1977

A Hypothetical Model for System Safety in Air Transportation

Herbert Matthew Bowden
University of Central Florida

A HYPOTHETICAL MODEL FOR SYSTEM SAFETY IN AIR TRANSPORTATION

BY

HERBERT MATTHEW BOWDEN
B.S.E., Florida Technological University, 1974

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Master of Science in Engineering
in the Graduate Studies Program of the College of Engineering
of Florida Technological University

Orlando, Florida
1977

INDUSTRIAL ENGINEERING

MEMORANDUM August 23, 1977

TO: Dean R. D. Kersten

FROM: Graduate Committee - Mr. Herbert M. Bowden

SUBJECT: Completion of Final Oral Examination

We are pleased to certify that Mr. Herbert M. Bowden completed his final oral examination in defense of his thesis entitled "System Safety in Air Transportation". Mr. Herbert M. Bowden is a candidate for the degree of Master of Science in Engineering.

George F. Schrader

Dr. G. F. Schrader, P.E.
Committee Chairman

George F. Schrader

G. F. Schrader, Ph.D., P.E.
Chairman, IEMS

GFS:lsy

A HYPOTHETICAL MODEL FOR SYSTEM SAFETY

IN AIR TRANSPORTATION

by

HERBERT MATTHEW BOWDEN

ABSTRACT

This thesis, "A Hypothetical Model for System Safety in Air Transportation," is addressed to an individual having a basic technical background and some familiarity with the air transportation system in the United States. The thesis identifies the need for and benefits to be obtained from a system-wide program of safety activities. The organizational framework for implementation of a system safety program is presented as well as techniques of safety analysis.

George F. Schrader

Director of Thesis

ACKNOWLEDGEMENTS

I would like to express my sincere appreciation to my Chairman, Dr. George Schrader, for his advice and encouragement in this effort. I would also like to thank Mrs. Eunice Willingham for typing this manuscript.

TABLE OF CONTENTS

Chapter

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

GENERAL

Scope and Purpose

This thesis, "A Hypothetical Model for System Safety in Air Transportation," was undertaken as a result of a joint effort by the United States Department of Transportation and the Transportation Systems Institute of Florida Technological University to conduct a research project in the field of transportation safety. This paper incorporates and expands on the concepts developed in this effort, published as "Manpower Analysis in Transportation Safety" by the United States Department of Transportation in June of 1977.

The objective of this thesis is to develop a hypothetical model of a system safety program for the commercial air carrier industry. The air carrier industry is composed of private air carriers, government agencies, and various associations and professional groups. The model includes systems analysis techniques applicable to the industry as well as the organizational framework to provide system-wide direction of safety activities.

Introduction

The first so-called air carrier, the St. Petersburg-Tampa Airboat Line, began operations on January 1, 1914. The company

owned three seaplanes powered by six cylinder engines with a top speed of sixty miles per hour. With a seating capacity of two or three passengers in an open cockpit, the airline transported over 1,250 passengers with no injuries before closing after three months of operation. The company closed because the ten dollar round trip fees were not yielding high enough profits, but the venture was the first of many, and made it clear that an air carrier could be operated in a safe manner (1).

Application and Implementation

The model developed in this thesis is applicable to all segments of the commercial air carrier industry in the United States. It may be used in preparing safety requirements for inclusion in governmental regulations and laws, system safety program plans, and other related documents.

Applicable Documents

The following documents form a basis for a workable system safety program in the air carrier industry.

1. Federal Aviation Regulations
2. State and Local Laws
3. Corporate Safety Program Plans

CHAPTER II

OVERVIEW OF THE INDUSTRY

Magnitude

According to the latest available statistics, the air carrier industry in the United States consists of thirty-eight domestic and international carriers and ten supplemental carriers. The domestic carriers have 2,518 aircraft available and employ 254,646 people, while the supplemental carriers have 156 aircraft available and employ 5,002 people. In 1973 the total revenues for domestic carriers were $8,983 million, compared with $328 million for the supplemental carriers. Operating at an average airborne speed of 410 miles per hour, in 1973 the domestic carriers flew a total of 1,281 million passenger miles (2).

Summary of the Safety Record

Considering the number of passengers that can ride on today's large aircraft, it is clear that the loss of only one vehicle can produce a drastic effect on statistics of the number of injuries and fatalities. Due to this effect, statistics on air carrier fatalities should not be studied without relating them to the comparable statistics on the number of accidents. Table 1 illustrates the number of accidents in the air carrier industry in 1962, 1971, and 1972. For all certificated, scheduled opera-

tions, the number of accidents increased slightly from 1971 to 1972, however the average annual number of accidents over the ten year period decreased slightly. For all non-scheduled and supplemental carriers, there is a large percentage increase in the number of accidents in 1972 over 1971. Both of these statistics do however show an average annual decrease during the ten year period.

Table 2 illustrates the number of fatalities in the air carrier industry over the same time periods. The number of fatalities show a decline in 1972, however in scheduled service operations, there is a slight average annual increase in the number of fatalities during the ten year period. Perhaps this is due in part to the growth of the industry and the larger capacity of the aircraft. It should be noted that during the years 1962 to 1972, the number of accidents experienced an average annual decrease of 3.4 percent, while the number of fatalities increased an average of 2.7 percent a year. Exactly the opposite is true during 1972. The number of accidents increased by 4.3 percent while the number of fatalities decreased by 6.4 percent. This may be due in part to improved safety programs and equipment.

Figure 1 shows the ratio of NTSB Classified Accidents per 1,000 departures for twelve major air carriers in the United States during the years 1964 to 1972. While these figures are inconclusive, it appears that the air carriers with the larger operations experience a lower ratio of accidents per departures, implying that experience pays off in fewer accidents.

TABLE 1

ACCIDENTS IN AIR TRANSPORTATION

Type of Carrier	1962	1971	1972	Average Annual Percent Change	1971-1972 Percent Change
All Certificated Air Carriers	68	46	48	-3.4	4.3
Scheduled Service	50	42	43	-1.5	2.4
Domestic	40	33	37	-0.8	12.1
International	10	9	6	-5.0	-33.3
Non-Scheduled Service	18	3	5	-12.0	66.7
Domestic	N/A	2	4	N/A	100.0
International	N/A	1	1	N/A	0.0
Supplemental	5	1	2	-8.8	100.0
	N/A	1	2	N/A	100.0
	N/A	0	0	N/A	0.0

SOURCE: U. S. Department of Transportation, Summary of National Transportation Statistics, 1974 (Washington, D.C.: Government Printing Office, 1974), p. 27.

TABLE 2

FATALITIES IN AIR TRANSPORTATION

Type of Carrier	1962	1971	1972	Average Annual Percent Change	1971-1972 Percent Change
All Certificated Air Carriers	146	203	190	2.7	-6.4
Scheduled Service	146	198	186	2.5	-6.1
Domestic	146	198	186	2.5	-6.1
International	0	4	1	0	-75.0
Non-Scheduled Service	139	5	4	-29.9	-20.0
Domestic	N/A	5	4	N/A	-20.0
International	N/A	0	0	N/A	0.0
Supplemental	3	0	0	-100.0	0.0
	N/A	0	0	N/A	0.0
	N/A	0	0	N/A	0.0

SOURCE: U. S. Department of Transportation, Summary of National Transportation Statistics, 1974 (Washington, D.C.: Government Printing Office, 1974), p. 27.

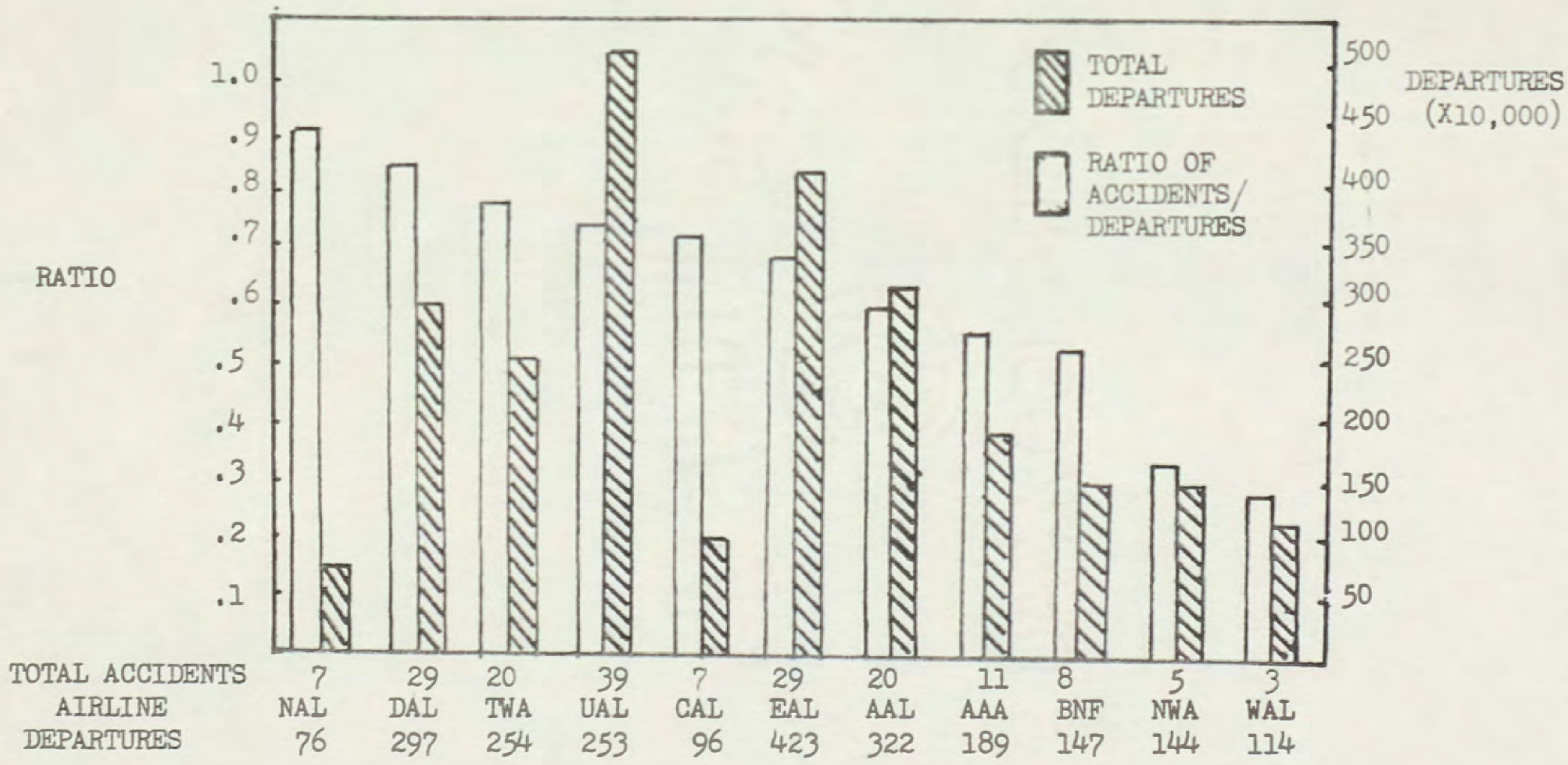


Fig. 1. Ratio of NTSB Classified Accidents per 1,000 Departures for Years 1964-1972. SOURCE: U. S. Department of Transportation, Manpower Analysis in Transportation Safety (Washington, D.C.: Government Printing Office, 1977), p.2-7.

Trends in Aviation Accidents and Fatalities

The safety record of the air carrier industry when compared to that of general aviation appears to be very good. Fugure 2 shows an eleven year history of aviation accidents and fatalities for both general aviation and the air carrier industry. During that period, less than two percent of all aviation accidents occurred in the air carrier industry. However, those relatively few accidents resulted in an average of nearly seventeen percent of the fatalities during that period and in 1974 this fatality contribution increased to over twenty-six percent. Thus, although the accident records of the air carrier industry have been showing a modest improvement during the past four or five years, the increasing fatalities resulting from those accidents have been alarming. As was mentioned previously, the larger size of the aircraft is a major contributing factor in this statistic.

Definitions

The following definitions from Glossary of Aeronautical Terms, published by the Transportation Safety Institute in 1973 are applicable to the study of air transportation safety.

1. Airway

   An air route along which aids to air navigation, such as landing fields, beacon lights, radio direction finding facilities, intermediate fields, etc., are maintained

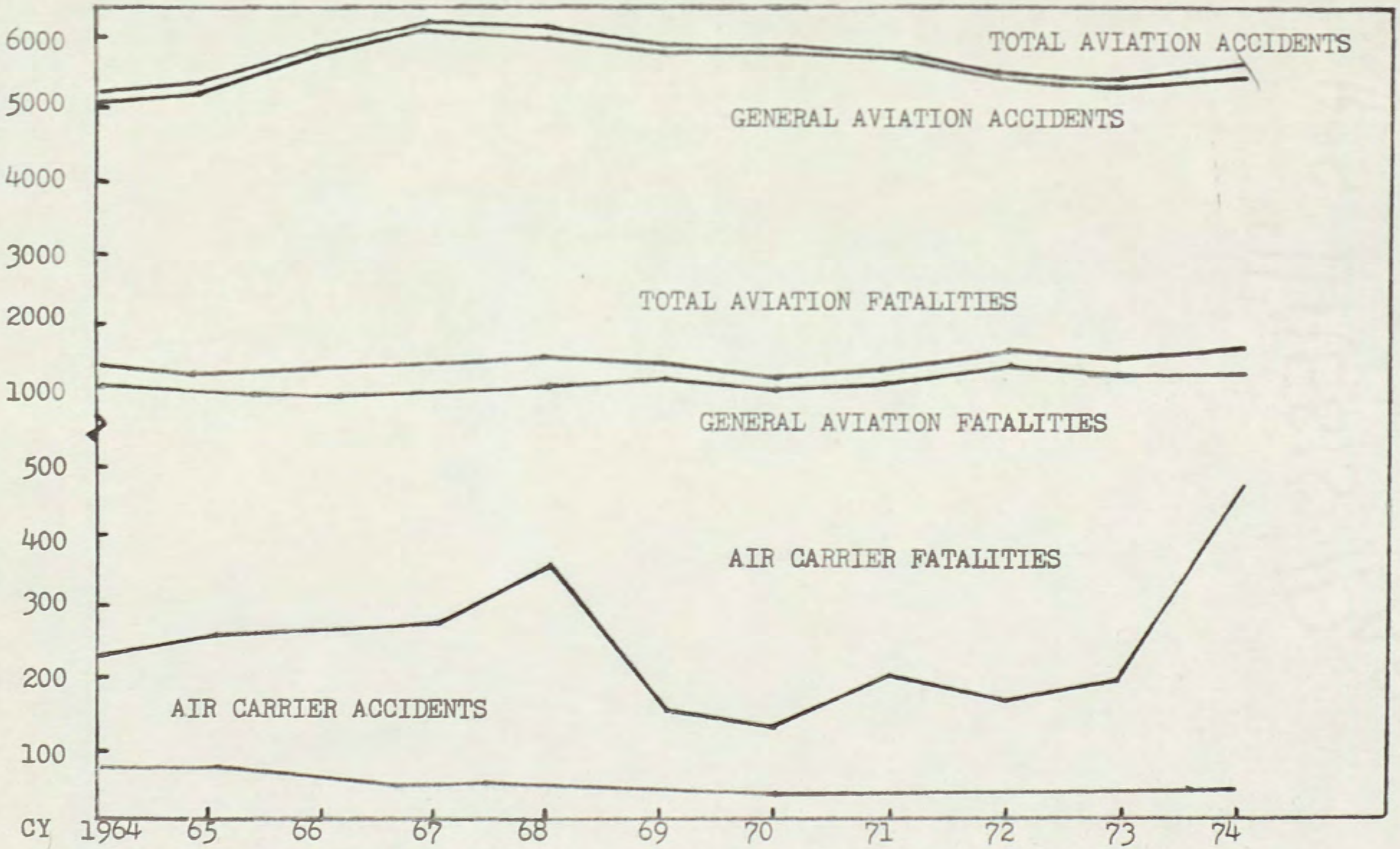


Fig. 2. Trends in Aviation Accidents and Fatalities

SOURCE: U. S. Department of Transportation, Manpower Analysis in Transportation Safety (Washington, D.C.: Government Printing Office, 1977), p. 2-9.

2. <u>Airworthy</u>

In a condition suitáble for safe flight

3. <u>Airworthiness Certificate</u>

A certificate issued by the FAA or a designee and certifying that the aircraft met, at the time of inspection, current airworthiness standards

4. <u>Certificate of Public Convenience and Necessity</u>

Certificate issued by the CAB, in compliance with Section 401 of the Federal Aviation Act of 1958, authorizing a carrier who has furnished proof of service to engage in transport of passengers or cargo

5. <u>Certificated Route Air Carrier</u>

One of a class of air carriers holding certificates of public convenience and necessity, issued by the CAB, authorizing the performance of scheduled air transportation over specified routes and a limited number of nonscheduled operations. This general carrier grouping includes all-purpose carriers (i.e., the so-called passenger/cargo carriers) and all-cargo carriers, and comprises all of the airlines certificated by the CAB except the supplemental air carriers. Certificated route air carriers are often referred to as <u>scheduled airlines</u>, although they also perform nonscheduled

service

6. <u>Civil Aircraft of the U. S.</u>

Any aircraft registered as provided in the Federal Aviation Act of 1958

7. <u>Local Service Carriers</u>

Certificated domestic route carriers operating routes of lesser density between the small traffic centers and between those centers and principal centers.

8. <u>Passenger</u>

An occupant of an aircraft in flight other than a crewmember

9. <u>Pilot Certificate</u>

Authorization issued by the FAA for a pilot to operate aircraft to an extent stipulated by the ratings and limitations of his certificate. Grade of certificate includes; ATP, Commercial, Private, and Student. Ratings and limitations include such items as: ASEL, ASMEL, ASMEL&S, Glider, Rotocraft, DC3, DC6, DC8, 707, 727, 747, Instructor, and not valid for night flight or color signal control

10. <u>Proficiency Flight</u>

A flight made by a pilot or other aircrew member or members to develop or improve in flying duties

11. <u>Passenger-Mile</u>

A measurement whereby one passenger is transported one mile

12. <u>Supplemental Air Carrier</u>

One of a class of air carriers now holding certificates, issued by the CAB authorizing them to perform passenger and cargo service supplementing the scheduled service of the certified route air carriers. Supplemental air carriers are often referred to as nonskeds, i.e., nonscheduled carriers

13. <u>Time in Service</u>

With respect to maintenance time records, means time from the moment the aircraft leaves the surface of the earth until it touches at the next point of landing

CHAPTER III

SAFETY ACTIVITIES

Safety Data

Data regarding air carrier safety is available from the NTSB and the FAA on a regular basis. The NTSB publishes its reports on aircraft accidents and the FAA initiates directives regarding the design of the aircraft involved. The NTSB annually publishes its findings and statistics in an "Analysis of Aircraft Accident Data." Unfortunately, this data is provided as the result of investigations into accidents or incidents. On a system level, this information provides a base to incorporate known hazards into the design of equipment and the training programs of personnel involved in its operation.

Government Safety Programs

In September of 1973, the United States Department of Transportation issued an order dealing with its safety policy. The Office of the Assistant Secretary for Environment, Safety, and Consumer Affairs was created to establish within the Department a principal point of contact on matters concerning all aspects of transportation safety.

The Federal Aviation Administration (FAA) was established as an integral part of the Department of Transportation by the

Transportation Act of 1966. Prior to its becoming an entity of the DOT, the FAA was an independent agency of the U. S. Government, established by the Federal Aviation Act of 1958.

The primary safety mission and functions of the FAA have been to regulate air commerce in such a manner as to best promote its development and safety.

The FAA is responsible for the following activities.

1. Licensing pilots, other airmen and related air agencies
2. Certification of the design, manufacture, and performance of every civil aircraft
3. Certification of airports serving CAB certified air carriers
4. Safely operating the nation's airways and ensuring efficient use of airspace
5. Installing and maintaining complex electronic air traffic control and navigation systems
6. Administering a grant-in-aid program to airports and providing advisory services to communities in the design and construction of public airports.
7. Conducting research in almost every phase of aviation

The Federal Aviation Act of 1958 continued the existing Civil Aeronautics Board (CAB) as an agency of the U. S. Government. This board consists of five members appointed by the President,

and is concerned with all phases of the development and regulation of civil aeronautics. The specific duties are detailed in the Federal Aviation Act of 1958.

The National Transportation Safety Board (NTSB) investigates all accidents involving civil aircraft. It publishes reports and makes recommendations to the FAA regarding the safe and efficient use of the airways.

Areas of Safety Regulation

The regulation of aviation safety rests primarily in the hands of the FAA. Their regulations cover the following areas.

1. Registration of Aircraft
2. Regulatory Functions of Air Traffic Control
3. Certification of Aircraft and Airmen
4. Investigation of Accidents

The authority for these regulatory functions may be found in the Federal Aviation Act of 1966. Further discussion of these areas is appropriate.

Registration and Regulation of Aircraft

All aircraft operating in the United States must be registered with the FAA. This process is much like registering an automobile, with the exception that all aircraft are registered with the same agency. The FAA establishes reasonable rules for registration and identification of aircraft, engines, propellers, and other appliances and safety items.

Minimum standards are established by the FAA governing the design, materials, workmanship, construction, performance, inspection, servicing and overhauling of aircraft, engines, propellers and appliances as well as the equipment and facillities for such inspection and production.

Rules and regulations are also established affecting the reserve fuel supply carried in flight, as well as the maximum number of periods of service which airmen may perform in a given period of time.

Certification

The FAA issues five basic types of certificates in all phases of aviation (3). The first certificate is the Airman Certificate. The FAA establishes physical as well as mental requirements for all pilots, traffic controllers, mechanics, etc.

The second certificate involves the aircraft itself. The FAA issues a Type Certificate to an aircraft, engine, propeller or other applicance. The facilities and equipment that will be used to manufacture these parts are inspected and, if satisfactory, will be issued a Production Certificate. Only after the finished product has been tested will an Airworthiness Certificate be issued. This certificate must be renewed annually.

Air carriers are issued an Air Carrier Operating Certificate. For safety reasons, the terms, conditions, and limits of operation, routes and airways traveled are specified in this

certificate. Any change in the carrier's schedule or route must be recertified.

All airports must have their landing lights, landing areas, radio directional apparatus and like equipment inspected and given an Air Navigational Facility Certificate.

Any flight training school or maintenance and repair facility must be certified. The FAA determines if the schools have certified instructors and the curriculum is acceptable, and whether the maintenance and repair facilities have adequade equipment and personnel to perform their specified functions. If these requirements are met, an Air Agency Rating Certificate is issued to the school or maintenance facility.

Air Traffic Control Systems

Ground based air traffic control systems monitored by controllers were originally intended to separate airline flights during poor visibility weather. When this system was initiated, airline flights were much fewer in number and IFR (Instrument Flight Rules) flights were scarce. Today, with the extreme increase in volume of all types of air traffic, such a system has built in hazards. When an aircraft takes off or lands at a large airport, it is passed through several controllers, each monitoring several aircraft in his jurisdiction. The possibility of human error is large, and no amount of training can force a system to operate beyond its capacity. It has become clear that the respon-

sibility for collision avoidance must be removed from the human controller and delegated to a real-time computer facility.

One of the first steps toward such a system was the implementation of the Automated Radar Terminal System (ARTS) in Atlanta in 1967. The implementation of the Common IFR Room (CIFRR) in 1968 at Kennedy International combined the IFR rooms of Kennedy, LaGuardia, and Newark. Such systems drastically increased efficiency and safety in crowded areas with several airport facilities (4).

The basic functions of the computerized air traffic control system are as follows: to track ground speed, identify aircraft within the controlled area, sequencing, final approach spacing, metering and multiple runway feeding. The mechanics and hardware associated with such systems are beyond the scope of this thesis. There are, however, several periodical articles on these systems, two of which are listed in the Footnotes, References 4 and 6.

Safety Programs of Air Transportation Related Organizations

There are several private organizations involved with the development of safe air transportation. Among these are the Airline Pilots Association (ALPA) and the Air Transport Association (ATA). These organizations provide a broad base of support for pilots and owners of aircraft to aid in this development. As an example of their activities, the members of the ALPA went on strike early in 1975 to force stronger control over the transporting of

hazardous materials.

CHAPTER IV

SYSTEM SAFETY PROGRAM OBJECTIVES AND MILESTONES

Objectives of the System Safety Program

The System Safety Program must include all phases of development, production and operation of the air transportation systems. The program objectives should include the following as a minimum (5).

1. To insure that a level of safety consistent with the safety goals of the industry are designed into the system
2. Hazards associated with each component of the system are identified and evaluated to be controlled to an acceptable level or eliminated.
3. Procedures to control hazards inherent in the operation of the system to protect personnel, property, passengers and equipment
4. New materials, production and testing techniques are properly evaluated prior to their acceptance.
5. Knowledge of the "state of the art" is maintained to insure maximum utilization of new developments
6. All historical data from any safety related program is utilized when available

The safety goals of the industry should be established by a joint study by the air carriers, aircraft and ground equipment manufacturers, and government regulatory agencies. By designating one agency as a clearing house for all industry safety information, the safety activities of all segments of the industry can be directed toward these common goals. As the primary regulatory agency, The FAA has access to information from all segments of the industry, and is the only conponent with the ability to enforce the guidelines that will be needed to implement a system-wide safety program.

Details on how these system safety goals should be established and maintained are discussed in the following sections of this chapter.

System Safety Program Management

As previously stated, the FAA should provide the direction to establish system-wide safety goals and activity milestones to insure the efficient operation of the system safety program. This should be done on an annual basis, and in a formal atmosphere.

This will require the presentation of an annual System Safety Program Plan (SSPP) to the FAA from each air carrier, system level equipment manufacturer, and government agency involved with the air transportation industry. From the evaluation of these inputs as well as FAA conducted studies, an overall SSPP would be formulated by the FAA.

The basic components of the SSPP provided by each segment would vary. The air carriers would concentrate on personnel training, preventive maintenance programs, replacement of obsolete and outdated equipment, and route certification.

Areas of concern among aircraft and ground equipment manufacturers would focus on applications of systems analysis techniques to the design, manufacture, and operation of their products, as well as continued research and development activities.

From the data provided by annual accident summaries and analyses of the NTSB, the FAA can focus the activities of the other segments in a common direction. These statistics indicate where the greatest need for advancement toward the established system safety goals exists.

In addition, each segment should identify any problem areas resulting from its interface with the other segments. Proposals should include alternative courses of action as well as cost impact studies.

The following three chapters provide further discussions of each segment of the industry and areas of their concern. Chapter Six discusses some of the hazards associated with airports and airways, or the system environment. Chapter Seven identifies the organization structure and safety tasks associated with the three major classifications of commercial air carriers. Finally, Chapter Eight discusses some of the hazards associated with the aircraft in its use by the air transportation industry. Conclusions and

recommendations drawn from these discussions are summarized in Chapter Nine.

Obstacles to Achieving a System Safety Program

Within the present framework of air carrier safety activities, there are a number of obstacles to the success of a system-wide program in air safety.

For such a program to function properly, it must be well defined and under constant evaluation, by the individual airlines themselves and the FAA. The FAA is constantly plagued by inadequate funding resulting in an inability to enforce its safety regulations due to a lack of personnel. Other groups such as the Airline Pilots Association (ALPA) and the Air Traffic Controllers Union (PATCO) have become instruments of collective bargaining rather than safety related activities (6).

Perhaps the biggest problem is that safety is not always cost effective. The lure of higher profits often leaves safety related programs behind in today's economic climate.

These problems are only a few that face the safety conscious organizations of the airlines and the FAA, and are mentioned here to reinforce the idea that a strong, regulated system level program will make our airways safer.

CHAPTER V

SYSTEM SAFETY ANALYSIS

System Safety Concepts

The high complexity and cost of new aircraft, missles, and space vehicles requires that their design meet performance specifications before any hardware is built. The result is the development of a systems approach to safety. The aircraft or missle is examined for the effects of any malfunctions on the operation of the aircraft or missle. This technique identifies those hazards which may result in system operational failures, thus focusing the design function on critical areas.

A system can be defined as an orderly arrangement of components which are interrelated and which act and interact to perform some tasks or functions in a particular environment (7). Figure 3 illustrates a generalized model of a system showing the elements "environment", "people", and "tools" combining to perform a task. It is in the interaction of these components where hazards exist and accidents occur.

The generalized system model is readily adapted to the air carrier industry. Figure 4 illustrates the generalized model in the air carrier industry, with the environment being the airways and airports, the prople being the personnel involved in the

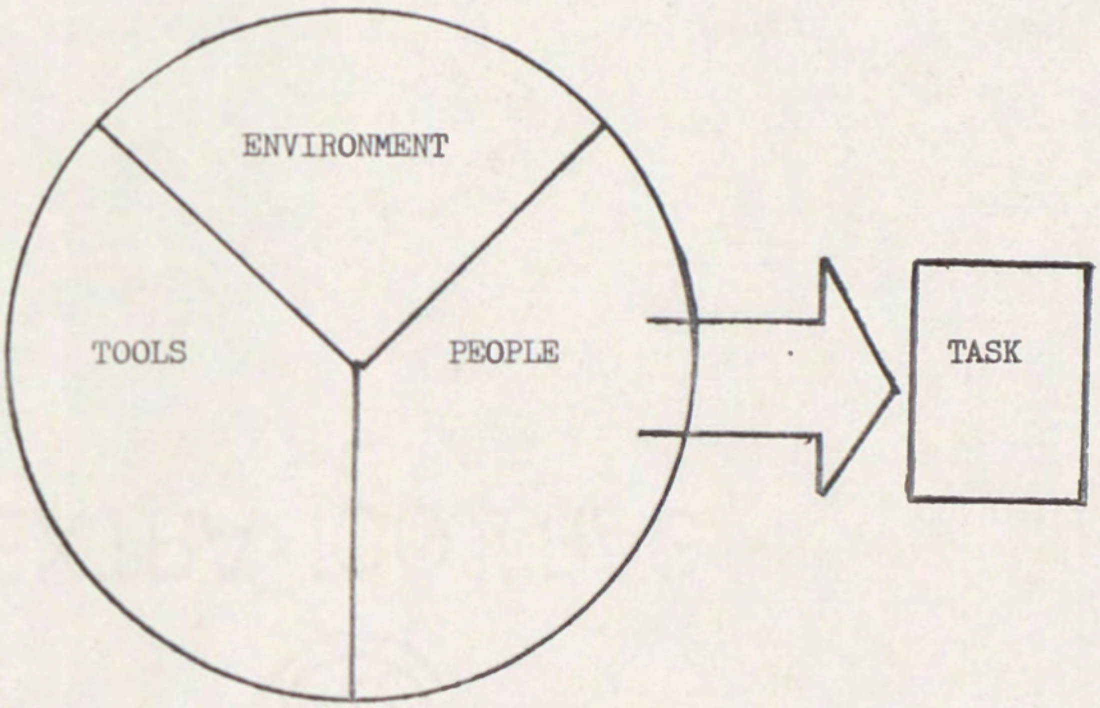


Fig. 3. Generalized System Model

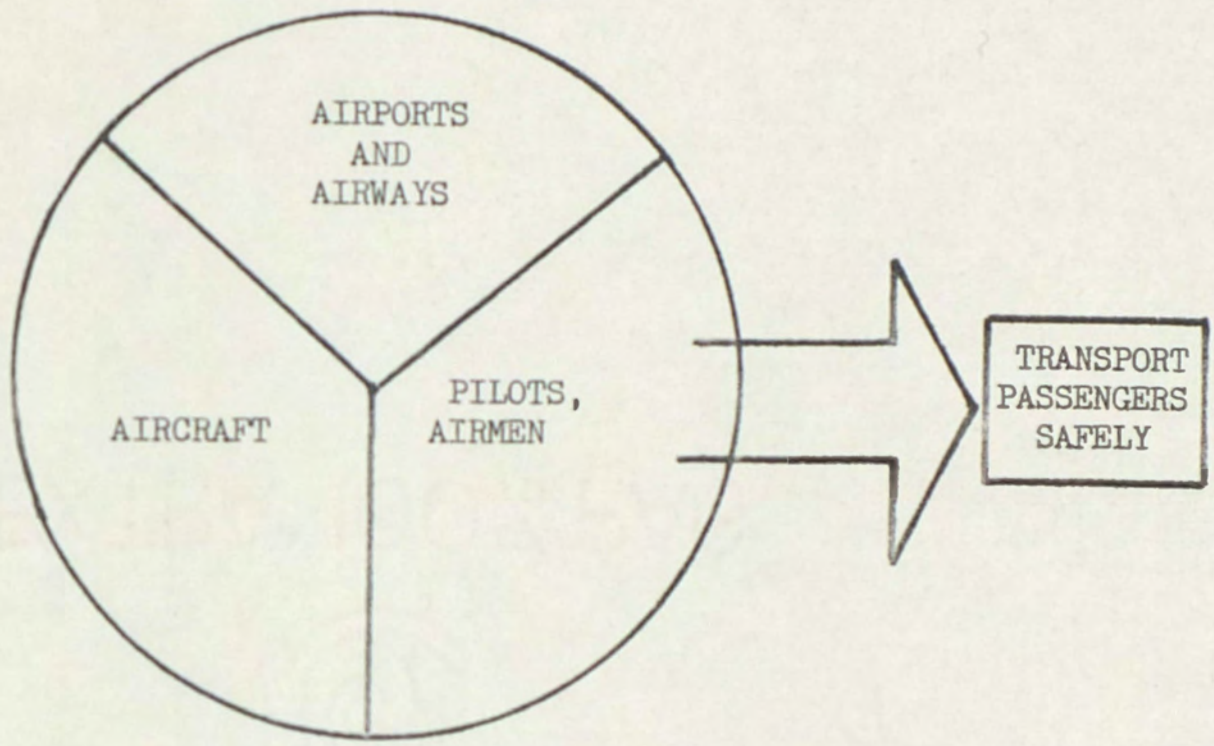


Fig. 4. Air Transportation System Model

carrier's operation, and the tools consisting of the aircraft being used. Further discussions of each component are necessary, and are provided in the following chapters.

System Safety Precedences

The actions for satisfying safety requirements in order of precedence follow the natural hierarchy of activities in the operation of an air carrier system.

The first level of activity is the design phase. The major effort throughout the design phases shall be to select appropriate safety design features.

The second level of safety activity is the design of safety devices. Known hazards which cannot be eliminated through the design shall be reduced to an acceptable level through the use of appropriate safety devices.

In cases where a hazard exists which cannot be controlled either through the design phase or a safety device, adequate warning devices must be designed to allow for their timely detection.

Following the design of warning devices, appropriate emergency procedures must be implemented to prevent personnel injury during an uncontrollable hazard occurrence.

Hazard Level Categories

Hazard recognition involves the critical examination of human, task, and environmental variables relative to accident causation. Further classification and examples are defined (8).

1. Task variables

Variables inherent or characteristic of the operation itself.

a. Mechanical failures; failure of machine or other device in aircraft or ground support units.

b. Inadequate emergency preparation; evacuation procedures may be inefficient, fire protection inadequate as a result of inefficient planning

c. Design inadequacies; unsafe design characteristics in aircraft, which are not usually detected until too late

2. Environmental variables

Variables that affect the physical or psychological climate.

a. Weather; failure of pilot to have or be given up to date weather information

b. Bird infestation; this has been a problem at several airports

c. Others such as noise levels and illumination levels in aircraft

d. Psychological climate; influenced by workplace characteristics, time, etc.

e. Hazardous materials aboard aircraft

3. Human variables

Characteristic of the operator involved.

a. Pilot error; rely on controller or instruments

b. Controller error.

c. Time.

d. Health

e. Boredom

f. Sex, age, culture, personality.

Hazard Classification

Hazards must be classified in relation to their potential for equipment damage and personal injury. The following four classifications provide a framework for the analysis and control of hazards (9).

Class I hazards are considered safe. They include conditions that will not result in personnel injury or equipment damage. Examples might include malfunctioning reclining seats, tiolets, or other miscellaneous equipment. Weather is also a safe hazard, providing prior notification has been obtained and the aircraft is equipped to fly through it.

Class II hazards are considered marginal. These hazards may degrade system performance or damage equipment, but counteraction or control can be undertaken such that seriour injury to personnel or significant damage will not occur. Examples would

include the failure of landing lights, jammed doors, contaminated food, etc.

Class III hazards are considered critical. They include hazards that will cause personnel injury or serious equipment damage. Class III hazards will require immediate corrective action for personnel or system survival. Examples might include loss of radio contact, malfunctioning radar equipment, etc.

Class IV hazards are considered catastrophic. These hazards will cause system loss, death, or seriour, irreversible injuries to personnel. Examples would include any mechanical engine failure, on board environmental systems failure, inadequate emergency procedures, pilot and controller error, design errors, hazardous materials, etc. Table 3 summarizes the hazard classification scheme presented here.

System Safety Analysis

Identification of Analysis Techniques

Safety analyses are performed to identify hazards in order to implement action for their elimination or control. The primary objectives of these analyses are as follows (10).

1. Identify hazards and determine corrective action
2. Evaluate tradeoff considerations
3. Determine appropriate safety design requirements
4. Determine appropriate operational and test requirements

TABLE 3

HAZARD CLASSIFICATION

Class	Hazard	Equipment Damage	Personal Injury
I	Safe	None	None
II	Marginal	Minor	None
III	Critical	Substantial	Transient Injury
IV	Catastrophic	System Loss	Irreversible Injury or Death

5. Follow up to determine if the qualitative or quantitative requirements have been accomplished

Qualitative and Quantitative Analysis

A qualitative analysis is utilized during the design phase to provide an assessment of the safety of a system design. A quantitative analysis provides a numerical assessment of a system design, and might involve the calculations of the probability of occurrence, or the risk of a hazard occurrence.

Preliminary Hazard Analyses

A preliminary hazard analysis is one of the first activities performed during the design phase, and will be used in imposing design criteria. Some of the areas considered during the preliminary analysis are as follows.

1. Isolation of fuel sources and storage
2. System environmental requirements
3. Effects of electrostatic discharges, electromagnetic and ionizing radiation on the system
4. Crash safety.
5. Operation and maintenance of the system
6. Manpower training and certification
7. Internal transportation features and emergency procedures
8. Fire propagation prevention
9. Equipment layout design, human engineering

Subsystem Hazard Analysis

The subsystem analysis identifies subsystem failures which would result in hazardous conditions. This type of analysis is an expansion of the preliminary hazard analysis, and determines the relationships of the safety characteristics of each component in the overall system and the effects of a failure in any one component.

System Hazard Analysis

The subsystem analysis provides the basis for a system level analysis. The interrelationships of each subsystem are studied to determine the safety problems of the total system. Examples of such system level analyses would include the following.

1. Single or combinations of failures in each subsystem which could result in a hazardous condition
2. Determination that any subsystem operating in its normal capacity will not degrade any other subsystem

Operating Hazard Analysis

As well as the actual aircraft design analyses previously discussed, analyses must be conducted to determine the safety requirements for all personnel involved in the operation of the aircraft. Further, all emergency procedures and equipment used in all phases of the operation of the aircraft must be evaluated for safety requirements. These analyses will aid in the processing of

design changes to eliminate hazards, as well as special procedures for all areas of the operational system.

Techniques of Systems Analysis

The previous sections developed a hierarchy through which systems analysis techniques should be used. This format will become important in the following discussions on Failure Mode and Effect Analysis and Fault Tree Analysis.

Failure Mode and Effect

The first step in conducting a failure mode and effect analysis is to form a diagram of the system under study showing all of its components. This makes it an easy matter to visualize the interrelationships of the components.

Once the model is drawn, a form similar to the one in Figure 5 is devised. This form allows the analyst to identify possible failure modes of each component, their classification, and their effects on the system in question. Estimates on failure frequency can be made from existing accident data, test results, or engineering judgement.

The final two columns force the analyst to question methods for detection and correction.

Fault Tree Analysis

Fault Tree Analysis was first conceived in 1972 by H. A. Watson of Bell Telephone Laboratories in connection with an Air

Component	Failure or Error Mode	Effects On			Hazard Class 1234	Failure Freq.	Detection Methods	Compensating Provisions
		Components	Sub-System	System				
Radio Out	Electrical Power Failure	Dependent on IFR Visual	Less Communi-cations capability	Minor	3	Remote	Manual Testing	Move to visual and/or instru-ment flight
Emergency Evacuation Procedure Inadequate	Emergency	Injury to personnel passeng-ers		Catast-rophic	4	Remote	Visual	Develop new Procedures
Landing Gear Failure	Jammed Closed	Possible Personal Injury	Landing System Inoperable	Catast-rophic	4	Remote	Warning Signals Visual From Ground	None other than emergency procedures.
Inoperable Restroom Facilities	Mechanical Failure in Water Lines	Discomfort to Personnel	None	None	1	Remote	Manual Testing	Repair pro-cedures at next stop.
Engine Fire	Fuel Leak with-in Engine Compartment	Critical to all system components	Critical to all system components	Critical to all system	4	Remote	Alarm Signals, Visual	Built in fire protection systems emergen-cy procedures.

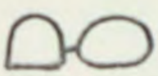
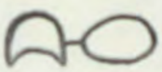
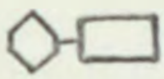
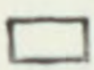
Fig. 5. Failure Mode and Effect Analysis

Force contract for study of the Minuteman launch control system (11).

Fault tree analysis starts with an undesirable event. From this point, it is necessary to reason backwards to visualize all of the ways in which it could occur. These causes then become events and the process is repeated, and so on. The process is terminated when an independent event has been reached. A fault tree is really a logic diagram tracing all the events that can lead to an undesired event. Table 4 illustrates and defines the symbols used in forming a fault tree. Figure 6 illustrates a sample fault tree analysis of a fire alarm system aboard an aircraft.

TABLE 4

FAULT TREE SYMBOLS

	AND Gate-Requires co-existence of all gate inputs for output
	OR Gate-Requires any one gate input for output, if more than one input exists, output will still occur
	PRIORITY AND Gate-Same as AND gate with the stipulation that one event must precede the other. Description is written in oval
	EXCLUSIVE OR Gate-There will be no output if two or more specified inputs co-exist. Description is written in oval
	INHIBIT Gate-If input event occurs and the condition is satisfied, an output event will be generated; if the condition is not satisfied, no output will occur. Description is written in rectangle
	An event (usually a fault or malcondition) expressed in functional terms
	An event described by a basic component or part failure (these are independent events)
	An event at which fault sequence is terminated for lack of information or consequences
	An event that is normally expected to occur
	Transfer symbol used to transfer an entire sequence of events to another part of the tree
	Another transfer symbol which transfers the functional sequence but the elements may have different numerical values

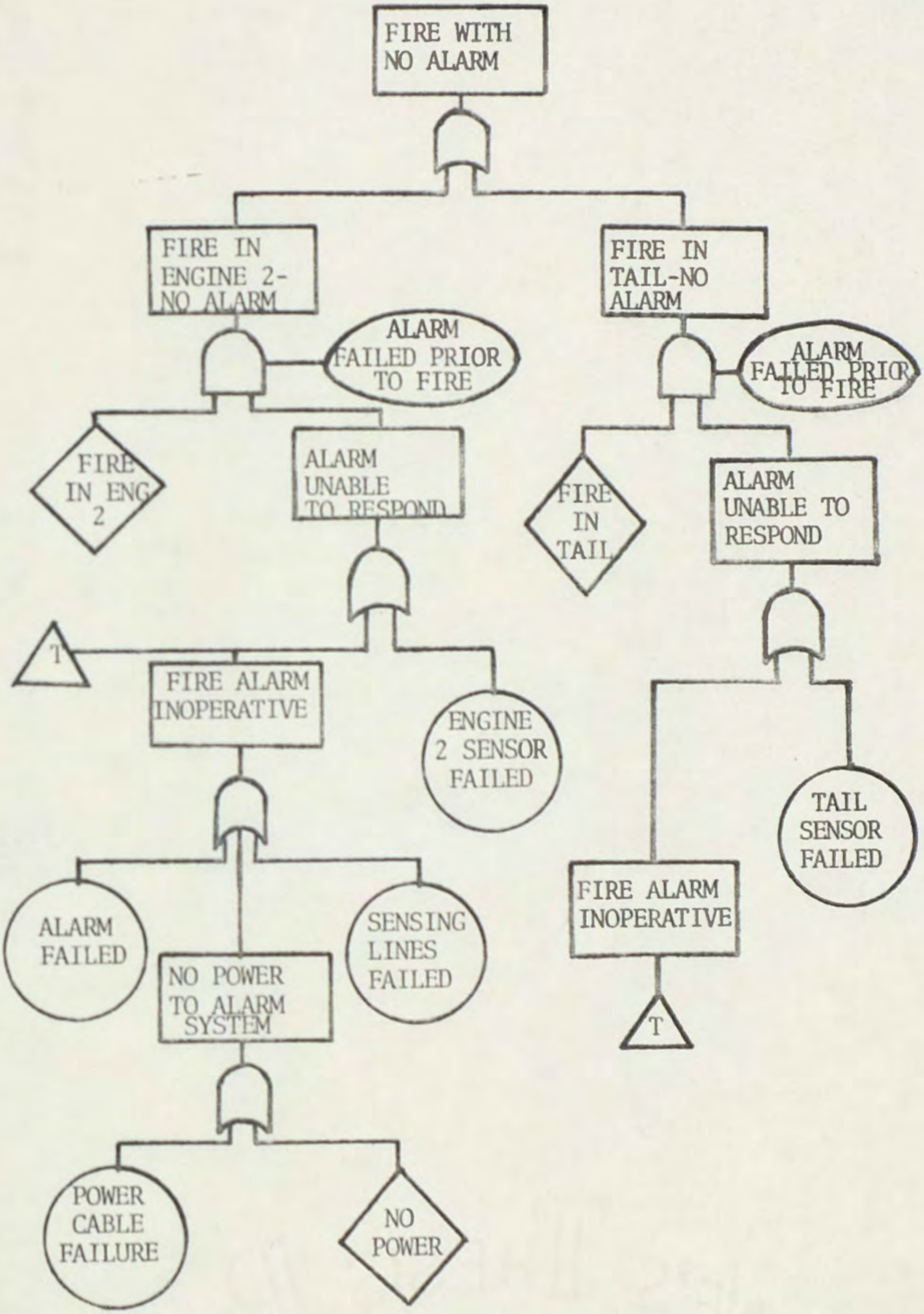


Fig. 6. Fault Tree Analysis of Aircraft Fire Alarm System

CHAPTER VI

SAFETY CRITERIA OF AIRWAYS AND AIRPORTS

Air carriers are issued an Air Carrier Operating Certificate by the FAA. For safety reasons, the terms, conditions and limits of operation, routes and airways travelled are specified in this certificate. Any change in the carrier's schedule or route must be recertified.

The equipment in use at any airport must be well known to all who may use it. An unknown change would create a hazard to any pilot attempting to use the facility. All airports must have their landing areas, lights, radio directional apparatus and like equipment inspected and given an Air Navigational Facility Certificate.

The development and acceptance of new equipment related to the operation of our airways should be regulated through a strictly controlled product assurance program, utilizing the systems analysis concepts presented in Chapter Five. Further guidelines for improved safety in ground equipment are discussed in Chapter Eight relative to aircraft procurement.

CHAPTER VII

ORGANIZATION, RESPONSIBILITY AND AUTHORITY

The objective of this section is to examine the current and future staffing requirements for typical safety organizations within the private sector of the air transportation industry. A survey was conducted during 1974 to obtain information on the organizational structure and functions of the safety departments of a representative sample of the airlines operating in the United States.

While only twenty-five percent of the air carriers in the industry responded, sufficient information was obtained to group the safety organizations of the air carriers into three basis classifications, determined primarily by the size of the air carrier itself. The largest safety organization is associated with the large international carriers. The second classification is associated with the larger regional carriers, while the third and smallest is representative of the small regional carrier. The latter, as will later be seen, represents virtually no formal safety organization at all. Figures 7, 8, and 9 illustrate the structures of the generalized safety organizations for each of these air carrier classifications, while the pages following describe the functions and responsibilities of those organizational positions. Nine di-

git occupational codes have been assigned to each position so as to provide a basis for determining standard qualifications for each position. These codes are an extension of the occupational code format used by the U. S. Department of Labor in their Dictionary of Occupational Titles. The occupational codes for the air carrier safety organizations were developed as part of the research activities of the Transportation Systems Institute at Florida Technological University previously mentioned. A detailed explanation of the code classifications used in this section are given in the Appendix of Manpower Analysis in Transportation Safety, published by the U. S. Department of Transportation in June of 1977.

In addition, four basic qualification criteria are also given for each generalized job description. The General Educational Development (GED) has six levels ranging from the application of common sense to a simple situation to the implementation of logical or scientific thinking to intellectual and practical problems. The second index, the Specific Educational Development (SED), denotes specific educational achievement levels required for safety personnel, and has six levels ranging from a high school diploma to an advanced degree. The Specific Vocational Preparation (SVP) index denotes particular in training service requirements ranging from simple demonstrations to several years of on the job experience. The final index, the Occupational License Requirement (OLR) denotes special licensing requirements for safety personnel. Again, a detailed explanation of these four indices is provided in the afore-

mentioned report.

Safety Organization of a Large International Carrier

Figure 7 illustrates the safety organization of a typical large international carrier. It is represented at the upper corporate level by a Vice-President of Safety. Reporting to the Vice-President are the Ground Safety, Flight Safety, and Airport Operations Departments. Within each department is a Director, or Manager, with a staff of analysts whose responsibilities include the collection and analysis of safety data, and the recommendation and implementation of safety policies and procedures.

It should be noted that the responsibility for the safety of the aircraft while in flight belongs to the pilot. The pilot must determine whether the aircraft is airworthy and direct any actions necessary to complete a safe flight.

Safety Organization Position Descriptions

Generalized job descriptions for the positions shown in Figure 7 are given on pages 44 through 54. Each job description indicates the primary tasks and qualifications associated with that position.

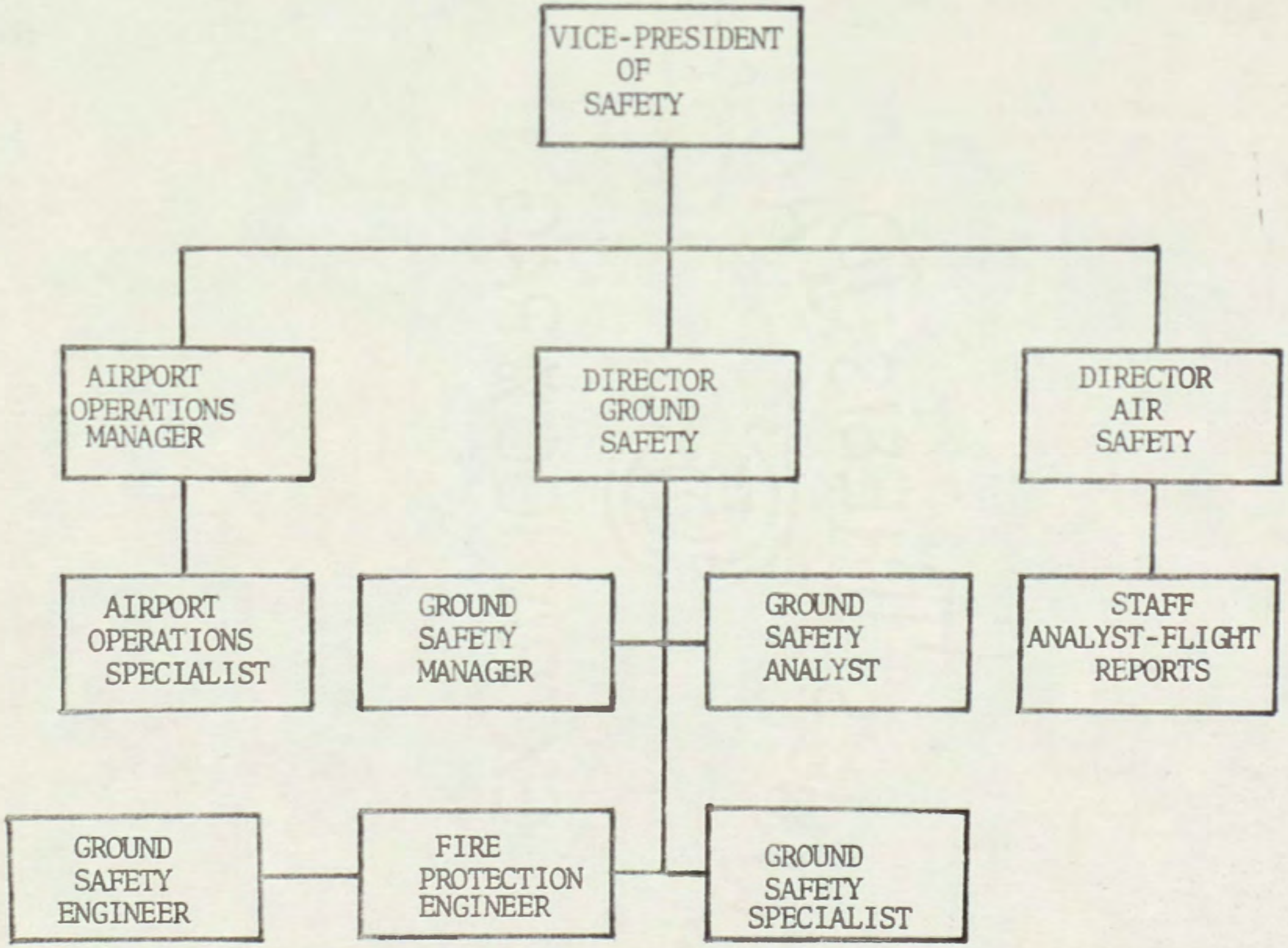


Fig. 7. Typical Safety Organization Structure - Large International Air Carrier

Job Title

Director of Ground Safety

Scope

To develop and administer the company's ground safety programs

Tasks

1. Develops and functionally directs the company's ground safety, fire prevention and damage control activities
2. Plans and functionally directs training programs in accident prevention and fire protection

Qualifications	Levels
General Education Development	6
Specific Education Development	3
Specific Vocational Preparation	8
Occupational License Requirements	6

Occupational Code

912.138.400

Job Title

Ground Safety Manager

Scope

To assist the Director of Ground Safety in all duties

Tasks

1. Assists the Director of Ground Safety in developing and functionally directing the company's ground safety plans by representing him with all divisions within a designated geographic area
2. Monitors and assists all divisions compliance with Federal, State, and Local safety, health, and fire protection regulations

Qualifications	Levels
General Education Development	6
Specific Education Development	3
Specific Vocational Preparation	7
Occupational License Requirement	6

Occupational Code

912.138.400

Job Title

Ground Safety Engineer

Scope

To develop new procedures/equipment/designs to assist company in its safety goals

Tasks

1. Develop, install, and maintain safety standards, procedures, programs, specifications and devices for all ground facilities, equipment and systems
2. Reviews equipment, facilities and systems design proposals developed by his staff, vendors and field elements
3. Tests and recommends modifications to new and existing ground equipment and facilities
4. Investigate accidents involving ground support equipment and recommends corrective action

Qualifications	Levels
General Education Development	6
Specific Education Development	3
Specific Vocational Preparation	8
Occupational License Requirement	6

Occupational Code

912.218.422

Job Title

Ground Safety Analyst

Scope

To collect data, analyze accident trends, and make recommendations for better safety performance

Tasks

1. Develops meaningful safety performance data
2. Conduct a program of continuing analysis of accident trends and causes in the company's ground operations

Qualifications	Levels
General Education Development	6
Specific Education Development	3
Specific Vocational Preparation	7
Occupational License Requirement	6

Occupational Code

912.288.420

Job Title

Ground Safety Specialist

Scope

To assist on a local level in defining safety problems and recommending methods of correction

Tasks

1. Develops plans and programs to improve overall safety performance of ground operations
2. Evaluates new accident prevention methods
3. Participates in accident and special investigations as requested

Qualifications	Levels
General Education Development	6
Specific Education Development	3
Specific Vocational Preparation	7
Occupational License Requirement	6

Occupational Code

912.288.432

Job Title

Fire Protection Engineer

Scope

To assist the Director of Ground Safety in maintaining adequate ground safety apparatus to reduce accidents

Tasks

1. Provide assistance in developing and formulating ground safety policies and programs to reduce employee accidents
2. Establish an adequate fire prevention program
3. Educate employees in existing hazards and developing safety consciousness
4. Participate in Union/Company safety meetings
5. Studies accident hazards and health risks and establishes the corrective or preventive procedures

Qualifications	Levels
General Education Development	6
Specific Education Development	3
Specific Vocational Preparation	8
Occupational License Requirement	6

Occupational Code

912.368.432

Job Title

Director of Air Safety

Scope

To develop methods and programs to improve flight safety program

Tasks

1. Develops methods of monitoring and evaluating trends in aircraft or operational irregularities and recommends corrective action
2. Evaluates flight equipment and procedures for compliance with safety standards
3. Keeps management advised of developments in flight safety and recommends appropriate management action

Qualifications	Levels
General Education Development	6
Specific Education Development	3
Specific Vocational Preparation	8
Occupational License Requirement	6

Occupational Code

912.218.430

Job Title

Staff Analyst-Flight Reports

Scope

To maintain accident files and to analyze and prepare accident reports

Tasks

1. Prepares procedures for reporting of in-flight irregularities
2. Maintains accident files
3. Analyzes, prepares and coordinates written reports of aircraft incidents as required by FAA and NTSB
4. Supervises the collection and handling of in-flight irregularity reports and other permanent flight records

Qualifications	Levels
General Education Development	6
Specific Education Development	3
Specific Vocational Preparation	7
Occupational License Requirement	6

Occupational Code

912.388.440

Job Title

Airport Operations Manager

Scope

To maintain current airfield data and to develop standards for air field traffic control

Tasks

1. Develops company standards for aircraft parking and ground maneuvering
2. Responsible for acquisition and maintenance of current airport physical data, operating restrictions and limitations which may effect operating policies or procedures including necessary airfield obstructions data

Qualifications	Levels
General Education Development	6
Specific Education Development	3
Specific Vocational Preparation	8
Occupational License Requirement	6

Occupational Code

912.118.421

Job Title

Airport Operations Specialist

Scope

To assist Airport Operations Manager in his duties

Tasks

1. Develops company aircraft parking standards
2. Personal inspection of airports
3. Maintains current airport files and assists in advertising of airfield changes

Qualifications	Levels
General Education Development	6
Specific Education Development	3
Specific Vocational Preparation	7
Occupational License REquirement	6

Occupational Code

912.388.460

Safety Organization of a Large Regional Carrier

The typical organization structure of a large regional air carrier is illustrated in Figure 8. Its internal organization is similar to that of the large international carrier, however the number of personnel involved is smaller. There is an overall Director of Safety who reports to the Vice-President of Operations. The organization is then divided into flight safety and air safety departments, each with its own manager. The functional responsibilities of the organization as a whole are the same as with the large international carrier, with the operations related activities being shared by each department.

Safety Organization Position Descriptions

Generalized job descriptions for the positions shown in Figure 8 for the typical large regional carrier are given on pages 58 through 62. The same occupational codes and qualification indices are given.

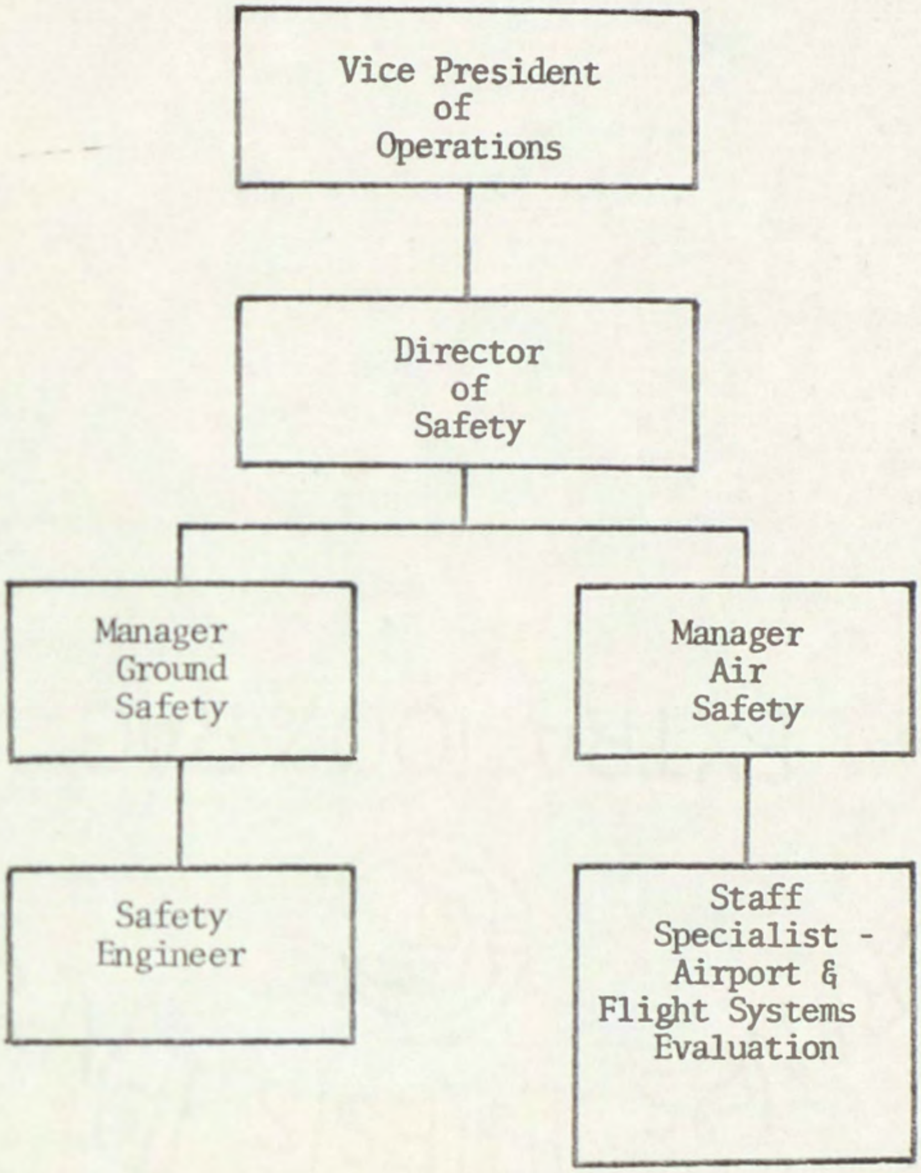


Fig. 8. Typical Safety Organization Structure - Large Regional Air Carrier

Job Title

Director of Safety

Scope

To develop and functionally direct the company's ground and air safety activities

Tasks

1. Develops, recommends the administration of policies, plans, and programs related to ground and flight safety
2. Conducts surveys and inspections of facilities with regard to safety
3. Develops and directs the conduct of educational safety awareness training programs
4. Investigates accidents as chairman of company investigating team

Qualifications	Levels
General Education Development	6
Specific Education Development	3
Specific Vocational Preparation	8
Occupational License Requirement	6

Occupational Code

912.138.400

Job Title

Manager of Air Safety

Scope

To functionally assist the Director of Safety in developing and implementing the company's flight safety activities

Tasks

1. Develop and administer flight and ground safety programs
2. Conduct safety inspections
3. Represent company with FAA, ATA, LATA, etc.
4. Compile, analyze and report flight accident statistics
5. Identify potential hazardous situations and initiate corrective action

Qualifications	Levels
General Education Development	6
Specific Education Development	3
Specific Vocational Preparation	8
occupational License Requirement	6

Occupational Code

912.238.430

Job Title

Staff Specialist

Scope

To assist the manager of Air Safety in compiling information on accidents and preparing reports

Tasks

1. Prepares procedures for reporting of in flight irregularities
2. Supervises the collection of in flight reports and flight records
3. Maintains accident files
4. Analyzes, prepares written reports on accidents for FAA

Qualifications	Levels
General Education Development	6
Specific Education Development	3
Specific Vocational Preparation	7
Occupational License Requirement	6

Occupational Code

912.288.440

Job Title

Manager of Ground Safety

Scope

To functionally assist the Director of Safety in the company's ground safety activities

Tasks

1. Develop policies for accident prevention programs in ground operations
2. Develop plans for education and promotion of programs
3. Prepares and conducts safety surveys
4. Keep abreast of new developments in apparatus

Qualifications	Levels
General Education Development	6
Specific Education Development	3
Specific Vocational Preparation	8
Occupational License Requirement	6

Occupational Code

912.128.400

Job Title

Safety Engineer

Scope

To assist the Manager of Ground Safety in developing ground safety facilities and procedures

Tasks

1. Develop, install and maintain safety standards and programs
2. Review equipment and system design proposals
3. Tests and recommends modifications to new and existing ground equipment
4. Investigate accidents involving ground equipment

Qualifications	Levels
General Education Development	6
Specific Education Development	3
Specific Vocational Preparation	8
Occupational License Requirements	6

Occupational Code

912.168.422

Safety Organization of a Small Regional Carrier

As indicated in Figure 9, the small regional air carriers have virtually no professional safety staff other than one person who serves as the focal point for the coordination of the company's safety activities. This is not to say that there is no safety activity. One airline's personnel director stated that a formal safety staff tends to become self serving, with safety becoming an end in itself. Another disadvantage to a formal safety staff is that the functional and operational personnel tend to disassociate themselves from safety activities, leaving them up to the safety staff. This type of structure presents an opportunity for very close communication between the functional and management personnel. Since all the company's planes are based in a central location, the pilots see the other operational personnel daily, and reports any problems which will receive immediate attention.

Safety Organization Position Descriptions

The job description on page 64 gives the tasks and qualifications for the Director of Safety for the small regional air carrier. As before, this description includes the occupational codes and qualification indices used in the other position descriptions.

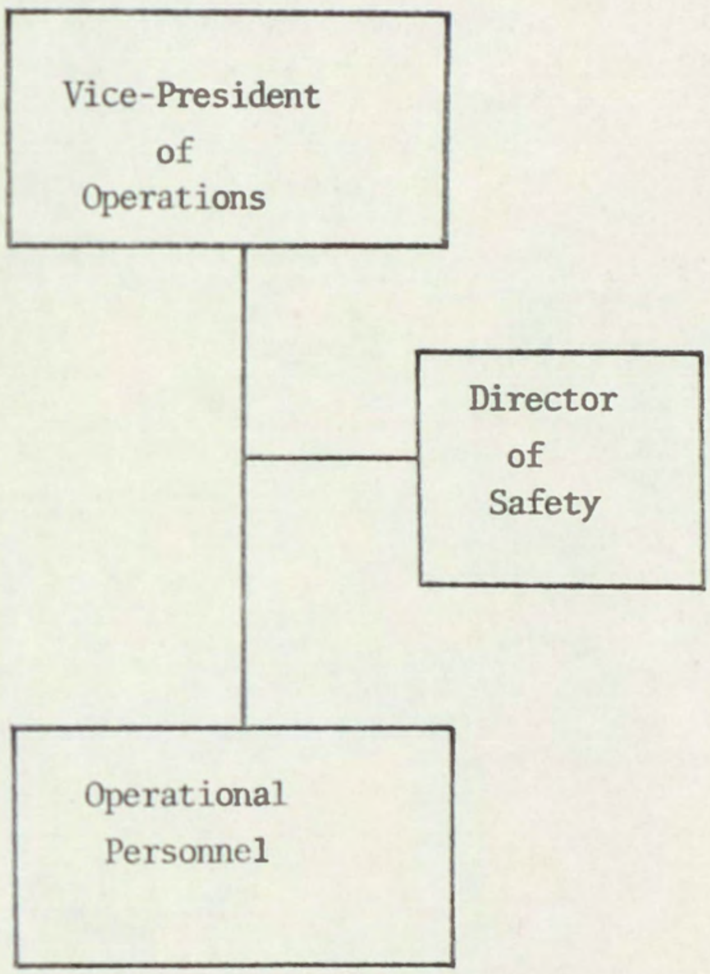


Fig. 9. Typical Safety Organization Structure-Small Regional Air Carrier

Job Title

Director of Safety

Scope

To develop and maintain the company's ground and air safety activities

Tasks

1. Develop, recommend, and coordinate approved policies, plans, etc in air transportation safety
2. Conduct surveys and inspections
3. Develop and conduct safety awareness programs
4. Analyze and interpret reports on flight accidents
5. Investigates accidents

Qualifications	Levels
General Education Development	6
Specific Educational Development	3
Specific Vocational Preparation	8
Occupational License Requirement	6

Occupational Code

912.138.400

CHAPTER VIII

HAZARDS ASSOCIATED WITH AIRCRAFT

Prior to placing an aircraft into the nations airways, there must be some assurance that it will operate safely. This requires that the problem of safety be studied at the concept formulation, engineering development, production and operational phases of the aircraft's life, utilizing the system analysis concepts presented in Chapter Five.

The concept formulation phase requires the identification of areas of possible safety consideration. The safety activities in the engineering development phase qualify and quantify the conceptual problems.

Vendors supplying aircraft to the airlines must identify critical production and assembly procedures and facilities as well as testing and inspection requirements that may affect the safety of the aircraft. A well planned quality assurance system must be contractually defined to insure that safety achieved during the design phases is maintained through production.

The operational phase should include an ongoing Product Improvement Program (PIP). This program will monitor the safety of the aircraft in operation and formulate any necessary changes in its design or safety features. Such a program would also allow

for the continual upgrading of equipment as advanced technology required.

A program of quality control for the procurement of aircraft is necessary to achieve a base to build an overall safety program on. If the aircraft is unsafe by design, the other safety activities become meaningless. The FAA has the responsibility for the certification of aircraft. A formal organization along the lines of the Department of Contract Administrative Services (DCAS) would provide for a maximum level of safety activity during aircraft procurement.

CHAPTER IX

CONCLUSIONS AND RECOMMENDATIONS

The stated purpose of this thesis was to develop a hypothetical model of a system safety program for the commercial air carrier industry. The model includes the utilization of systems analysis techniques discussed in Chapters Four and Five, as well as the organizational framework for system-wide direction of safety activities as presented in Chapters Four and Seven.

An evaluation of the safety programs in existence determines that most of its activities result from after the fact analysis of accident data. Reports on accidents are analyzed to determine if any trends exist. If it can be determined that one does, then actions are taken to eliminate or reduce the hazards involved. The same is true for the manufacturers of the aircraft and related ground equipment.

The primary recommendations of the thesis are summarized as follows.

1. A formal system-wide System Safety Program Plan (SSPP) as presented in Chapter Four
2. A formal quality assurance system for all phases of aircraft and ground equipment procurement as presented in Chapter Eight

3. Complete conversion to a computerized national air traffic control system as directed in Chapter Three

The air carrier system in the United States today has the best safety record of any in the world. But the potential for loss of life is so great in only one accident, that it is imperative that systems like those described in this thesis be implemented if this safety record is to be maintained.

FOOTNOTES

1. Poyntz Tyler, Airways of America (New York: The H. W. Wilson Co., 1958), p. 17.

2. U. S. , Department of Transportation, Summary of National Transportation Statistics (Washington, D. C.: Government Printing Office, 1974), p. 18.

3. U. S., Department of Transportation, Federal Aviation Administration 8th Annual Report (Washington, D.C.: Government Printing Office, 1966), pp. 3-12.

4. Gordon D. Friedlander, "At the Crossroads in Air Traffic Control," IEEE Spectrum 7 (June 1970): 26-40.

5. U. S., Department of Defense, System Safety Program for Systems and Associated Subsystems and Equipment: Requirements for (Washington, D.C.: Government Printing Office, 1969), pp. 5-7.

6. John K. King, "Air Safety As Seen From the Tower," IEEE Spectrum 12 (August 1975): 67-71.

7. J. L. Rect, "System Safety Analysis-A Modern Approach to Safety Problems," National Safety News 4 (December 1975): 21-23.

8. Ibid., p. 25.

9. Ibid., p. 26.

10. U. S., Department of Defense, System Safety Program for Systems and Associated Subsystems and Equipment: Requirements for (Washington, D.C.: Government Printing Office, 1969), p. 7.

11. J. L. Rect, "System Safety Analysis-A Modern Approach to Safety Problems," National Safety News 4 (December 1975): 22.

BIBLIOGRAPHY

Blumenthal, Sherman C. Management Information Systems: A Framework for Planning and Development. Englewood Cliffs: Prentice-Hall, 1969.

Burkhardt, Roger. The Federal Aviation Administration. New York: Frederick W. Praeger, 1967.

Friedlander, Gordon D. "At the Crossroads in Air Traffic Control." IEEE Spectrum 7 (June 1970): 26-40.

Hammer, Willie. Handbook of System and Product Safety. Englewood Cliffs: Prentice-Hall, 1972.

King, John K. "Air Safety As Seen From the Tower." IEEE Spectrum 12 (August 1975): 67-71.

Malasky, Sol W. System Safety Planning/Engineering/Management. Rochelle Park: Prentice-Hall, 1972.

Poyntz, Tyler. Airways of America. New York: The H. W. Wilson Co., 1958.

Rect, J. L. "System Safety Analysis-A Modern Approach to Safety Problems." National Safety News 4 (December 1965): 22.

Transportation Safety Institute. Glossary of Aeronautical Terms. Oklahoma City: Transportation Safety Institute, 1973.

U. S., Department of Defense. System Safety Program for Systems and Associated Subsystems and Equipment: Requirements for. Washington, D.C.: Government Printing Office, 1974.

U. S., Department of Transportation. Federal Aviation Administration 8th Annual Report. Washington, D. C.: Government Printing Office, 1966.

U. S., Department of Transportation. Summary of National Transportation Statistics. Washington, D.C.: Government Printing Office, 1974.