cause of accidents we can take action to prevent future accidents. It is possible that rather than logically identifying real causes of accidents, the accident investigator is doing nothing more than confirming his preconceived conclusions. In order to minimize this possibility, the investigator should utilize a logical, systematic, and thorough approach which is more analytical in nature in order to isolate and identify accident causes. A method of system safety analysis which has been developed over the past ten years termed Logic Diagram Analysis or Fault Tree Analysis, is ideally suited to this task. The logical processes of fault tree development are in fact identical to the logical processes of accident investigation. The investigator and the analyst deduce from available evidence, beginning with the fact of the accident or pre-accident itself until the probable cause can be identified and substantiated. Utilization of this analytical tool by the investigator to organize his thinking is termed Accident Logic Diagramming. Standard event and logic gate symbology have been developed and may be consistently applied to actual accident situations. However, for the purposes of accident investigation, certain modifications to the basic logic diagramming system are required. Since the undesired event in question has already occurred, then the matter of event probabilities and quantitative risk evaluation is not necessary. Accident Logic Diagramming is strictly a qualitative assessment. As a result all possible causative conditions can be logically diagrammed, regardless of the availability of numerical failure data. The man, the machine, and the environment can be logically combined as an interacting system.

Several obvious advantages are realized with Accident Logic Diagramming. First, the logical thought processes are presented in a visible, logical, easily understood diagram for others to see and comment upon. This factor alone increases the likelihood that ideas will be shared and investigative methods will be questioned. Second, a documented, graphical checklist of areas to investigate logically develops with the diagram, minimizing the possibility that important evidence will be overlooked early in the accident investigation. Finally, the Accident Logic Diagram becomes a flow chart and a realistic indicator of investigative progress. Notes on evidence can be made next to the diagram events to which they apply, indicating whether the events did or did not occur. It is recommended that the Accident Logic Diagram be prepared as early as possible in the investigation cycle, and that it be continually expanded. Eventually as the actual accident cause factor(s) is isolated and identified, necessary corrective actions can be taken, thus reducing or eliminating the possibility of future accidents due to similar cause factors.

CONCLUSION

General John D. Ryan stated, "The application of measures to achieve higher levels of System Safety is recognized today as a vital concern for the entire engineering community as well as for our managers and operators. This goal is clearly essential, because it represents the principal means of preserving the combat capability of the Air Force. We, therefore, must consciously focus our efforts on reaching that goal. . ." System Safety is a

vital concern in the achievement of accident prevention. The application of the System Safety concept in design and in operations should be a principal means of avoiding all conceivable situations which can place our nation, its resources, or its population in jeopardy. As our nation continues to design and manufacture equipment which is more expensive, more complex, with greater degrees of automation for use by and around a public which is aroused and more intelligent, System Safety becomes increasingly important. As a result, System Safety education is also becoming increasingly important. At the University of Southern California, as safety educators we are confident and optimistic that the challenges of System Safety education will be met.