Special Edition

www.FSinfo.org

March 2003

Flight Safety Information

Essays In System Safety

Editor: Curt Lewis, P.E., CSP

FSI Contents

March 2003

Essays in System Safety

Flight Safety Information

Published by www.FSInfo.org

Managing Editor
Curt Lewis, PE, CSP
Curt.Lewis@fsinfo.org

Associate Editor
Ryan Boerboom
boerbor@erau.edu

Webmaster
Randy Engberg
Randy.Engberg@fsinfo.org

FSINFO.ORG

P.O. Box 155602
Fort Worth, TX 76155
Phone: 817-685-9198
Fax: 817-795-3771

Special Edition

Included in this issue are several excellent essays written by students in my recent graduate System Safety course. Their hard work is very appreciated.

Thanks,
Curt.

ISO 9000

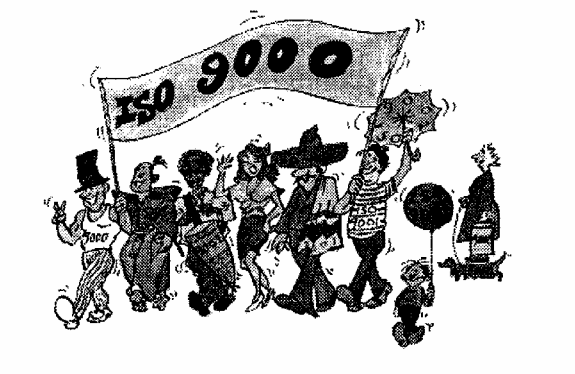
System Safety
ASCI 611

Dave Bastian

March 5, 2003

ISO 9000 is a family of generic standards and guidelines which focus on the promotion of "quality management" and what an organization does to ensure that its products or services meet a set of standards or guidelines and most importantly "what the customer requirements are" (ISO). If an organization has in place a quality assurance program, such as setup and outlined in the ISO 9000 standards and guidelines, the processes or practices, which govern the output of their product or services, will be of quality and most importantly meet their customers needs. The size of an organization is immaterial because quality products and services are required by all customers worldwide and these guidelines can be applied to organizations large or small to ensure management is committed to quality, as well as customer needs (ISO). Organizations who employ ISO 9000 guidelines and standards convey to customers, their commitment to quality products and services, and also be assured of being able to compete favorably in the market place and maintaining or increasing their market share.

ISO 9000 is rapidly becoming the most popular quality standard in the world for quality management systems. ISO headquarters, currently located in Geneva, Switzerland, was founded in 1946 by the United Nations who recognized the need for standardization of products and services on a global level. International trade could and would be affected if a global standard could not be implemented and practiced by all organizations. Currently more than 90 countries worldwide employ ISO 9000 as their national standard (ISO). Industry standards came about due to a lack of quality of



products and service, consequently resulting in customer dissatisfaction. We as the purchaser of those products or services have the right to expect quality products and services and state those needs to manufactures or service organizations responsible for them. These demands or customer requirements must be made to and received by a responsible and committed management. Managements duty and responsibility is to have in place or implement a quality assurance program that will be responsive to the customer's needs and ensure that quality of goods and services are being address at all levels.

Quality is defined in the ISO 8402 as, "totality of characteristics of an entity that bare on its ability to satisfy stated and implied needs." This definition of quality places the responsibility of customer relations on an organization wishing to be ISO 9000 compliant. During the "pre-industrial revolution quality was based upon a visual appearance, durability, and usability" (QASNA). The old adage, "kick the tires and light the fires," mentality was the accepted standard. If it looks good, and sounds good, it must be of good quality. This visual perception of quality was a good way of gauging the quality of a product or service, until a problem surfaced. The question of the day then was, "how do we take care of this; who do we call; who is

responsible for this?" Without a quality management program in place, such as ISO 9000, finding a suitable remedy could prove difficult or nonexistent. The industrial revolution was a dynamic period of time for technology and the mass production of goods and services (QASNA). This need for an increase of goods and services made apparent the lack of quality throughout industries. The production management processes incorporated during those times emphasized "detection rather that prevention" (QASNA). Customers expected quality to be built into the processes, but management had different expectations regarding when and where quality fit in. It was the Japanese's recognition of the aspects of quality: namely "reliability, durability, cost effectiveness, and customer satisfaction," that resulted in the quality assurance culture we have today (QASNA). The management's attitude, for those organizations that utilize ISO 9000, is one in which the manufacturing community, suppliers, and consumers work closely to ensure that products and services comply with industry standards. ISO 9000 organizations are committed and responsive to the customer's needs and designing quality into the products and services. Those organizations that employ a quality management program that effectively manages production and services in response to customer and supplier needs, further enhance the quality culture and ensure themselves as a competitor in their industry.

Quality is a general term and needs a way to be measured so as to imply value. The ISO 9000 standards, if implemented by any organization, are a way is to impose a set of standards and raise the bar of quality and consumer confidence. Developing standards and processes that can be improved upon, allows quality to become a measurable term, which consumers can acknowledge and rely on. Implementing a quality management program based upon a known International Standard such as ISO 9000 benefits both the organization and the consumer in many ways. Customers' will benefit by doing business with an organization with a commitment to quality and service. Organizations will experience an, "increase in market share, reduction in customer complaints, increase in profits, more demand for their products and services, and better working conditions for employees"(ISO).

ISO 9000 standards consist of several quality assurance models, which give organizations a choice of models in which to organize their processes. The standards are the ISO 9001, 9002, and 9003. The differences are not in quality, but one of processes, which may vary amongst industries. The chart below shows the layout of the ISO 9000 family of standards prior to the last revision, 1994:

ISO 9000 Family of Standards

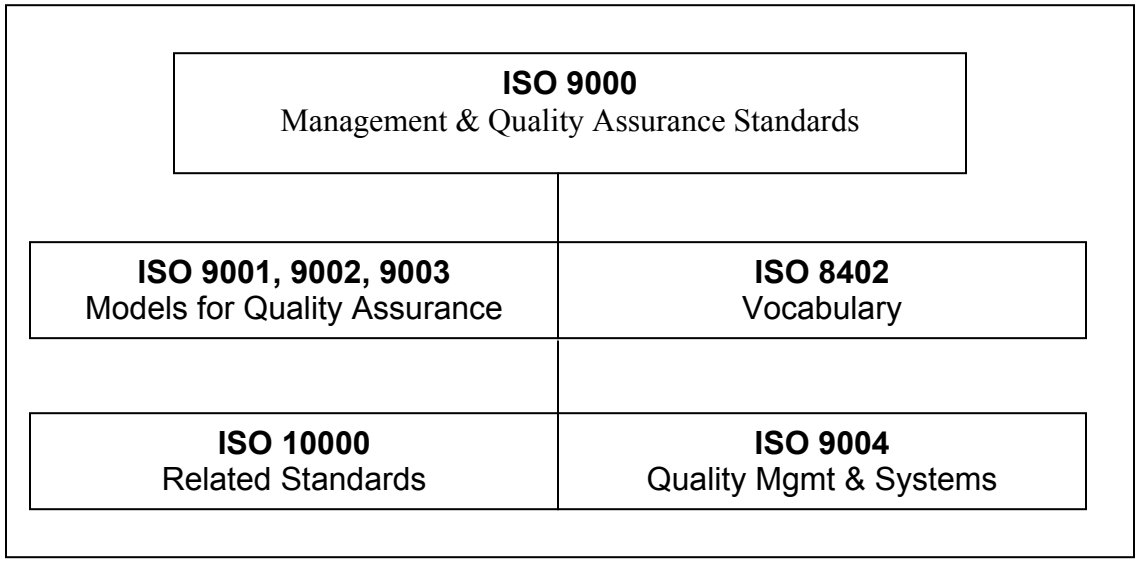


Chart 1. QASNA, Inc., ISO 9000 Auditor/Lead Auditor Course, 1999.

Since 1994, a new revision has been developed, combining ISO 9002 and 9003 into ISO 9001:2000. ISO 8402 has been combined with parts of ISO 9000 to become ISO 9000:2000. ISO 9004 and 10000 have also been revised to 2000 standards. These new standards become effective December 2003 and organizations have until then to comply (ISO). Many new changes have been incorporated and involve a better "process model, increased management responsibility to continually improve their quality management processes, greater customer involvement, and increased documentation for auditing results" (ISO).

An organization deciding to implement ISO 9000 quality management standards has obviously defined their goals and needs in the area of customer satisfaction. The next step is to set up a quality management program utilizing the requirements of ISO 9001, ISO 9002, or ISO 9003. The guidelines chosen depend entirely on the needs of the organization and its goals. There are many resources available to assist in the implementation of an ISO 9000 quality management program. Once the program is in place, and has passed all internal evaluations, the program will have to be audited by an external, third party. This external, third party will have been trained and certified to evaluate and certify ISO 9000 quality management programs. If the organizations quality management program meets or exceeds ISO 9000 standards, a certificate is issued and the organization to allow to register its name amongst other ISO 9000 organizations worldwide (Praxiom Research Group).

In today's market place, regardless what country it is, quality products and services offered at every level must be of good quality as defined by the end user. Organizations that have a quality management program in place will be able to provide consumers with quality products

and services, while at the same time receiving extensive benefits themselves in the marketplace locally or even globally. Implementing and receiving ISO 9000 certification puts an organization out front for consumers to seek out quality products and services.

References

International Organization for Standardization. (2002). Changes Made in the 2000 version of ISO 9000. Retrieved February 18, 2003, from http://isoeasy.com/changes made_ in_the_2000_version.htm.

International Organization for Standardization. (January 13, 2003), ISO Easy. Retrieved January 21, 2003, from http://www.isoeasy.org

International Organization for Standardization. Maintaining The Benefits and Continual Improvement. Retrieved January 27, 2003, from http://www.iso.ch/iso/en/iso 9000-14000/iso 9000/selection_use/ Maintaining.html

International Organization for Standardization. Quality Management Principles. Retrieved January 27, 2003, from http://www.iso.ch/iso/en/iso 9000-14000/iso 9000/qmp.html

International Organization for Standardization. The Basics. Retrieved January 27, 2003, from http:// www.iso.ch/iso/en/iso 9000-14000/tour/plain.html

International Organization for Standardization. The Basics. Retrieved January 27, 2003, from http:// www.iso.ch/iso/en/iso 9000-14000/tour/busy.html

National Aeronautics Space Administration. (January 21, 2003). Quality Management Systems. Retrieved January 27, 2003, from http://iso 9000.nasa.gov

Praxiom Research Group. (May 25, 1997). ISO 9000 Introduction, May 30, 2002. Retrieved January 15, 2003, from http://connect.ab.ca.-praxiom/index.htm

ISO 14000

By

Marty Maughon

Submitted in Partial Fulfillment of the Requirements of
MAS611 Aviation System Safety
Winter 2003

Embry-Riddle Aeronautical University
Fort Worth Resident Center
3/2003

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

The dependency on product usage between nations has grown tremendously. Travelers would like their electronic equipment, credit cards, and other accessories to work in other countries without altercation. The International Organization for Standardization (ISO) is a worldwide federation of national standards that establishes standards for countries to follow. This paper will examine ISO 14000 as well as look at the history and organization of ISO.

Chapter II

Review of Relevant Literature

What is ISO?

The International Organization for Standardization (ISO) is a worldwide federation of national standards with one member representing each of 140 countries. The organization was established in 1947 and is based out of Geneva, Switzerland. ISO is a non-governmental organization that promotes the development and implementation of voluntary international standards, both for particular products and for environmental management issues.

ISO's name is derived from the Greek work isos, meaning, "equal." The prefix "iso" is used in English words to denote "same or equal", such as "isometric" and "isonomy." The translation for ISO is the same in every language which is easier than translating an acronym for each country.

ISO Standards

ISO standards are developed through a voluntary, consensus-based approach. These standards are agreements

containing technical specifications to be used as guidelines to ensure that materials, products, and processes are fit for their purpose. The ISO member countries decide on a position concerning the new standards and each country's positions are then negotiated with other member countries. After negotiations, draft versions of the standards are sent out for review by each country. The country then must cast its final vote on the rough drafts. Each country can include various organizations such as industry, government, and other vested-interest parties, including various non-government organizations to decide the final vote for that country.

ISO Membership

Currently, ISO has awarded over 35,000 ISO 14000 certificates in 112 countries. Membership is divided into three categories: member body, correspondent membership, and subscriber membership. Only one member body of each country can be admitted to ISO. This group shares the country's predominant view on standardization for the country. Each member body takes responsibility for informing interested parties of relevant international standardization information for their country, ensuring the overall view of the country's interest is presented during

negotiations, and providing a corresponding country's financial commitment to support the central operations of ISO, through payment of membership dues. Member bodies can take part and exercise full voting rights on any technical committee and policy committee of ISO.

Correspondent members are usually countries that have not yet fully developed national standards. Correspondent members do not take an active role in the technical and development work, but are permitted to be kept informed about technical and policy information of interest to them.

ISO has also established a third category called subscriber membership, for countries with very small economies and are less affected by international standardization. Subscriber members are allowed to pay reduced membership fees that enable them to maintain contact with international standards developed by the organization.

ISO 14001

The ISO 14001 standard requires that an organization put in place and execute a series of practices and procedures that result in an environmental management system. ISO 14001 is not a technical standard, unlike many ISO standards, and does not replace technical requirements

or regulations. It also does not set prescribed standards of performance for organizations. According to the EPA, the major requirements of an EMS under ISO 14001 include:

- A policy statement including commitments to prevent pollution, and to continually strive to prevent pollution in accordance with applicable statutory and regulatory requirements.
- Identification of organization’s activities, which might impact the environment, including those that are not regulated.
- Setting objectives for the environmental management system.
- Implementing the EMS (environmental management system) to meet these objectives. This includes activities like training employees, establishing work instructions, and actual metrics to measure the targets.
- Establishing a program to periodically audit the operation of the EMS.
- Checking and taking corrective action when deviations from the EMS occur, including periodic evaluations of the organization's compliance with applicable regulatory requirements.

- Undertaking periodic reviews of the EMS by top management to ensure its continuing performance and making adjustments to it, as needed.

ISO 14000 Sections

The Standard Proposed

Many companies conduct environmental audits of their facilities to see if they conform to applicable local, state, and federal regulations. However, these audits do not guarantee continuous improvement or future conformance. A well-established environmental management system must be implemented to ensure continuous improvement. The basis of ISO 14001 is to provide the minimal structure for such a system. An ISO 9000 system can be used as the model of a single management system that addresses both quality and environmental issues. Finally, you can use the proposed ISO 14001 for several purposes, such as, creating an EMS, auditing an EMS, seeking third-party certification, seeking customer recognition of an EMS, and declaring an EMS to the general public.

Requirements

Section four contains requirements that have to be met. The word "shall" means that specific action must be

taken in order to comply with the standard. Thus, a well-documented EMS can be demonstrated to an auditor as being in compliance and effective.

Environmental Policy

Management must write and make known a company wide policy on environmental issues. The policy must address issues on anything that may impact the surrounding environment, such as noise, quality of work life, and quality of life. Therefore, environmental policy must be written relevant to the size and nature of the company and the impact it has on the environment. One objective must state that continuous improvement is one of the strategic goals of the company. The company must also include in its policy that it will comply with all relevant regulations. The company policy must make provisions for reviewing policy and timelines for future reviews which, include the stated targets and objectives. Employees and even the public must be made aware of the policy.

Planning

Planning begins by defining the company can control the environmental results of its operations, products, and services. Then, the company must produce an updated list of

environmental regulations and requirements that may apply to the company. This information is then used to begin setting targets and objectives.

Targets and objectives should be measurable to auditors. In addition, it must be taken into consideration the impacts the company has that can be controlled economically. Also, the concerns of other outside parties have to be considered while adhering to the environmental management policy the company has implemented.

Each target and objective is then assigned to a specific job title for control and continuous improvement. A specific timeframe will have to be created. As new projects or production methods are adopted, the EMS plan will have to be changed or expanded to include these developments.

Implementation and Operation

Just like ISO 9000, lines of responsibility must be defined and resources must be provided to get the job done. Top management must assign a manager as the official EMS coordinator. This coordinator is responsible for ensuring implementation and then regularly reviewing the EMS and reporting to management. All of this has to be documented.

All employees that can have a significant impact on the environment have to be trained to meet identified levels of skills and knowledge. This is very similar to the training requirements of ISO 9000.

In addition, training must be given to all employees on the importance of conformance to the company's environmental policies and procedures, the type of impacts the company has on the environment, and the responsibility for controlling those impacts and potential damage and consequences from noncompliance.

Any communication internal to the organization concerning environmental issues shall be documented, as well as, implementing a formal system for recording and acting on communications received from external sources, such as customers, regulators, environmental groups, etc. Likewise, a formal procedure is needed for releasing environmental information to the public.

An environmental control plan has to be developed for daily operations. Such a plan would be very similar to the quality control plans required in the 1994 version of ISO 9000. Flow Charts would be used to identify parts of your process where environmental control is required. Each of these points would be listed on the plan along with the criteria to be met, and how to react if they are not met.

In addition, communication channels used to inform suppliers and contractors of the company's requirements should be included.

Unique to ISO 14001 is the need for a procedure to cover emergencies. This allows management to assess the damage while working to correct the situation. After any accident or emergency is corrected, the management should review what happened and decide how to prevent reoccurrence and whether procedure should be changed.

Checking and Corrective Action

After a problem has been identified, a plan for corrective action must be developed. First a system must be set up where key environmental characteristics are measured and recorded. These are done in a fashion similar to an SPC system, that is, a regularly scheduled activity assigned to specific people. Then the written data has to be handled, analyzed, and stored under an ISO 9000 procedure for quality records. In addition, any measurement equipment will come under an ISO 9000 procedure for the maintenance and calibration measuring devices.

ISO 14000 corrective action procedures must identify when to react, who responds, and what actions should be taken. The ISO 9000 version of this can be used to meet

this requirement. At least annually, you should perform an internal audit of the complete EMS. The procedure for this will be identical to those required under ISO 9000. The key difference is that the internal auditors will need to have knowledge, experience, and/or training in environmental assessment. They need to understand why a particular characteristic is being checked and what potential impacts it could create. Thus, ISO 9000 internal auditor training or lead assessor training is recommended, followed by a seminar on environmental assessments.

Management Review

At regular intervals, usually at least once a year, your top management need to review the complete EMS for completeness and effectiveness. This review will consist of the results of internal audits, reports on new requirements and regulations, and the management's discussion of the strategic plan for the company. Then upper management decides whether to modify or change the existing EMS to better meet the changing needs and targets of the company. This also must be documented.

Conclusion

The five basic requirements of an EMS really are a combination of environmental concerns and ISO 9000 requirements. An interesting aspect of ISO 14001 is the proposed idea of written targets and objectives. This would make conformance and improvement obvious to anyone that took the time to look at a series of charts. Employees would gather regular readings of environmental impacts. These could be charted and posted for everyone to see. The target for each chart would be noted. Thus, continuous improvement would be a regular part of the EMS system.

ISO 14001 will not help you when auditors come from organizations like the Environmental Protection Agency (EPA) or Occupational Safety and Health Administration. Conformance to ISO 14001 will not guarantee conformance to regulations. Management must ensure the company sets targets and objectives to ensure such continuous conformance.

REFERENCES

International Organization for Standardization. Retrieved February 26, 2003, from the World Wide Web: http://www.iso.ch/iso/en/aboutiso/introduction/whatisISO.html

International Organization for Standardization. Retrieved February 26, 2003, from the World Wide Web: http://www.iso.ch/iso/en/aboutiso/introduction/index.html

International Organization for Standardization. Retrieved February 26, 2003, from the World Wide Web: http://www.iso.ch/iso/en/aboutiso/introduction/whoisISO.html

International Organization for Standardization. Retrieved February 26, 2003, from the World Wide Web: http://www.iso.ch/iso/en/iso9000-14000/tour/magical.html

National ISO 9000 Support Group. Retrieved February 26, 2003, from the World Wide Web: http://www.isogroup.iserv.net/14001.html

United States Environmental Protection Agency. Retrieved February 26, 2003, from the World Wide Web: http://www.epa.gov/owm/iso14001/isofaq.htm

APPLYING ETOPS FAIL-SAFE DESIGN CONCEPTS IN A LONG RANGE STRIKE AIRCRAFT DESIGN

by

John W. McDaniel Jr.

A Research Paper
Submitted to the Extended Campus in Partial
Fulfillment of the Requirements of the Completing
ASCI 611

Embry-Riddle Aeronautical University
Extended Campus
Fort Worth Resident Center
February 2003

ABSTRACT

Aircraft designed to perform Extended-Range Operations with Two-Engine Airplanes (ETOPS) flight operations use mature technology applied using the FAA's Fail-Safe Design Concept to safely and reliably transit long distances away from useable airfields. The ETOPS design approach holds potential for future Long Range Strike (LRS) aircraft that are also tasked to fly long distances from safe havens. This paper is a report on a case study that examines the application of ETOPS design on LRS aircraft and any potential improvement in reliability that can be achieved in the process.

CHAPTER I

INTRODUCTION

Overview

The paper begins with background on ETOPS and ETOPS Fail-Safe design reliability. The paper then identifies areas where the application of ETOPS design principles (FAA, 1988) could be used in design of a hypothetical, high subsonic, Long Range Strike (LRS) aircraft. The hypothetical LRS aircraft is referred to as the LRS-X within this paper, and is a hypothetical variant of the world's most advanced LRS aircraft, the Northrop Grumman B-2A.

Important system and subsystems design features of the most successful ETOPS aircraft, such as the Boeing 777 (B777) will be considered for application within the hypothetical construct. For the purposes of this study it is assumed that the well-documented human factors aspects of ETOPS maintenance and management programs (FAA, 1999) that support ETOPS inherent (i.e. design) reliability, will be managed to yield comparable operational reliability.

The paper briefly describes the use of an established process by which aircraft reliability is modeled and correlated to an average (arithmetic mean) aircraft Unscheduled Maintenance Time (UMT) and corresponding distribution around the mean. UMT is the average time it takes to perform unscheduled maintenance between sorties. A system-level UMT model of an LRS-X will be constructed by adapting ETOPS system design concepts to the B-2A's design. A UMT model will be used to generate LRS-X

UMTs for comparison with B-2 UMTs to determine if ETOPS design principles hold potential benefit for the next-generation LRS aircraft design.

Background

The Origins of ETOPS

Historically, all twin-engine commercial aircraft were required to plan flight routes to ensure that at no time, the aircraft was too far away from a suitable alternate landing field. In 1936, this standard was set at 100 miles. From 1953 to 1985, the regulations required commercial aircraft to fly routes that would take them no more than 60 minutes from the nearest alternate landing field in case of emergency (Kinnison, 2002). The limitation was a legacy from the reliability of twin piston-engine powered airplanes, but had been kept in place through the years for jet-engine powered commercial aircraft (FAA, 1988). FAA Circular AC 120-42 extended the 60-minute limit up to 180 minutes, and for some special cases 207 minutes in recognition of the increased reliability of twin-engine aircraft. In 1953, the United States had codified regulations prohibiting twin-engine aircraft from flying more than one hour's single-engine flight time from a suitable airport, in Federal Aviation Administration Federal Aviation Regulation (FAR) 121.161 (Kinnison). Until the latest generation of commercial aircraft, it was judged that reliability of aircraft systems, especially their jet engines, was not sufficient to regularly transit oceans or uninhabited frontiers with a required margin of safety. Newer model aircraft introduced since the 1980s were designed with far more inherent system reliability than earlier aircraft. Using this improved reliability as a rationale, manufacturers and operators persuaded domestic and international regulatory agencies to allow twin-engine commercial aircraft to be used on ETOPS operations.

ETOPS Fail Safe Design Concept

The ETOPS Fail-Safe Design Concept is delineated in Appendix 2 of AC-120-42A (FAA, 1988). Within Appendix 2, The concept is summed-up neatly in two paragraphs, which read as follows:

> In any system of subsystem, the failure of any single element, component, or connection during any one flight (brake release through ground deceleration to stop) should be assumed, regardless of its probability. Such single failures should not prevent continued safe flight and landing, or significantly reduce the capability of the airplane or the ability of the crew to cope with the resulting failure conditions.
>
> Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, unless their joint probability with the first failure is shown to be extremely improbable.

These two paragraphs, though simple, encapsulate what makes an ETOPS Aircraft design different from its predecessors. Traditional reliability design would assume no failures would present themselves in the successful completion of a flight, and would also allow or assume a significant reduction in capability when a failures do occur. Traditional reliability design would also not involve a requirement limiting crew workloads within a range of effort that would not tax the "ability of the crew to cope with the resulting failure conditions".

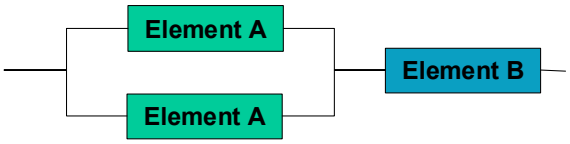
The contrasts in traditional versus fail-safe design concepts are easily illustrated. The traditional design philosophy could be viewed as closely aligned with the Series

Reliability (Figure 1.) approach to reliability design. Using the Series Reliability approach, a system is designed so that the system capability is optimized to perform best when all elements are functioning, but rapidly degrades as elements fail. Within the series reliability model (Reliability Analysis Center, 1995), increased redundancy actually increases probability of failures occurring.

Series Reliability in a System

Figure 1.

A Fail-Safe design philosophy on the other hand is more closely aligned with the Parallel Reliability design approach (Figure 2.), where a single failure does not critically degrade a system's performance.



Parallel Reliability in a System

Figure 2.

A practical example that contrasts these two design philosophies can be found in the propulsion system design of modern transport aircraft. This example will be examined at length, because of the importance of the propulsion system as the aircraft's source of electrical and hydraulic power as well as propulsion.

The Boeing 747-400 and Airbus A340 are large four-engine aircraft, whose propulsion scheme was designed using the traditional series reliability approach. Thus each of these aircraft experience, as a system, degradation in performance with the progressive loss of engines, and cannot maintain level flight at any altitude on one

engine. In these aircraft, if the two engines that lose thrust of are both on the same wing, the resulting asymmetrical thrust situation also brings increased controllability challenges. The Boeing 777 however, with propulsion systems built to a parallel reliability concept, experiences a more graceful degradation with one engine operable. This enables it to fly on one engine for up to three hours, and even perform an automatic landing under normal ETOPS operating rules in an engine-out condition.

In theory, a four-engine aircraft can proceed and complete it's flight on three engines, but many times the safest option is to land at the nearest airfield (Boeing, 2002). Superficially, it appears that a four-engine aircraft would have an edge in reliability, except that by having four engines, the probability of the first engine failure for independent cause is twice as high as a two-engine aircraft. It also has three times the probability of a second, independent, engine failure, since there are three engines still running versus one engine still running on the two-engine aircraft.

The math is relatively straightforward. Total probability of engine failure (F_t) = number of engines (n) times the probability of one independent engine failure ($n*F_1$) plus the probability of a failure due to common cause of multiple engines (F_M) or more simply: $F_t = (n* F_1) + F_M$. We may hold F_M as a constant between the two concepts for two reasons. Failure of multiple engines for a common cause implies human error, which has a potential to occur equally in both twin and four-engine designs. If human error is not at the root of multiple engine failures, it has been calculated that a loss of multiple engines in ETOPS operations is extremely improbable (van Beveren, 2000), therefore F_M approaches zero. Thus, the number of engines used is the largest variable between ETOPS twin-engine and four-engine aircraft propulsion reliability.

While the consequences of losing both engines on an ETOPS aircraft can be catastrophic, the probability of losing both engines on any one flight is extremely remote. One analyst put the probability of losing both engines within 180 minutes of each other during 180 minutes of ETOPS operation at 1 in 416 million (van Beveren).

CHAPTER II

APPLYING ETOPS DESIGN CONCEPTS TO A NEW LRS AIRCRAFT

Analysis of B-2A and B777 aircraft systems subject (Northrop, 1993; Wild, 1996) indicates a high commonality between the two aircraft in subsystem hardware and software technology, with the major difference related to how some of the technology is applied. This is not surprising, given that most of the B-2A design was finalized shortly before the B777 and that Boeing was an associate contractor on the B-2A, responsible for much of the B-2A systems' design. Highly detailed data is available on B-2 reliability, and will be used as a baseline. B777 ETOPS design concepts will be applied to the Propulsion, Auxiliary Power, Electrical Power, and Hydraulics systems to test for improved design reliability. There will also be an exploration of the effects of a possible simplified aircraft structure.

B-2A Systems not evaluated for B777 ETOPS design applications are the Environmental Control System, Crew Accommodations, Landing Gear, and Radar/Navigation/Avionics. These B-2A systems are either already much simpler than a B777's, already comparable, or are so different that a comparison would be useless.

Propulsion

The B-2 is powered by four General Electric F118 engines in the 19,000-Pound Static Thrust Class. For the purposes of this LRS-X analysis, these engines are replaced by two Pratt and Whitney PW2000 derivatives with approximately 40,000 Pounds of Thrust. These engines were selected because they are already in service on the B757, and have an extensive ETOPS history (Boeing, 1999), as well as the fact they have the

potential to be installed within the existing B-2A Outer Mold Line (OML) as illustrated in Figure 3.

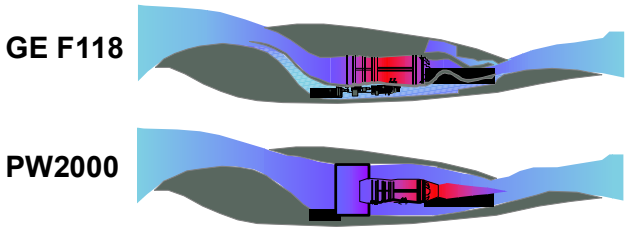


Figure 3.

Auxiliary Power

The B-2A uses two Auxiliary Power Units (APUs) to provide Direct Current (DC) power and engine start capability. This is distinctly different from the B757/67/77 series of aircraft that can also use the APU as added in-flight redundancy for AC power. For the LRS-X analysis, Each APU is assumed to have a 90 Kilovolt-Ampere (KVA) AC generator.

Electrical Power

Electrical Power Generation

The B-2A has a split-parallel electrical bus system where four generators provide power on four channels to four buses. Two 75 KVA (90 KVA surge) generators provide power to channels 1 and 2 in parallel, and the other two generators provide power to channels 3 and 4 in parallel. The two parallel systems are isolated (split) but synchronized. Any two channels have the capacity to support mission completion and any one can channel can support a return to base. Within this study, the generator and bus system will mimic the B777 arrangement, with a primary and backup generator on each engine, while using the APU generators also as backup. Since the LRS-X will have

two APU generators, the LRS-X will have the same level of redundancy as the B777 with a Ram Air Turbine (RAT), without using a RAT.

Electrical Power Distribution

The B777 uses an Electrical Load Management System that replaces a large number of complex relays and circuits used in previous designs, including the B-2A. The B777 system is assumed within the LRS-X model.

Hydraulics

The hydraulics systems of the B-2A are in many ways simpler than the B777s, because it has a less-complex landing gear and control system schematic. However, simplified hydraulics are possible if the aircraft control system is simplified as will be investigated in the simplified structure excursion of the model.

CHAPTER III

MODELING UNSCHEDULED MAINTENANCE TIMES

B-2A Sortie Regeneration Times, or SRTs, involves calculating the probable unscheduled maintenance time (UMT) and adding it to the average time to load munitions and complete the scheduled service of the aircraft. Northrop Grumman (1998) has implemented a model that uses historical Mean Time Between Failure (MTBF) data as an input, applies adjustment factors for variation in sortie times, and variations in selected maintenance techniques (not a factor in this analysis). This model is used to feed another model that predicts numbers of B-2A sorties that can be generated over time with a high degree of accuracy. UMTs are predicted by first rank-ordering the probability of failure of different aircraft elements by failure mode, and their associated mean time to repair (MTTR). Then the failure modes are rank-ordered by the probability they will be the longest repair, referred to in the model as the "long pole", that is required. The model as it is applied is inherently conservative, taking no benefit from reduced weights possible with a two-engine propulsion scheme, nor recognizing simplification of collateral systems.

CHAPTER IV

MODEL RESULTS

Using the UMT model, the analyst can derive the mean UMT and distribution of probable UMTs. The baseline distribution for the B-2A for a 30-Hour mission is seen in Figure 4.

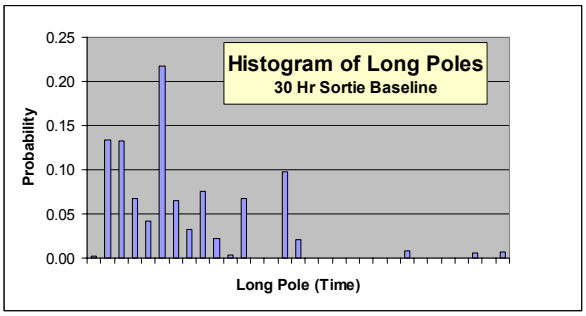


Figure 4.

Applying the ETOPS fail-safe design changes as described in the preceding section to the inputs of the UMT model results for the LRS-X in the output found in Figure 5.

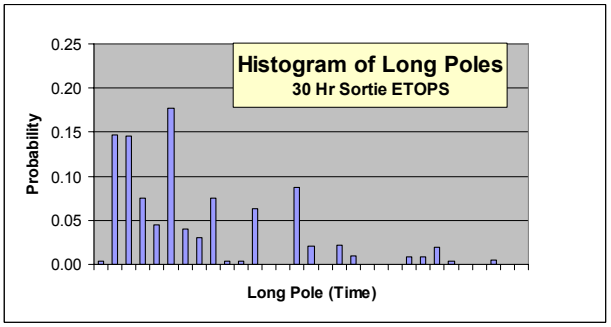


Figure 5.

The resultant average UMT for the LRS-X is approximately 1.8% lower than the baseline B-2A. There was no improvement measured within a simplified structure excursion.

CHAPTER 5

DISCUSSION

The small reduction in average UMT correlates with an earlier study (McDaniel, 2001) that identified the baseline B-2A system reliability as comparable to the Boeing 747 (B747) when flying similar mission profiles. The change also correlates to published data (Boeing, 2002) on relative dispatch reliability between the B777 and B747 (Figure 6.).

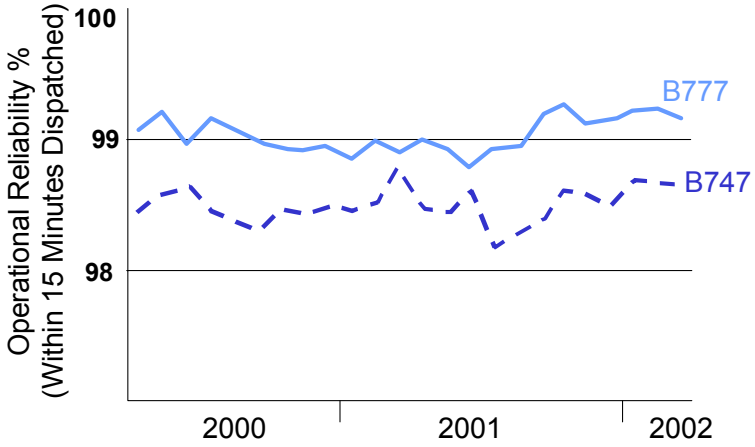


Figure 6.

The simplified structure excursion that was conducted did not yield any measurable improvement over the LRS-X ETOPS configuration. This non-impact on overall UMT is due to the fact that the only significant change in aircraft planform was an approximate 20% reduction in control surfaces, and associated systems, all of which have low failure rates and rapid repair times.

CONCLUSION

Applying the ETOPS fail-safe design principles to a high-subsonic future LRS aircraft has the potential to yield improved maintenance, and in turn sortie, performance over that which is possible with contemporary four-engine bomber design. Before ETOPS fail-safe design principles can be recommended for use in a new design the cost of implementation, along with possible advantages in operational effectiveness would have to be factored to establish a return on investment.

REFERENCES

Boeing. (January, 1999). *Multi-engine maintenance.* Retrieved February 22, 2003, from http://www.boeing.com/commercial/aeromagazine/aero_05/textonly/m02txt.html

Boeing. (September, 2002). *An Airbus advertising campaign at the Farnborough Air Show stoked the fires in the debate between ... two engines and four engines.* Retrieved February 24, 2003, from http://www.boeing.com/news/frontiers/archive/2002/september/i_ca1.html

FAA (1988, December 30). *Extended range operations with two-engine airplanes (ETOPS)*. (Advisory Circular AC 120-42A).

FAA (1999, December 14). *Airworthiness inspector's handbook: Volume 2.* (Ch 12).

Kinnison, H. (2002, January-February). Heading ETOPS. *Flight Safety Australia*, 40-43.

McDaniel, J.W. (2001). [Turn time comparison: B-2 versus 747]. Unpublished raw data.

Northrop Corporation (1993), *B-2 first look aircraft systems handbook (FLASH)*. Los Angeles, CA: Author

Reliability Analysis Center (1995). *Reliability toolkit: commercial practices edition*. Rome, NY, Rome Laboratory/ERSR.

van Beveren, T., (April 3, 2000). *Pilot group charges economics, not safety, behind twin-engine.* Retrieved March 3, 2003, from http://www.aviationsafetyonline.com/articles/articles_in_english.html#ENGLISH

Wild, T.W. (1996). *Transport category aircraft systems*. Englewood, CO: Jeppesen Sanderson.

AT ISSUE: ELECTRONIC VIDEO IMAGERY IN THE COCKPIT

By

Steven R. Mitchell

Submitted in Partial Fulfillment of the
Requirements of ASCI 611 System Safety in the
Aviation/Aerospace Industry
Spring 2003

Embry-Riddle Aeronautical University
NAS Fort Worth JRB Resident Center
March 2003

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

AT ISSUE: ELECTRONIC VIDEO IMAGERY IN THE COCKPIT

Aviation has long been a proving ground for many transportation related safety improvements including on-board recording devices. Recent advances in flight data and cockpit voice recorder technologies have made it possible to capture vast amounts of information. Not only providing important data to accident investigators, but allowing operators to monitor and modify operational procedures so that investigators can hopefully prevent more accidents and incidents.

The National Transportation Safety Board (NTSB) accident investigation experience over the years has shown that on-board recording devices can be one of the most useful tools available. Recording devices help the NTSB investigators quickly find out what happened by isolating the problem, and thus help prevent a similar accident from happening again. With the increasing number of airline passengers and subsequent accidents, there is a growing need for better accident investigation tools.

High profile accidents, which are potentially disastrous to airline operators and manufacturers, have

become commonplace with the global media. The shortcomings of current technology often leave many unanswered questions as to the particulars of an accident. Implementing cockpit image recorders aboard commercial airliners as a means of enhancing the current cockpit voice recorder as well as some functions of the flight data recorder will provide the NTSB investigators the much needed tools to solve and hopefully prevent future accidents.

CHAPTER II

ON-BOARD RECORDING DEVICES: THE IMPORTANCE

In 1994, just outside Pittsburgh, USAir flight 427, a Boeing 737, crashed, the second crash of the world's most popular aircraft in three years. The plane's flight data recorder recorded only 11 parameters. As a result, the NTSB's investigation into that extremely complex accident took more than four years to complete. Six years after the accident, the FAA finally announced a plan to redesign the 737's rudder system. Contrast that accident with the NTSB's investigation into the crash of an American Eagle ATR-72 in Roselawn, Indiana in 1994, and two 1996 accidents involving the Boeing 757. All three accidents demonstrated how the availability of adequate data immediately following accidents can allow the investigators to focus on investigative efforts, identify safety problems, and implement solutions in a relatively timely manner.

Because the ATR's flight data recorder recorded 98 parameters, the NTSB was able to quickly focus on how the aircraft operated in icing conditions, and issued urgent safety recommendations just eight days after the accident. Both of the Boeing 757 accidents required underwater recoveries under extremely difficult conditions. A Birgen Air flight crashed off the coast of the Dominican Republic

in 7,200 feet of water. Off the coast of Peru, an Aeroperu flight crashed in more than 600 feet of water. The flight data recorders on-board both planes were capable of recording 350 parameters. Once the recorders were recovered, they provided investigators with the data necessary to define the problem and to determine actions taken by the flight crews. As a result, in the Birgen Air case, NTSB investigators did not recover the remainder of the aircraft. In the Aeroperu accident, only a few additional parts had to be recovered. Because of the information provided by the recorders, the countries involved saved millions of dollars in investigative and recovery costs, and the traveling public's confidence in the aircraft was maintained. Based on the NTSB's experience during the USAir flight 427 investigation, as well as other investigations in which insufficient information was available, the NTSB issued safety recommendations to the U.S. Federal Aviation Administration (FAA) to increase the number of flight data recorder parameters.

At the end 2002, all newly manufactured aircraft were to be required to record a minimum of 88 parameters and older aircraft had to be retrofitted. Increasing the

number of parameters on flight data recorders will more than likely not solve all of the problems encountered because of gaps in recorded information. The NTSB recommended an upgrade to the cockpit voice recorder.

Following the NTSB investigations into ValuJet flight 592 in May 1996, and TWA flight 800 in July 1996, as well as foreign investigations involving SilkAir flight 185 in December 1997, and Swissair flight 111 in September 1998, the NTSB issued recommendations to the FAA to address problems created when there is an interruption in the electrical power to the cockpit voice recorder causing the NTSB to lose the last critical moments of an accident flight.

In 1999, the NTSB recommended that the FAA require a cockpit voice recorder that recorded two hours of data, rather than the current 30 minutes. The NTSB also recommended 10 minutes of backup power in case of a power loss and a redundant cockpit voice recorder near the front of the cockpit. This would significantly increase the likelihood of recovering valuable audio information. The NTSB also wanted to improve the crash survivability of all recorders. Unfortunately, the FAA has yet to take action to implement these critical requirements.

Recent innovations in recorder and power supply technologies have made it possible to provide an independent power source that would operate a solid-state flight recorder for 10 minutes. With the advent of solid-state recorders, the NTSB may soon have combination recorders available that will store audio, data, and even images.

CHAPTER III

ELECTRONIC IMAGING IN THE COCKPIT

An issue that has generated a great deal of controversy over the past few years involves electronic cockpit imagery. The NTSB believes that cockpit image recorders are the natural next step in on-board recorders and with the possibility of implementation in the near future. The NTSB believes that there should not be further delay of implementation of available technology that may help the NTSB investigators more quickly determine the probable cause of accidents and to hopefully prevent future accidents.

Recording images of the cockpit is not a new idea. It has only recently become both technically and economically feasible. Technological advances in electronics make it possible for the NTSB to capture images of what is happening inside the cockpit so that questions regarding flight crew actions can be readily resolved. With the limits of current flight recorders and the implementation of fly-by-wire controls and glass cockpits, the NTSB needs to take advantage of that technology. The idea is not to replace the cockpit voice recorder or the flight data recorder, or duplicate information already recorded, but to

capture information that is not already recorded. That would enable the NTSB to more easily determine causes of accidents and implement solutions to improve safety. Cockpit image recorders would provide key information that would allow the NTSB to determine if any human factor issues, such as non-verbal communication, information overload, distractions and procedural problems exist. A cockpit image recorder could tell the NTSB which pilot was at the controls, what controls were being manipulated, pilot inputs to or what information was on the video displays such as the display screens and weather radar. Cockpit image recorders would also provide crucial information about the circumstances and physical conditions in the cockpit that are simply not available to investigators, despite the availability of modern cockpit voice recorders and 100-parameter digital flight data recorders.

The NTSB first discussed the need for image recording the cockpit environment in a report of a September 1989 incident involving USAir flight 105, a Boeing 737, at Kansas City, Missouri. In this incident, the aircraft collided with four transmission cables during approach. The crew then executed a missed approach and landed

uneventfully in Salina, Kansas. The NTSB determined that the probable cause was the flight crew's failure to adequately prepare for and execute a non-precision approach and the subsequent premature descent below minimum descent altitude. The NTSB report pointed out the limitations of existing flight recorders to fully document the flight crew's actions and communications. An image recording of the cockpit environment would have established the availability and use of appropriate checklists and approach charts, the use of hand signals by the flight crew to communicate commands for airplane configuration changes, and what configuration changes were made. This data would have also provided investigators with insights into the nature of the crew's briefing and approach chart review as they prepared for the localizer back course approach. The NTSB findings also noted that the introduction of the aircraft with electronic "glass" cockpits and the use of data link communications would enable the flight crew to make display and data retrieval selections. These would not be detected by either the cockpit voice recorder or flight data recorder, but could be captured by image recording. Because the NTSB recognized that image-recording devices were not yet feasible, the NTSB did not

make a recommendation on the use of video recordings at that time.

In the 11 years since that incident, considerable progress has been made in both video and electronic recording storage technologies. Electronic recording of images in the cockpit is now both technologically and economically viable, and solid-state memory devices can now capture vast amounts of audio, video and other electronic data. As a result of an October 1997 accident involving a Cessna operated by the Department of Interior which was not required to have a cockpit voice recorder or flight data recorder, the NTSB recommended that the FAA require crash-protected video recording systems on all Part 135 aircraft not currently required to have a crashworthy flight recorder device.

In recent years, the NTSB investigations of other accidents involving Cessna's and similar turbine-powered aircraft had been hampered by a similar lack of flight data recorder and cockpit voice recorder information. In this case, there were no recorded communications between the accident aircraft and air traffic control and other aircraft. A cockpit image recorder may have provided crucial information about conditions in the cockpit and the

flight crew's actions. It would have also provided investigators with critical factual information such as altitude, airspeed, engine power, flight control inputs, aircraft configuration, plus human factor and atmospheric conditions.

CHAPTER IV

RECOMMENDATIONS TO THE FAA

The NTSB recommended that the FAA require Part 121, 125, or 135 aircraft currently equipped with a cockpit voice recorder and a flight data recorder to also be equipped with a crash-protected cockpit image recording system. The NTSB made this recommendation because of the inadequate information about the cockpit environment in several recent major investigations, including ValuJet flight 592 and EgyptAir flight 990 in October 1999, as well the SilkAir flight 185 and Swissair flight 111 investigations. In each of these investigations, crucial information about the circumstances and physical conditions in the cockpit was simply not available to investigators, despite the availability of good data from the flight data recorders and cockpit voice recorders.

In the case of ValuJet flight 592, a cockpit image recorder may have provided critical information about the exact smoke and fire conditions present in the cockpit during the last few minutes of the flight. A cockpit image recorder also may have shown the smoke and fire conditions and the status of the flight instrument displays in the cockpit of Swissair flight 111 that led to the flight

crew's decision to descend from cruise flight and divert to Halifax. Because there is no data on the cockpit voice recorder and flight data recorder for the final minutes before the SilkAir flight 185 crash, the Indonesian investigation was hampered by a lack of information concerning what occurred in the cockpit.

The availability of a cockpit image recording may have allowed investigators to focus their efforts more effectively. The need for an image recording of the cockpit environment was most evident in the EgyptAir investigation. The NTSB's investigators believe that electronic cockpit imagery would help resolve issues surrounding the flight crew's actions in the cockpit that resulted in the changes in the aircraft's controls, as well as the circumstances that prompted those actions.

The use of a cockpit image recording system would also permit the recording of controller-pilot data link communications. Current analog cockpit voice recorders are not able to record controller-pilot data link messages. Cockpit voice recorders will need to be replaced by other systems on all aircraft using controller-pilot data link. The communication system architecture on many aircraft will make it difficult and expensive to record controller-pilot

data link messages directly onto a flight recorder. In those instances, the image recording of the cockpit record controller-pilot data link display would be an acceptable and cost effective means of complying with regulatory requirements.

The international aviation community is also aware of the safety benefits of crash-protected video recorders. ICAO's (International Civil Aviation Organization's) Flight Recorder Panel agreed that the use of image recordings in aircraft cockpits would be very useful. The panel further noted that the European Organization for Civil Aviation Equipment (EUROCAE) was developing minimum operational performance specifications for such recorders. As a result of the Montrose, Colorado accident, the NTSB recommended to the FAA that it incorporate EUROCAE's performance standards for a crash-protected video recording system into a technical standard order. The NTSB believes the FAA should work with EUROCAE to help expedite and to incorporate the performance standards defined into an FAA technical standard order for a crash-protected cockpit image recording system as soon as practicable.

CHAPTER V

THE ISSUE OF PRIVACY

Pilots oppose the use of the video cameras in the cockpit stating that it is a breach of privacy into flight crew's workspace. Unions such as the Air Line Pilots Association think very much the same as the pilots do. The unions believe that today's technology is sufficient enough so that cockpit image recorder is not necessary. The victims and the lawyers representing the victims disagree and want to be active participants in the NTSB investigations. The new upgrades and the cockpit video recorders will be very beneficial to the airlines themselves.

The cockpit image recorders may determine if there were flaws in the manufacturing of the aircraft or pilot error. The passengers who board the aircraft everyday will stand to benefit from the information emotionally and economically; confidence in the government to solve these issues is paramount. The NTSB wants the image recorders to show the whole cockpit to include all flight crewmembers. The NTSB has stated that the faces of the pilots will not be necessary in the implementation of the image recorders. Two hours of color video will be in constant use in the

cockpits. The image recorders need to be color due to the color coordination of some of the flight screens in the cockpit. The use of the image recorder can show the actual settings of the instruments. The image can be compared to what the flight data recorder indicates and be beneficial in aircraft crashes. This kind of information can be critical if both recordings show different readings. The NTSB has indicated that the circuit breaker to the image recorder will be inaccessible to any of the crew during flight. This decision arises from the idea that the pilot from a SilkAir 737 pulled the circuit breaker to the flight data recorder before allegedly crashing the aircraft. The NTSB, along with taxpayers, will also be affected economically with the implementation of the recorders. Currently, the NTSB has spent more than 13 million dollars and 2,400 workdays trying to solve the crash of EgyptAir 990. Economic projections for this crash may run as high as 17 million dollars before the investigation is either solved or unsolved. The pilots of the airlines are concerned that the actual cockpit image recordings might be leaked to the public. Images such as these would then be put on tabloid television for the world to see. Pilots are also concerned that the flight data may or will be used

against them in court, but then again the image recording can also clear them as well. Pilots believe that the information may also be used against them by the airlines to impose disciplinary actions.

Pilots view the video recorders as an infringement on privacy in the workplace. A United DC-9 pilot was quoted as saying, "It'll be just like the old Soviet Union, with Big Brother watching you," (Carley, 2000). Pilots believe that the cockpit is their office and that the image recorder is being unjustly used to monitor flight crew actions. Pilot unions such as the Air Line Pilots Association believe the usefulness of the image recorder is over-rated. With today's modern technology, the upgrades to existing recorders and the implementation of Flight Operations Quality Assurance program should provide enough information for safety purposes. The NTSB is sensitive to the privacy concerns that have been expressed by the pilot associations and others with respect to recording images of flight crews. In order to protect crew members' privacy, the NTSB, in its request for reauthorization, urged Congress to apply the same protections that exist for cockpit voice recorders to the use of image recorders in all modes of transportation. Under these provisions, a

cockpit image recording would not be publicly released. The NTSB also is aware of concerns regarding the treatment of video as well as other types of recordings in foreign accidents, and is working with ICAO to improve protections afforded to record information on an international level. However, given the history of complex accident investigations and the lack of crucial information regarding the cockpit environment, the safety of the flying public must take precedence over all other concerns.

CHAPTER VI

CONCLUSION

Data recorders play an incredible integral role in the safety of commercial airlines. Since the NTSB is the watchdog for all airline industries, the NTSB increasingly want to upgrade and implement new recorders in the name of safety. Many people and organizations are still at odds whether the image recorders will be beneficial to help with safety and solve airline crashes. With more aircraft in the skies, the FAA and the NTSB will continue to make advances in data collection for many years to come. In recent years, the air transportation industry and the federal government have spent a significant amount of effort and money on different programs to make the skies safer. Some examples of these efforts include the Department of Transportation Aviation Safety Action Plan, the White House Commission on Aviation Safety and Security, the National Civil Aviation Review Commission, and the FAA Safer Skies Initiative. These efforts have identified the most important issues affecting air safety. These programs advocate a strong industry focus on risk management and an aggressive, proactive safety program. The current aviation industry thrust is to provide the air transportation

industry with the tools to detect and remedy the unsafe and undesirable trends that will eventually result in accidents, and thereby prevent the next accident without having to wait for an aircraft to fall out of the sky. When it comes to improving air safety, cockpit image recorders may not be the only answer. The cockpit video cameras continue to be used in a training capacity. Airline companies use the cameras to assess students, which provide the student and instructor with instant feedback on positive and negative aspects of their training. Much can be learned by using the video camera in this function to ensure training is efficient and effective.

REFERENCES

Carley, W. M. (2000, April 7). Talk of Cameras in Cockpits Faces Opposition from Pilots. The Wall Street Journal. Retrieved February 12, 2003, from http://home.pacific,net.sg/~aries8/ws07042000.htm

Frenzel, R.H. (2000, April 11). Statement of Robert H. Frenzel, Senior Vice President for Aviation Safety and Operations Air Transport Association of America before the Aviation Subcommittee, Committee of Transportation and Infrastructure. Retrieved 24 January 2003, from http://www.ntsb.gov/speeches/jhc990503.htm

Hall, J. (1999, May 3). Remarks by Jim Hall, Chairman of the National Transportation Safety Board at the International Recorder Symposium. Retrieved 24 January 2003, from http://www.ntsb.gov/speeches/jhc990503.htm

Lieb, David A. (2000). Photo Shoot for Safety. ABC News.com. Retrieved January 16, 2003 from, http://abcnews.go.com/travel/DailyNews/Minicamera_00403.html

National Transportation Safety Board (2000, April 13). Safety Board Proposed Cockpit Video Cameras in Planes by 2003. Retrieved February 14, 2003, from

http://neodysseytravel.com/vnews/display.v/ART/2000/04\13\38F48A3E2

Stark, Lisa (2000). Cockpit Cameras Could Help Solve Mysteries of Air Crashes. ABC News.com. Retrieved February 14, 2003, from http://abcnew.go.com/sections/us/DailyNews/cockpitcamera00411.html

Steenblik, Jan W. (2000, June/July). Cockpit Video Recorders: Lawyers, Cameras, and Money. Retrieved January 16, 2003 from http://cf.alpha.org/internet/alp/2000/Jun00p24.htm

APOLLO 1
FAILURE OF SYSTEM SAFETY

By

Roy L. Carman

Submitted in Partial Fulfillment of the Requirements
ASCI 611 Aviation/Aerospace System Safety
Spring 2003

Embry-Riddle Aeronautical University
Fort Worth Resident Center
March 2003

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

On January 27, 1967, the beginning of the day saw the Apollo 1 spacecraft being put to the test as astronauts Gus Grissom, Ed White and Roger Chafee were rehearsing a simulated countdown in preparation for a February launch. It wasn't going well. The test was delayed for an hour when Grissom smelled something in the oxygen system that reminded him of sour milk. It took an hour to track that down and correct. Then the astronauts were placed in the command module for the countdown.

The Apollo command module had been built by North American Aviation in Downey, California. It was a Block 1 spacecraft, designed strictly for Earth orbit. It did not have the docking probe or hatch for docking and did not the have the navigation computers needed for the long voyage to the moon. A new, improved Block 2 spacecraft would be built for the lunar landings. North American Aviation engineers were some of the best in the business but they had never built a moonship before. Changes were the only constant; sometimes the engineers couldn't keep track of all of them. When the Apollo 1 spacecraft was shipped out to the Cape, it wasn't finished. They would do the job on site at Kennedy Space Center. They never got the chance. At the hold at T minus ten minutes, the Apollo 1 spacecraft had caught on fire inside the capsule and all three crewmembers were killed.

CHAPTER II

THE INVESTIGATION

While the shock of the loss of Apollo 1 and her astronauts traveled around the nation and the world, NASA Administrator James E. Webb, had already called for an independent Review Board that would investigate the accident and determine its cause. The Apollo 204 Review Board's composition was made up of eight members with the Chairman being Dr. Floyd L. Thompson, Director of the Langley Research Center. The Review Board was charged with:

1. Review the circumstances surrounding the accident to establish the probable cause or causes of the accident including review of the findings, corrective action and recommendations being developed by the Program Office, Field Centers and contractors involved.

2. Direct such further specific investigation as may be necessary.

3. Report its findings relating to the cause of the accident to the Administrator as expeditiously as possible and release such information through the Office of Public Affairs.

4. Consider the impact of the accident on all Apollo activities involving equipment preparation, testing and flight operation.

5. Consider all other factors relating to the accident including design, procedures, organizations and management.

6. Develop recommendations for corrective or other action based upon its findings and determinations.

7. Document its findings, determinations and recommendations and submit a final report to the Administrator which will not be released without his final approval.

The makeup of the Apollo 204 Review Board were Dr. Thompson as Chairman,

- Dr. Maxime Faget, Director, Engineering and Development, Manned Spacecraft Center, NASA
- Lt. Colonel Frank Borman, Astronaut, Manned Spacecraft Center, NASA
- E. Barton Geer, Associate Chief, Flight Vehicles and Systems Division, Langley Research Center, NASA
- George Jeffs, Chief Engineer, Apollo, North American Aviation
- Dr. Frank A. Long, PSAC Member, Vice President for Research and Advanced Studies, Cornell University
- Colonel Charles R. Strang, Chief of Missiles and Space Safety Division, Air Force
  Inspector General, Norton AFB, California
- George C. White, Jr. Director, Reliability and Quality, Apollo Program Office, Headquarters, NASA
- John Williams, Director, Spacecraft Operations, Kennedy Space Center, NASA

George T. Malley, Chief Counsel, Langley Research Center, served as counsel to the Board.

The Apollo 204 Review Board met, for the first time, at Kennedy Space Center on January 28, 1967. An intense review was held of the accident followed by a very detailed evaluation of the management both at North American Aviation and NASA. During this time, the creation of 21 Task Panels, manned by experts in their fields, assisted the Review Board in a systematic manner.

One of the first things that the Review Board ordered was a series of fire tests to determine what would happen under a pure oxygen environment. They simulated the conditions that existed at the time of the fire and the materials present. The results were astounding. Materials that were used in the command module had undergone a fire test at 6psi of pure oxygen as part of the test for qualification. At 6psi, the materials had burned but were containable. The tests were then conducted at 16psi of pure oxygen and the previous tested materials exploded and gave off a poisonous gas. The cooling system burned too at 16psi as well as the Velcro that was placed everywhere inside the spacecraft. Even a bar of aluminum burst into flame when ignited in a 16psi oxygen atmosphere.

The purpose of the 16psi pure oxygen atmosphere was due to the structure of the spacecraft and the attempt to be as realistic as possible. The spacecraft was designed to handle a positive pressure differential of 8psi from inside to outside but only 1 to 2psi negative differential pressure from outside to inside. If the outside pressure was greater than 2psi, the pressure vessel could implode. This was the situation at the Cape on Launch Complex 34. At sea level pressure of 14.7psi, the Command Module had to be at 16psi to keep from imploding.

To everyone's horror, that high-pressure pad test was a fire waiting to happen. All it needed was an ignition source. There were plenty of candidates. There were frayed and even bare wires after the Command Module reached the Cape, all the result of shoddy workmanship at North American. Wire bundles on the floor were often stepped on by technicians or the astronauts. Wires in open trays were jostled and bumped during training sessions, potentially leading to frays in insulation. The exact ignition source was never identified. The fire almost certainly started below and to the left of Gus Grissom's couch. (Kraft, 2001, p. 274)

Another concern was the egress from the Command Module. If they could get the hatch open, could the astronauts have survived? This was a task that the Review Board had for the Task Panels. A demonstration was set up by the other astronauts in spacecraft 014 for the Review Board. It took 5 minutes to remove the inner and outer hatches. According to the preliminary analysis, the doomed astronauts didn't have that much time.

The command module hatch came in for sharp criticism. Ironically, it was a design that flowed from the old explosive Mercury hatch that sank *Freedom 7*(sic) (It should have read *Liberty Bell 7*. *Freedom 7* was Alan Shepard's ship) and nearly drowned Gus Grissom. The hatch was designed to never, never come off accidently (sic). Once it was locked in place, an astronaut had to grab a latch handle, insert it into an inside slot and turn the handle repeatedly to unlock it. It was tough work, requiring a lot of strength, and it was Ed White's job to do this. Once the hatch was free, White would have to pull it inward and drop it to the floor. He was desperately trying to do all that when he died. (Kraft, 2001, p. 274)

The Apollo 204 Review Board had the accident spacecraft moved to the Pyrotechnic Installation Building after the Launch Escape System and other hazardous items were removed from the spacecraft. With sistership 014 there as a guide to help in the removal and identification of items, ship 012 was disassembled. Each component was identified, tagged and photographed and laid aside.

After disassembly, the various Task Panels went to work looking at the interior of the spacecraft, the various systems and components and, in effect, ruling out what would not have caused the fire and what could. This was narrowed to a few items specially the Lower Equipment Bay Junction Box Cover Plate, Velcro and Raschel Netting, Static Inverter #2, Main Display Control Panel #8, Instrument Data Distribution Panel J800/J850 and the Octopus Cable. From this and other items, the Task Panels wrote their reports and submitted them to the Board for review. A final report was delivered to NASA Administrator James E. Webb on April 5, 1967. In it the Apollo 204 Review Board transmitted its findings, determinations and recommendations regarding the accident, how it occurred and how to fix it.

Description of Test Sequence and Objectives

The purpose of the Space Vehicle Plugs-Out Integrated Test, Operational Checkout (OCP) FO-K-0021-1, Spacecraft 012 is to demonstrate all space vehicle systems and operational procedures in as near a flight configuration as is practical and to verify their capability in a simulated launch. System verification is performed, an abbreviated final countdown conducted and a flight simulation made. All communications and instrumentation systems are activated and proper measurements are monitored at

appropriate ground stations. At the start of the simulated flight, umbilicals are disconnected and the spacecraft is on simulated fuel-cell power.

Specific objectives of this test for Spacecraft 012 as stated in the Final Procedure Document were:

a) To verify overall spacecraft/launch vehicle compatibility and demonstrate proper function of spacecraft systems with all umbilicals and Ground Support Equipment disconnected.

b) To verify no electrical interference at the time of umbilical disconnect.

c) To verify astronaut emergency egress procedures (unaided egress) at the conclusion of the test.

The preliminary outline for this test procedure was written by North American Aviation, Inc. (NAA) in July 1966. The test procedure was reviewed and revised periodically over the next few months. In September, the flight crew requested that emergency egress practice, which was not in the original test outline, be added. This addition was requested because a subsequent test, Countdown Demonstration, would involve a fully fueled Launch Vehicle and this latter test was identified as hazardous. This egress test was then added to the Space Vehicle Plugs-Out Integrated Test.

The Plugs-Out Test was initiated on January 27, 1967 at 1255 GMT (7:55 am EST) when power was applied to the spacecraft for this test. After completion of initial verification tests of system operation, the flight crew entered the Command Module. The Command Pilot entered at 1800 GMT (1:00 pm EST) followed by the Pilot and Senior Pilot. The Command Pilot noticed an odor in the Spacecraft Environmental Control

System suit oxygen loop and the count was held at 1820 GMT while a sample of the oxygen in this system was taken. This odor has been determined from subsequent analysis not to be related to the fire. The count was resumed at 1942 GMT with hatch installation and subsequent cabin purge with oxygen beginning at 1945 GMT. Communication difficulties were encountered and the count was held at approximately 2240 GMT to troubleshoot the problem. Various final countdown functions were still performed during the hold as communications permitted. From 2245 GMT until about 2253 GMT, the flight crew interchanged equipment related to the communications systems in an effort to isolate the communications system problem. This problem consisted of a continuously live microphone that could not be turned off by the crew. The live microphone condition was first noted by the test crew about 2225 GMT and records indicate that the condition first occurred between about 2057 GMT and 2218 GMT. During the troubleshooting period, problems developed in the ability of various ground stations to communicate with one another and with the crew. None of the communications problems appear to have had a direct bearing on the fire.

By 2220 GMT (6:20 pm EST), all final countdown functions up to the transfer to simulated fuel cell power were completed and the count was held at T-10 minutes pending resolution of the communications problems.

Chronology of the Fire

It is most likely that the fire began in the lower forward portion of the left-hand equipment bay. This place the origin to the left of the Command Pilot and considerably below the level of his couch.

Once initiated, the fire burned in three stages. The first stage, with its associated rapid temperature rise and increase in the cabin pressure, terminates approximately 15 seconds after the verbal report of fire. At this time (about 2331:19 GMT) the pressure vessel, which was the Command Module cabin, ruptured. During this first stage of the fire, flames moved rapidly from the point of ignition, traveling along the Raschel net debris traps which were installed in the Command Module to prevent items from dropping into equipment areas during tests or flight. At the same time, Velcro strips, positioned near the ignition point, also burned.

Based upon pressure and temperature measurements taken during the fire, the fire was not intense until about 2331:12 GMT. The slow rate of build-up of the fire during the early portion of the first stage is consistent with the view that ignition occurred in a zone containing little combustible material. The slow rise of pressure could also result from the absorption of most of the heat by the aluminum structure of the Command Module. The original flames rose vertically and then spread out across the cabin ceiling. The debris traps provided not only combustible material and a path for the spread of flames but also fire-brands of burning molten nylon. The scattering of these firebrands contributed to the spread of the flames.

By 2331:12 GMT, the fire had broken from its point of origin. Evidence is strong that a wall of flame extended along the left wall of the module, preventing the Command Pilot, occupying the left hand couch, from reaching the valve which would vent the Command Module to the outside atmosphere. Although operation of this valve, located on a shelf above the left hand equipment bay, is the first step in established emergency egress

procedures, such action would have been to no avail because the venting capacity was insufficient to prevent the rapid build-up of pressure due to the fire. It is estimated that opening the valve would have delayed the Command Module rupture by less than one second.

Emergency procedures called for the Senior Pilot, occupying the center couch, to unlatch and remove the hatch while retaining his harness. A number of witnesses, who observed the television picture of the Command Module, discerned motion that suggests that the Senior Pilot was reaching for the inner hatch handle. The Senior Pilot's harness buckle was found unopened after the fire indicating that he initiated the standard hatch opening procedures. Data from the Guidance and Navigation System indicate considerable activity within the Command Module after the fire was discovered. This activity is consistent with movement of the crew prompted by proximity of the fire or with the undertaking of standard emergency egress procedures.

The Command Module is designed to withstand an internal pressure of approximately 13 pounds per square inch above external pressure without rupturing. Data recorded during the fire show that this design criteria was exceeded late in the first stage of the fire and that the rupture occurred at about 2331:19 GMT. The point of rupture was where the floor or aft bulkhead of the Command Module joins the wall essentially opposite the point of origin of the fire. About three seconds before rupture, the final crew communication began at 2331:16.8 GMT.

Rupture of the Command Module marked the beginning of the brief second stage of the

fire. This stage is characterized by the period of greatest conflagration due to the forced convection that resulted from the outrush of gases through the rupture in the pressure vessel. The swirling flow scattered firebrands throughout the crew compartment spreading the fire. This stage of the fire ended at approximately 2331:25 GMT. Evidence that the fire spread from the left hand side of the spacecraft to the rupture area was found on further examination of the module. Damage to the crew suits is also indicative of the spread of the fire from left to right. The Command Pilot's suit was damaged the worst while the Senior Pilot's and Pilot's suits sustained progressively less damage. Further evidence of the intensity of the fire includes burst and burned aluminum tubes in the oxygen and coolant systems at floor level. The pressure in the Command Module is estimated to have dropped to atmospheric pressure five or six seconds after the rupture. The third and final stage of the fire began at about 2331:25 GMT.

The third stage was characterized by rapid production of high concentration of carbon monoxide. Following the loss of pressure in the Command Module and with the fire now throughout the entire cabin, the remaining atmosphere in the crew compartment became unable to support continued combustion. Heavy smoke now formed and large amounts of soot were deposited on most spacecraft interior surfaces as they cooled. The third stage of the fire could not have lasted more than a few seconds because of the rapid depletion of oxygen. It is estimated that the Command Module atmosphere was lethal by 2331:30 GMT, about five seconds after the start of the third stage.

The Findings

1. There was a momentary power failure at 23:30:55 GMT.
2. Evidence of several arcs was found in the post-fire investigation.
3. No single ignition source of the fire was conclusively identified.
4. The Command Module contained many types and classes of combustible material in areas contiguous to possible ignition sources.
5. The test was conducted with a 16.7 pounds psi absolute, 100 % oxygen atmosphere.
6. The rapid spread of fire caused an increase in pressure and temperature which resulted in rupture of the Command Module and creation of a toxic atmosphere. Death of the crew was from asphyxia due to inhalation of toxic gases due to fire. A contributory cause of death was thermal burns.
7. Non-uniform distribution of carboxyhemoglobin was found by autopsy.
8. Due to internal pressure, the Command Module inner hatch could not be opened prior to rupture of the Command Module.
9. Those organizations responsible for the planning, conduct and safety of this test failed to identify it as being hazardous. Contingency preparations to permit escape or rescue of the crew from an internal Command Module fire were not made.
    a. No procedures for this type of emergency had been established either for the crew or for the spacecraft pad work team.
    b. The emergency equipment located in the White Room and on the spacecraft work levels was not designed for the smoke condition resulting from a fire of this nature.
    c. Emergency fire, rescue and medical teams were not in attendance.

d. Both the spacecraft work levels and the umbilical tower access arm contain features such as steps, sliding doors and sharp turns in the egress paths which hinder emergency operations.

10. Frequent interruptions and failures had been experienced in the overall communication system during the operation preceding the accident.

11. Revisions to the Operational Checkout Procedure for the test were issued at 5:30pm EST, January 26, 1967 (209 pages) and 10:00am EST January 27, 1967 (4pages)

12. Differences existed between the Ground Test Procedures and the In-flight Check Lists.

13. The fire in Command Module 012 was subsequently simulated closely by a test fire in a full scale mock-up.

14. The Command Module Environmental Control System design provides a pure oxygen atmosphere.

15. Deficiencies existed in Command Module design, workmanship and quality control such as:

    a. Components of the Environmental Control System installed in Command Module 012 had a history of many removals and of technical difficulties including regulator failures, line failures and Environmental Control Unit failures. The design and installation features of the Environmental Control Unit makes removal or repair difficult.
    b. Coolant leakage at solder joints has been a chronic problem.
    c. The coolant is both corrosive and combustible.
    d. Deficiencies in design, manufacture, installation, rework and quality control existed in the electrical wiring.
    e. No vibration test was made of a complete flight-configured spacecraft.
    f. Spacecraft design and operating procedures currently require the disconnecting of electrical connections while powered.

g. No design features for fire protection were incorporated.

16. An examination of operating practices showed the following examples of problem areas:

    a. The number of open items at the time of shipment of the Command Module 012 was not known. There were 113 significant Engineering Orders not accomplished at the time Command Module 012 was delivered to NASA; 623 Engineering Orders were released subsequent to delivery. Of these, 22 were recent releases which were not recorded in configuration records at the time of the accident.

    b. Established requirements were not followed with regard to the pre-test constraint list. The list was not completed and signed by designated contractor and NASA personnel prior to the test even though oral agreement to proceed was reached.

    c. Formulation of and changes to pre-launch test requirements for the Apollo Spacecraft Program were unresponsive to changing conditions.

    d. Non-certified equipment items were installed in the Command Module at time of test.

    e. Discrepancies existed between NAA and NASA MSC specifications regarding inclusion and positioning of flammable materials.

    f. The test specifications were released in August 1966 and were not updated to include accumulated changes from release date to date of the test.

The Determinations

1. The most probable initiator was an electrical arc in the sector between -Y and + Z spacecraft axes. The exact location best fitting the total available information is near the floor in the lower forward section of the left-hand equipment bay where Environmental Control Unit (ECU) and the oxygen panel. No evidence was discovered that suggested sabotage.
2. The test conditions were extremely hazardous.
3. Autopsy data leads to the medical opinion that unconsciousness occurred rapidly and that death followed soon thereafter.
4. The crew was never capable of effecting emergency egress because of the pressurization before rupture and their loss of consciousness soon after the rupture.
5. Adequate safety precautions were neither established nor observed for this test.
6. The overall communication system was unsatisfactory.
7. Neither the revision nor the differences contributed to the accident. The late issuance of the revision, however, prevented test personnel from becoming adequately familiar with the test procedure prior to its use.
8. Full-scale mock-up fire tests can be used to give a realistic appraisal of fire risks in flight-configured spacecraft.
9. This atmosphere presents severe fire hazards if the amount and location of combustibles in the Command Module are not restricted and controlled.
10. These deficiencies created an unnecessarily hazardous condition and their continuation would imperil any future Apollo operation.
11. Problems of program management and relationships between Centers and with the contractor have led in some cases to insufficient response to changing program requirements.

Recommendations

1. The amount and location of combustible materials in the Command Module must be severely restricted and controlled.
2. That the time required for egress of the crew be reduced and the operations necessary for egress be simplified.
3. Management continually monitor the safety of all test operations and assure the adequacy of emergency procedures.
4. All emergency equipment (breathing apparatus, protective clothing, deluge systems, access arm, etc.) be reviewed for adequacy.
5. Personnel training and practice for emergency procedures be given on a regular basis and reviewed prior to the conduct of a hazardous operation.
6. Service structures and umbilical towers be modified to facilitate emergency operations.
7. The Ground Communications System be improved to assure reliable communications between all test elements as soon as possible and before the next manned flight.
8. A detailed design review be conducted on the entire spacecraft communication system.
9. Test Procedures and Pilot's Checklists that represent the actual Command Module configuration be published in final form and reviewed early enough to permit adequate preparation and participation of all test organizations.
10. Timely distribution of test procedures and major changes be made a constraint to the beginning of any test.
11. Full-scale mock-ups in flight configuration be tested to determine the risk of fire.
12. The fire safety of the reconfigured Command Module be established by full-scale mock-up test.

13. Studies of the use of a diluent gas be continued with particular reference to assessing the problems of gas detection, control and the risk of additional operations that would be required in the use of a two-gas atmosphere.
14. An in-depth review of all elements, components and assemblies of the Environmental Control System be conducted to assure its functional and structural integrity and to minimize its contribution to fire risk.
15. Present design of soldered joints in plumbing be modified to increase integrity or the joints be replaced with a more structurally reliable configuration.
16. Deleterious effects of coolant leakage and spillage be eliminated.
17. Review of specifications be conducted, 3-dimensional jigs be used in manufacture of wire bundles and rigid inspection at all stages of wiring design, manufacture and installation be enforced.
18. Vibration tests be conducted of a flight-configured spacecraft.
19. The necessity for electrical connections or disconnection with power on within the crew compartment be eliminated.
20. Investigation be made of the most effective means of controlling and extinguishing a spacecraft fire. Auxiliary breathing oxygen and crew protection from smoke and toxic fumes be provided.
21. Every effort must be made to insure the maximum clarification and understanding of the responsibilities of all the organizations involved with the objective being a fully coordinated and efficient program.

Summary of Apollo 204 Board Review

The investigation of the Apollo 204 Review Board of the Apollo accident determined that the test conditions at the time of the accident were “extremely hazardous.” However, the test was not recognized as being hazardous by either NASA or the contractor prior to the accident. Consequently, adequate safety precautions were neither established nor observed for this test. The amount and location of combustibles in the Command Module were not closely restricted and controlled and there was no way for the crew to egress rapidly from the command module during this type of emergency nor had procedures been established for ground support personnel, outside the spacecraft, to assist the crew. Proper emergency equipment was not located in the “White Room” surrounding the Apollo Command Module nor were emergency fire and medical rescue teams in attendance.

There appears to be no adequate explanation for the failure to recognize the test being conducted at the time of the accident as hazardous. The only explanation offered the Review Board is that NASA officials believed that they had eliminated all sources of ignition and since to have a fire requires an ignition source, combustible materials and oxygen, NASA believed that necessary and sufficient action had been taken to prevent a fire. Of course, not all ignition sources been eliminated.

The Apollo 204 Review Board reported that it took approximately 5 minutes to open all hatches and remove the two outer hatches after the fire was reported; that the first firemen arrived about 8 to 9 minutes after the fire was reported and that the first medical team did not arrive until about 12 minutes or more after the fire was reported. Therefore, there was not expert medical opinion available on opening the hatch to determine the

condition of the three astronauts although medical opinion based on autopsy reports concluded that the chances for resuscitation decreased rapidly once consciousness was lost and that resuscitation was impossible by the time that hatch was opened.

This type of accident was completely unexpected by both NASA and the contractor despite the amount of documentation of fire hazards in pure oxygen environments. NASA's long history of successes in testing and launching space vehicles with pure oxygen cabins at 16.7 psi and lower pressures led to overconfidence and complacency.

CHAPTER THREE

CONCLUSION

When people look back at the Apollo 1 fire and the loss of life it created, they can't help but wonder how could we have allowed this to happen. This was a totally avoidable accident if the people in charge had allowed system safety programs to work. The causes are many but one overriding point came across: the United States was in a race with the Russians to put a man on the moon. If we took a few short cuts, so much the better. Because of this attitude and the problems with the management both at NASA and North American Aviation, three men died needlessly.

One of the first steps would have been to identify the safety hazard of using a pure oxygen environment in a test. In flight, the oxygen pressure would have been only 5psi and materials had been tested for that type of atmosphere. But when the spacecraft was pumped up to 16.7 psi of pure oxygen, no one thought about the possible effects of a fire in that type of environment. On the Mercury and Gemini programs, this was done on a regular basis. However, the spacecraft were cleaner and more secure than the Apollo spacecraft. Because no problems were encountered before, why should there be any now? Another factor was the classification of the type. The plugs-out test was deemed *not hazardous* because the launch vehicle was not fueled. They never thought that a pure oxygen cabin would be a problem since all of the ignition hazards had been eliminated or so they thought.

Of course, they hadn't and the fire resulted as a consequence. There wasn't even a fire extinguisher onboard the spacecraft since the thought of fire never occurred to them.

Another problem was the hatch. It was a design compromise between the Apollo Program Manager, NASA engineers and North American Aviation. Astronauts and some NASA engineers had called for a one piece hatch that could be opened in a hurry but it was vetoed in place of a light-weight two piece hatch that could be bolted in. Weight was the big problem. The Apollo spacecraft was designed with an off-set center of gravity to take advantage of atmospheric lift forces during re-entry. The problem was that the hatch was opposite the off-set center of gravity and any changes to the hatch resulted in a change to the center of gravity. Changing the hatch meant changing the aerodynamics of re-entry. A one piece hatch would weigh more and that was a big problem since one more pound of weight equaled many more pounds of propellant to get it into space. Once in space, there was no worry about the hatch coming off since it was designed as a plug-type hatch. It was that design that killed the astronauts. During the fire, the pressure had built so rapidly that there was no one on Earth that could have opened the hatch from the inside. They didn't identify the hazards associated with a two piece hatch.

These are some of the most identifiable problems with the Apollo 1 fire and aftermath. The Apollo 204 Review Board report was very critical of the lack of cooperation between NASA and NAA. The prior spacecraft, Mercury and Gemini, had been built by McDonnell-Douglas and the cooperation shown there was outstanding. But not with NAA. It was like Mercury and Gemini never existed and so the lessons learned form those spaceflights were never used.

Astronaut Tom Stafford once said that the Apollo 1 fire was a blessing in disguise. The wreckage of Apollo1 was there for everyone to see not orbiting the Earth as a silent tomb or drifting in the translunar void. Although three men had died, three or perhaps six more lives had probably been saved.

After the congressional hearing, after the blame game and after the closest chance that the space program might be shut down, NASA and NAA built one of the safest spacecraft around. One of the changes that NASA did was to create the Office of Manned Space Flight Safety and name Jerome Lederer as Director. This gentleman had already lived an incredible life and was 65 when named. He was promoted to Director of Safety for all of NASA and retired in 1972. The Office of Manned Space Flight Safety would be responsible for the review of all aspects of design, manufacturing, test and flight from a safety standpoint.

America was caught up in the race for space and it was no holds barred to develop and get into the thick of the race. Problem was that a lot of safety items were left behind in the process and Apollo 1 was a grim reminder of what happens when you don't "what if."

REFERENCES

Brubaker, Paul (2002). Apollo 1 Tragedy: Fire in The Capsule (1st ed.) Berkeley Heights, New Jersey: Enslow Publishers Inc.

Chaikin, Andrew (1994). A Man on the Moon Volume 1: A Giant Leap (2nd ed.) Richmond, Virginia: Time-Life Publishing Co.

Cunningham, Walter (1977). All American Boys (1st ed.) New York, New York: MacMillan Publishing Co.

Kraft, Christopher C. Dr. (2001). Flight: My Life in Mission Control (1st ed.) New York, New York: Penguin Putnam Inc.

(1967) Apollo 204 Review Board - Final Report NASA History Office, NASA Headquarters, Washington, D.C.

SYSTEM SAFETY AND APOLLO 11

by

Richard Martinez

Submitted in Partial Fulfillment of the requirements of ASCI 611 Aviation/ Aerospace System Safety

Embry-Riddle Aeronautical University
Fort Worth Resident Center
March 2003

ABSTRACT

Researcher: Richard Martinez

Title: System Safety and Apollo 11

Institution: Embry-Riddle Aeronautical University

Degree: Master of Aeronautical Science

Year: 2003

This study will examine the Apollo 11 mission and the growth of the U.S. government-industry space program to make a lunar landing safely. The system safety areas of engineering, hazards, and human factors will be analyzed to determine its importance and dangers in the aerospace industry. The research will explore Apollo 11 mission training and summarize their hazards. The training importance to Apollo 11 will be discussed to compare how it provides advantage for Apollo 11 astronauts overall missions. The discussion will also include the importance of legislation passed to investigate NASA's operations.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

As the aerospace industry developed, system safety became an integral part of the industry. With more lives and expensive spacecraft at stake, system safety program provided adequate information to re-engineer designs during failures.

As the space exploration became more advanced NASA and local aerospace industry made a conjoining effort to design out every hazard in any component to increase safety.

Nevertheless, the nineteenth century proved to be enormous challenge for the Apollo program. Both the National Aeronautics and Space Administration (NASA) and the United States government industries managed the program. Their initiatives were commenced in the late 1950s to design and complete successful space program to conduct flight test into space. Nevertheless, the Apollo program would follow a series of space flights to orbit the earth and land men on the moon. The mission brought hazardous conditions to both equipment and the human crew.

Eventually, NASA constructed a training vehicle for space. The vehicle is known as the Lunar landing training vehicle (LLTV) which safeguarded the astronauts in space. It was an unusual spacecraft contraption, which helped increased human tolerances in space. Perhaps risk has always been a part of human endeavor, but astronauts still expect protection against

risk. The space era made the U.S. to also look into and mandate risk analysis in areas of the aerospace industry by introducing regulation. Thus, the risk analysis help identify possible deterioration in systems prior to placing human lives at danger. Unfortunately, failures can not be totally designed out of any program. According to Bahr (1997) "failure does not have to occur for a hazard to be present in the system" (p.145).

The failure attempts to define and improve the risk analysis of space flight in designing, building, and managing high-risk programs such as the Apollo program. It provides an efficient and effective approach to finding solutions to failures and for improving through actions or designs.

This research will examine NASA approach to system safety improved in the 1960s and it will focus on one space mission in particular to compare how they fit the profile in academia. This space mission is Apollo 11. Using the facts gathered in this study, the conclusion of this research will provide an outline and importance of safety in the aerospace industry.

CHAPTER II

REVIEW OF RELEVANT LITERATURE

First of all, "the U. S. National Aeronautics and Space Administration (NASA) sponsored government-industry conferences in the late 1960s . . . to develop ballistic missiles safe enough to carry humans into space" (Bahr, 1997, p.4).

The combine efforts of the government-industry served to design and develop a fully functional automated ballistic missile. The ballistic missile did not require manual control; however, the astronauts were able to take over manually, during a system failure, to maneuver the space vehicle to safety. (Baker, 1986, p.17).

The Apollo 11 mission had its' origin from this government-industry exploration to send men into space and back to earth safely. Despite the advent of this technological advancement, human interface with the space vehicles brought concern and complexity to NASA's technological program missions.

It has been estimated that 80%-90% of accidents are the result of human error (Hawkins, 1987 p. 32). Apollo 11 astronauts were screened for their mental and physical capacity. Many of the crews had valuable military background, and most of them were rated for their character of leadership capabilities. Despite of all the priceless qualifications, astronauts were not

immune to accidents. The space program was rather new to the U.S. government-industry in the 1960s and the interface between human-machine placed astronauts in unknown and unsafe external conditions. The "external performance-shaping factors [can be] made up of all the conditions that an individual encounters-including the entire work environment, especially the equipment design and the written procedures or oral instructions" (Bahr, 1997, p. 153). "The study of human factors human-machine interface attempts to maximize the potential for safe, efficient operation while eliminating hazardous conditions resulting from human error" (Wells, p. 168).

Nonetheless, this concern prompted NASA directors to look into a system safety approach. Thus, System Safety applies special technical and managerial skills to the a systematic, forward-looking identification and control of hazards throughout the life cycle of a project, program, or activity" (FAA, 2003, p.1)

"Operations were now geared to one-to-one interface with the astronauts. Flight control stood mission "watches." Flight directors began to develop "gouge" sheets, which established responses for given situations or conditions. Space flight involved real-time problem solving" (NASA, 2003 p.163-164).

Moreover, “the United States applied their work with . . . human information processing and control” (Nagel & Wiener, 1988). “Learning is an internal process. Training is a control of this process. The degree of success in this process control must be judged by the changes in performance or behavior resulting from the learning (Hawkins, 1987, p.194). Apollo 11 astronauts required countless training sessions to learn new equipment and function in a space environment.

Human ability to function appropriately in the natural space environment also required a defense against an airless atmosphere, extreme temperatures, and bacteria contamination. “The moon is unique solar system. It does not have an atmosphere . . . the daytime temperature at the surface rises 215 degree Fahrenheit, and at night the temperature sinks to -250 Fahrenheit” (Readers Digest, 1963, p. 17). Humans experience discomfort, irritability, and inefficiency in temperatures above 85 degrees Fahrenheit (Department of Transportation, p.24).

Fortunately on November 21, 1964 defense against the hostile environment proved suitable for space exploration. “Two spacecraft vehicles designed to measure space radiation and the air density achieved successful orbit" earlier within the decade (The Dallas Times Herald, 1964).

The Apollo 11 mission consisted of complex equipment or space vehicles such as the command module, lunar module, and service module with propulsion systems of volatile gases. The Apollo 11 space vehicle and launch vehicle were comprised of all types of dangers which contributed hazards to the equipment and humans. Failure to any of the systems, subsystems, or assembly could have been catastrophic to Apollo 11 missions.

Stephenson (2000) defines several important terms to identify the Apollo 11 space vehicle vulnerability. Component is a combination of parts, devices, and structures, usually self-contained, which performs a distinctive function in the operation of the overall equipment. For example, a "radar guidance system" is a component. Damage is the partial or total loss of hardware caused by component failure: exposure of hardware to heat, fire, or other environments: human errors; or other inadvertent events or conditions. For instance, a Lunar Module (LM) is subject to damage during an impact on the lunar moon surface. Failure is defined as the "inability of a system, subsystem, component, or part to perform its required function within specified limits, under specified conditions for a specified [time]." Again, these definitions conclude to one purpose: Systems safety.

As a result, NASA's studies also lead to system safety engineering. "System safety engineering is an engineering discipline that employs specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated mishap risk" (Department of Defense, 2000).

Developments through the early 1960s resulted in the Lunar Landing Training Vehicle, the trainer for airless space commonly known as the LLTV. The LLTV is the development of the late Aerospace Bell Company, which applied the vertical take-off and landing concept (VTOL) to simulate an airless environment. Results of the development of the LLTV created research and development programs in the U.S. to solve problems in the space vehicles. Nevertheless, the evolution of the LLTV had a major effect upon the success of the first lunar landings.

Many modifications to the LLTV were made to improve safety as accidents occurred. Several entirely new LLTV's were developed prior to being coupled with a command module. There was a great emphasis on energy-efficient propulsion to minimize fuel use. Radioactive properties, low level cooling systems, different module shapes were engineered and re-engineered to ensure the design and safety factors were made to ensure the

structural integrity of the space vehicle for reentry of the earth atmosphere (NASA, 2003).

It was an unusual way the astronauts were used to flying. The LLTV is certainly one of the unusual shaped space vehicle ever made. Its unique design features a thin robust, flat-bottomed, fuselage on very high wheel legs.

The two accidents in 1968, before the first lunar landing, did not deter Apollo program managers who enthusiastically relied on the vehicles for simulation and training (NASA, 2003). Innovative mechanisms such as the Lunar Landing Training Vehicle (LLTV) did not make training easier because the LLTV was difficult to fly. “Neil Armstrong ejected from a malfunctioning LLTV in 1968. He wasn’t hurt, but the LLTV was demolished in a fireball The LLTV control system was modified, but then the chief pilot had to eject when the new version went wrong.” (Kraft, 2001, p. 312).

In 1968 the Advisory Safety Aeronautical Panel (ASAP) was created in a legislation act to follow up on NASA operations during Apollo 1 fire and it has been a part of normal operations every year. It is a senior advisory committee that reports to the National Aeronautics and Space Administration (NASA) and Congress. “The Panel shall review safety studies and operations plans that are referred to it and shall make reports thereon,

shall advise the Administrator with respect to the hazards of proposed operations and with respect to the adequacy of proposed or existing safety standards, and shall perform such other duties as the Administrator may request"

On July 20, 1969 the United States of America successfully sent men in Apollo 11 to land on the lunar surface and returned safely (2003). Thus, the Apollo 11 mission did have marginal failures.

The advances in space vehicle systems have taken the aerospace industry to the point to not believe that there will not be failures. The prime cause of failures is the human. Robert Schulthesis and Mary Sumner (1998) describe computer systems use to create the bits that make up bytes, or characters. Analog transmission sends information using analog signals, or sin waves. The analogs were unable to process the larger amounts of incoming sensor data.

“Armstrong had averted possible disaster by taking full manual control of the vehicle on landing, selecting a safe spot for man’s first landing on the moon” (Los Angeles Times, 1969.

There were big error between the onboard guidance system and the radar’s report of how high they were. “Program alarm!” It was Armstrong’s voice. “1202! 1202!” The Eagle’s computer was having trouble completing its calculations. It was overloaded

with data and had flashed an alarm code. On Apollo 11, each time a 1201 or 1202 alarm appeared, the computer re-booted, restarted the important systems, like the steering and the descent engine kept running to let the crew know what was going on, but did not restart all the extra programs rendezvous radar jobs. It was an artifact from the Apollo 10 mission, and nobody changed the required setting. So now Eagle's computer was receiving streams of useless data and reacting with those sudden alarms. We could see on our displays that Armstrong was flying manually now and that fuel was getting low. "Neil Armstrong had to take over manual control to avoid landing into a crater on the moon" (Life magazine, 1969). Buzz Aldrin guided Neil Armstrong to a safe position on the lunar moon. The fuel tanks were now empty, they barely escaped another mishap or induced error (Kraft, 2001, p. 319-322).

Just over two-and-a-half hours later Armstrong, Aldrin, were back in the Eagle. The next day the Eagle lifted off from the Moon to rejoin the orbiting Columbia and its pilot, Michael Collins (Cassutt, 1987, p. 16).

Neil A. Armstrong . . .commander to Apollo 11 Mission stated " the next mission should do more exploration of the surface" Armstrong was satisfied with the way his pressurized suit and other equipment took care of him during his two hour

and 40 minute exposure to the airless environment of the moon (Los Angeles Times, 1969, p. 2).

"Regardless of the dangers involved, it all went like clockwork: Riding a ball of fire and preceded by a deafening sonic boom, the cosmic adventurers streaked down through a pewter-colored sky to splash down safely" (Los Angeles Times, 1969, 4 Sec. F).

CONCLUSIONS

Finally, the government-industry strived to define and improve the relationships among engineering, hazards, and human factors to enhance the application of hazard control. Nevertheless, the human factors sector will continue to identify new trends in aerospace industry order to accommodate the changes.

The exploration consisted of countless aerospace companies who contributed to this government-industry goal: System safety. Indeed, safety in the aerospace industry and space exploration became the number one concern.

Throughout the development of the Apollo spacecraft many company names appeared, several of whom made important contributions to furthering the reality of Apollo 11 lunar landing and space exploration: Bell Aerosystems developed the primary unusual framework and vertical takeoff and landing (VTOL) aircraft, General Electric developed the primary CF-700-2V turbofan vertical engines.

Throughout the 1960s, Apollo 11 missions faced dilemmas in many areas. The concept of safety itself is one of uncertainty. Absolute safety does not exist. Human activity will always and unavoidably involve risks. The concept of hazard is also uncertain. To make meaningful decisions regarding these risks, it is necessary that they be analyzed.

Systems safety allow the U.S. aerospace industry to identify the loops of our decision making process, with

engineering. Risks will always be part of the aerospace industry because of the external environment such as space and space vehicles used to perform missions.

System safety engineering is an ideal way to determine alternate solutions and changes to unique problems in space vehicles. The standards work with safety in mind. The system safety engineering enforces safety in redesign while maintaining an effective and efficient operation. The system gathers additional information during and after all operations to provide more accurate results, as well as help the aerospace industries identify trends and make necessary modifications to prevent future hazards.

REFERENCES

Alexander, K. (1989). Space vehicles. New York. Gallery books.

Armstrong's 'one giant leap'

Los Angeles Times (1969, July 27). 4 Sec. F.

Baker, W. (1986). *America in space: From America's first ventures in space exploration to futuristic space-age living.* New York: Crescent.

Cassutt, M. (1990). *Who's who in space: The first 25 years.* Massachusetts: G. K. Hall.

Hawkins, F. H. (1987). *Human factors in flight.* (2nd ed.), Brookfield: Ashgate.

Kraft, Chris, 2001, Flight: *My life in mission control. First NASA flight director.* New York: Dutton.

Life Magazines(1969, August 08). *Life On the moon footprints and photographs by Neil Armstrong and Edwin Aldrin*, (Vol. 67, No. 6) p.19

Longer moon walk feasible next time, Armstrong asserts.

Los Angeles Times (Vol. IXXXVIII), 1969 Aug. 01, p.2

Man walks on the moon 'small step for man . . .giant leap for mankind'. (1969, July 21) Los Angeles Times, Vol. I XXXVII, p.1

REFERENCES

Nagel, D. C., & Wiener, E. L. (1988). *Human factors in aviation*. San Diego: Academic Press, p.5.

NASA (2003) Retrieved February 24, 2003 (http://www.dfrc.nasa.gov/Newsroom/FactSheets/FS-026-DFRC.html)

NASA (n.d.). The Flight of Apollo. Retrieved January 29, 2003, from http://www.jsc.nasa.gov/history/suddenly_tomorrow/chapters/Chpt9.pdf#xml=http://spaceflight.herndon.wip.psiweb.com/cgi-bin/texis.cgi/webinator/search/xml.txt

Physiological Training Department of Transportation. (2003). Federal Aviation Administration Civil Aeromedical Institute Physiological Operations. Oklahoma: U.S. Government Printing Office, p. 24.

Readers Digest Great World Atlas (3rd Ed.)(1963-1968). *The moon: Earth's natural satellite:* New York: Reader's Digest Association, p. 17.

Schultheis, R., & Sumner, M. (1998). *Management information systems: The manager's view*. Boston: Irwin Mcgraw-Hill.

Section 6 of the NASA Authorization Act of 1968, Public Law 90-67, 42 U.S.C. 2477. (n.d.). Retrieved February 10, 2003, from http://www.hq.nasa.gov/office/codeq/asap/documents/publiclaw.pdf

REFERENCES

Stephenson, Joe (1991). System Safety 2000: *A practical guide for planning, managing, and conducting system safety programs*. Canada: John Wiley and Sons, pp. 292.

System safety definition retrieved February 16, 2003 (http://www.asy.faa.gov/Risk/SSProcess/SSProcess.htm.)

U.S. Department of Defense (2000). MIL-STD-882D, *Standard practice for system safety*. Washington, DC: U.S. Government Printing Office, p.3.3.14

U.S. space 'measuring devices successfully orbited from Vandenberg. (1964, November 22). The Dallas Times Herald p. A27.

Wells, A. T. (1997). "Commercial Aviation Safety" (2nd Ed.). New York: McGraw-Hill.

RELIABILITY CENTERED MAINTENANCE

By

Eva M. Donald

Term Paper

ASCI 611
Aviation/Aerospace System Safety

Embry-Riddle Aeronautical University
Extended Campus
NAS Fort Worth JRB Resident Center
February 2003

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

When aircraft were first developed they were simple machines and didn't require intense maintenance planning. By World War II aircraft and machines became much more mechanized, so much more emphasis was put on reliability and down time. These requirements led to a maintenance philosophy called "hard time maintenance". The presumption used for this philosophy was all items failed as they increased with age, so planned intervention was scheduled at increased intervals to prevent failure. (Moubray, J. 2000) Maintenance costs increased dramatically but didn't seem to increase the reliability of aircraft engines.

To cut maintenance costs and improve system/component reliability, a committee consisting of airline representatives and the Federal Aviation Administration (FAA) was formed. The committee was surprised to find that the overall reliability of an item did not decrease with age and the preventive maintenance process in use did not increase system reliability. This information led the committee to develop a maintenance program known as Maintenance Steering Group 1 or MSG 1. MSG 1 was improved upon and led to MSG 2. The Department of Defense became interested in what the airlines were doing and commissioned United Airlines to investigate how maintenance reliability and safety were interrelated. This report was called reliability-centered maintenance (RCM) and was used as the basis for MSG 3. Although it has been modified a few times it is in use today.

RCM is a maintenance philosophy built around the reliability of components in a system where each system/component is systematically analyzed. A successful RCM program relies heavily on accurate maintenance documentation. The key concepts and principles rely on determining what a failure mode is and their criticality. To develop a successful RCM program failure modes are used in a critical decision matrix. From this matrix preventive maintenance can be planned.

A key element of RCM is the Failure Mode, Effects and Criticality Analysis (FMECA). (Stark, J. 2000) When a product is new, information from a like item used in similar circumstances is used until operational data can be accumulated. The sources of data come from numerous areas such as on-wing, repair shop, or from the repair depot. Data is then analyzed and used as input to periodic maintenance decisions. Operational data is also used to understand inherent component failure.

The benefits of RCM maintenance program can be numerous such as sustaining higher levels of safety. The RCM process provides the maintenance community with tools to establish an appropriate preventive maintenance program. With a dynamic program, a maintenance person can reduce maintenance costs, unscheduled maintenance and shop visits.

CHAPTER II

PRE-RELIABILITY CENTERED MAINTENANCE (RCM) PHILOSOPHIES

Before anyone can understand what RCM means, one should have some background of past maintenance philosophies that lead up to RCM.

Until World War II, the aircraft industry was not very mechanized. Equipment was simply built, but often over designed, which meant the equipment was easily repaired. Therefore, this maintenance philosophy did not put a lot of priority on prevention of equipment failure, or as we refer to now as preventative maintenance.

During World War II, more equipment became mechanized due to increased demand of goods and lower manpower availability. Managers depended on machines much more and reliability and repair downtime was focused on more than before. At the same time the aircraft industry grew considerably with larger and more complex aircraft. The regulatory aviation body or the Federal Aviation Administration (FAA) (formally known as the Civil Aviation Board) became worried about aircraft reliability, which led to the next maintenance philosophy known as “hard time maintenance”. This philosophy was based on the likelihood that component/system failure increased with age, so if intervention was planned before the failure it should have reduce the number of failures. This wear out model was the basis of this concept of preventive maintenance. So, during the late 50’s and early 60’s maintenance consisted mostly of overhauls done at specific intervals. Unfortunately, this philosophy did not take into account the technical

characteristics of the failure and assumed that all failures were preventable. Maintenance costs increased considerably but did not seem to increase the reliability of some engines. In fact it seemed that frequency of overhauls had increased some failures.

With maintenance costs increasing and reliability either unchanged or decreasing the FAA and airlines decided to form a committee to investigate planned maintenance policies. The committee found the reliability and the overhaul frequency of equipment were not necessarily related and the belief that reliability declined with increased age was not always true. The facts were: 1) scheduled overhaul had little effect on the overall reliability of a complex item unless there was a dominate failure mode and; 2) there were other items which did not have an effective form of scheduled maintenance. This task force developed a propulsion system reliability program and each airline developed programs for their own areas of interest. This maintenance program became known as Maintenance Steering Group 1 (MSG 1) and was later improved into MSG 2. In the mid 1970's the department of defense (DOD) commissioned United Airlines to write a comprehensive manual on the relationship between maintenance reliability and safety. This report prepared by Stanley Nowlan and Howard Heap called it Reliability Centered Maintenance. (Moubray, 2000) This report was used as the basis for MSG 3, which is now in use.

CHAPTER III

DEFINITION OF RELIABILITY CENTERED MAINTENANCE

What is RCM? To put it briefly, it is a maintenance philosophy built around the reliability of various components of a system. RCM systematically analyzes aircraft components/systems to identify and implement the best preventive maintenance process. To develop a comprehensive RCM program an extensive knowledge of the system and its components is needed. An analytical process is tailored to different applications, customers, and stages of a product's useful life.

First, accurate maintenance documentation and automating maintenance records allows component/system failures to be proper analyzed. Additionally, with technology advancements, trend data can be systematically recorded from operating systems. The potential for this information is invaluable. Processes can be developed to promote safety or identify hidden failures, which can result in increased utilization and reduced costs. Additionally, improvements to components/systems can be implemented to increase reliability and overall reduce sustainment costs.

What RCM is not! It is not unscheduled maintenance, but may include opportunistic maintenance intended to achieve inherent reliability and reduce unscheduled maintenance. (Stark, 2000) It is not an infusion of new hardware, but management of both new and used assets to achieve inherent reliability. For example, during a readiness concern shop a new shop chief was appointed tot an Air Force jet engine. The shop chief encountered a shop that practiced on-condition type maintenance

(OCM). This maintenance philosophy fixes only what is unserviceable and returns the system to service. OCM cannot identify hidden or complex failure modes. So, when an engine was inducted into the shop, only the component or assembly that drove the engine in for maintenance was worked. This engine is made up of six major assemblies, the fan, core, combustor, low-pressure turbine (LPT), high-pressure turbine (HPT), and augmenter and exhaust nozzle assembly. If the engine was inducted into maintenance for a LPT change that assembly was all that was replaced. The rest of the hot section wasn't thoroughly inspected (for hidden failures) or the time remaining on the other assemblies were not considered. So an LPT with 500 hours of time remaining until time change might be installed with other assemblies that had 1000 or more hours of time remaining until time change. If the RCM maintenance philosophy was used, opportunistic maintenance could have been implemented. Not only should a LPT with about 1000 hours should have been used, but all of the assemblies should have been inspected to ensure they would remain in service until the next scheduled time change. Using an LPT with 500 hours would drive the engine back into the repair shop one extra time. Ultimately, RCM is a process used in maintenance planning to achieve affordable operational goals by reducing unscheduled maintenance, reducing costs, and improving engine builds to achieve safe operation of the engine until the next schedule inspection.

CHAPTER IV

KEY CONCEPTS AND PRINCIPLES OF RCM

The objective of maintenance is to determine the function and performance expectation of the system/component being considered. Functional failure is any deviation from the requirement or design of that item and occurs when an item is unable to fulfill an acceptable standard of performance. The severity of a functional failure determines the priority and level of maintenance required to resolve the unacceptable condition.

A failure mode is a specific physical condition that could cause a functional failure. Some components may have multiple failure modes, which all or some may result in a functional failure.

There are four functional failure categories, which are used in critical decision matrices. The first, defined as “safety evident”, could result in possible loss of aircraft or life. The second is “safety hidden” which is defined as an undetectable failure that could permit a subsequent failure that could cause loss of aircraft or life. The third, “economic/operational”, results in loss of operational use plus cost of repair. The fourth is “non-safety hidden” which involves only the cost to repair. These categories and probable occurrence are used to support the need for and criticality of corrective actions or schedule and unscheduled maintenance.

Planned maintenance is predetermined tasks performed at prescribed intervals and are identified as scheduled or preventive maintenance. A maintenance task can be a

servicing task such as replenishing consumables such as oil or fuel, or a more complex task such as replacing a turbine wheel at a specified interval. A scheduled maintenance program is dynamic and often may be changed by operational experience, on-going analysis, or incorporating improved configurations. The bottom line is RCM is focused on scheduled maintenance, although the RCM concept can be applied to unscheduled events with maintenance decisions. Reliability Centered Maintenance establishes a process, which reaches beyond scheduled maintenance to take actions to repair or replace items that are predicted to have a high probability of functional failure prior to the next scheduled maintenance interval.

CHAPTER V

KEY ELEMENTS OF RCM

RCM starts with a comprehensive, zero-based review of the maintenance requirements of each asset in its operating environment.

One of the key elements of RCM is the Failure Mode, Effects and Criticality Analysis (FMECA). (Stark, 2000) Using FMECA, one can systematically determine the functions for each component or part in a system. It can identify failure modes for each function or show how can the function fail.

The FME Criticality Analysis measures the effect of the failure mode on the basis of its impact. The worst failure mode results in a catastrophic failure or loss of aircraft or life. It is followed by critical failure mode, which results in major property damage or severe injury. Marginal failure mode results in minor property damage or minor injury. Lastly, the minor failure mode results in unscheduled maintenance or system damage, but no injury. It then measures its likelihood of occurrence during an operational interval. A 20% probability of occurrence is considered frequent, while less than 10% would be reasonably probable, occasional is less than 1%, while remote is less than .1%. To determine when a failure mode is unacceptable, undesirable, acceptable after high-level review or acceptable a criticality decision matrix is used as seen in the following table. (Stark, 2000)

	SEVERITY			
	Catastrophic	Critical	Marginal	Minor
Frequent	Unacceptable	Unacceptable	Undesirable	Acceptable after high level review
Reasonably Probable	Unacceptable	Unacceptable	Undesirable	Acceptable after high level review
Occasional	Unacceptable	Undesirable	Acceptable after high level review	Acceptable
Remote	Undesirable	Undesirable	Acceptable after high level review	Acceptable

Typical information found in FMECA is early criteria for maintenance, inspection, or logistic planning, determination of how a failure will be detected, probability of failure mode occurring to support critically analysis and actions available to the operator that reduce or eliminate a failure's impact. On a new product, since operation data is not yet available the FMECA is used as a proxy for the data. Operational data from similar items in similar applications are used to support FMECA development. But as the product is fielded and matures in an operational environment, data, which becomes available is used to support and upgrade maintenance decisions.

The sources of operational data can come from many different sources. On-wing, repair shop, or depot level inductions are sources of data. Conditional inspections are another source of data. Data analysis then considers typical input data to reach periodic maintenance decisions, such as hardware breakdown, cost of failure at all maintenance levels, and other statistical information. This could include time to failure of component

by failure mode, design life, impact on safety or the environment of each failure mode, can failure mode be predicted, function accept/reject criteria and consequence of failure.

Capturing operational data is necessary for the success of RCM analysis. Accurate data helps to provide the confidence needed to understand component inherent failure and to establish appropriate service limits.

The benefits of RCM maintenance program can be numerous. RCM will sustain higher levels of safety by providing a strategy for retaining inherent safety designed into the system. It also is used to prevent functional failures and reduce undetectable failures.

The RCM process provides the maintenance community with tools to establish an appropriate preventive maintenance program. It establishes specific data collection requirements and an audit trail that supports changes in maintenance requirements. With a dynamic program maintenance costs, unscheduled maintenance and shop visits can be reduced. This would result in increased operating time.

An RCM program is an integral element of a sound system Safety Program.

CHAPTER VI

CONCLUSION

Pre-Reliability Centered Maintenance aircraft and their systems were once maintained with "hard time maintenance" programs. These programs were too costly and didn't improve reliability, so a committee was formed to study system/component reliability. They developed maintenance program called MSG 1. This program was improved upon again and again. The DOD hired an airline to investigate the relationship between maintenance reliability and safety and this report was used to develop MSG 3.

The maintenance philosophy of a RCM program is focused on the reliability of components in a system. An analytical process is used to determine the failure modes and is fed into a critical decision matrix. From this matrix a preventive maintenance program is developed.

FMECA is a key element in developing a RCM program. Data fed into FMECA can be operational data or maintenance documentation. This accumulated data is analyzed and used as input into periodic maintenance decisions.

The payoff of developing a comprehensive maintenance program using RCM can be numerous. Aircraft will sustain higher levels of safety while reducing maintenance costs by reducing unscheduled maintenance and shop visits and increasing operational status. A successful RCM program must have commitment from the users as well as the owners.

REFERENCES

Moubray, J. (2000) Reliability Centered Maintenance. Retrieved February 14, 2003, from http://plant-maintenance.com/RCM -intor.shtml

Stark, J. (2000) Reliability Centered Maintenance Training Video (2000) GEK 10878

Moubray, J. (2000) Reliability Centered Maintenance. Retrieved February 16, 2003, From http://reliability-centered-maintenance.com/

COMPUTERIZATION OF AIRCRAFT MAINTENANCE

by

Chad Mansfield

Submitted in partial fulfillment of the requirements of
ASCI 611
Spring A 2003

Embry-Riddle Aeronautical University
Extended Campus
NAS Fort Worth JRB Residents Center
March 2003

TABLE OF CONTENTS

ABSTRACT

Writer: Chad Mansfield

Title: Computerization of Aircraft Maintenance

Institution: Embry-Riddle Aeronautical University

Degree: Master of Aeronautical Science

Year: 2003

Although computers have been around for years, integrating them into the aircraft maintenance industry is still in its infancy. As aircraft become more complex and systems more automated there is an increasing need for computer integration. Integration of not only Computer Based Training (CBT), but also of Portable Maintenance Aids (PMA's) which aid in reference and troubleshooting complex systems and various other maintenance tasks. Technology will not only have an impact on the Aircraft Maintenance Technician (AMT) from a human factor and training curriculum standpoint, but also it will impact the organizational information architecture as a whole. This will not only display changes in information management but also in financial and project management as well.

CHAPTER I

INTRODUCTION

> "Software safety is the newest member of the system safety field. With the incredible proliteration of computers and microprocessors to all countries of the world, their safety control becomes both paramount and difficult". (Bahr, p.161)

These changes have brought about all new challenges for not only the aviation industry but the global market as well. Globalization provides new and fast information all over the world. This has also prompted growth in many areas due to the fact that our economy can now function 24 hours a day, 7 days a week due to access to the many types of technologies and information. We now can expand business through our access to vendors, suppliers and customers worldwide. Our new economy has found wealth in information and technology and with that has been a transition from a blue-collar based industry to a white-collar service industry. "60 percent of the American gross national product and nearly 55 percent of the labor force" now account for information and technology areas (1998, p.5). This explosion of technology has spilled over into the aviation industry and specifically into aviation maintenance. Although other areas of aviation have encountered technological advancement, maintenance is just beginning to see the possibilities of computer integration from classroom curriculum to troubleshooting aids. The main reasons for the slow movement from technology into

maintenance is mainly due to earlier budgetary constraints within maintenance, unskilled personnel, and management priorities being placed in other levels of the organization.

Since this concept is practically new to maintenance, there have been many stumbling blocks along the way. Although other businesses may have a thorough understanding of its implications, maintenance is just the beginning to see its possibilities in the classroom and also the benefits it can offer in troubleshooting complex aircraft systems. Aviation software today is not only aircraft specific but also management specific. It can guide you in not only fixing the aircraft but also in managing it as well. The programs today are integrating all facets of the business, from computing flight plans to keeping track of aircraft components as well as invoicing.

This study does not only focus on the need of portable maintenance aids and their software applications but also on computer based training. This study will also touch upon the integration system and what technicians will need to know upon their installation. Technicians will also need to have an understanding of what this system can offer them and how they as individuals can stay abreast of this ever-changing market. We are now encountering an era of data overload, which requires the use and transmission of an abundant amount of information expeditiously and precisely.

CHAPTER II

WHY COMPUTERS IN AVIATION MAINTENANCE

There are many reasons for computers in aviation maintenance, the most obvious being to keep up with aircraft technology. Although maintenance in the past has been an industry that has kept all to itself, in today's emerging globalization of the aircraft manufacturers, airlines, and corporate operators, it has transcended a change of the entire aviation community.

With "the advent of new computer software specifically designed for maintenance operations, the job tracking workflow through the hangar-and of managing related maintenance management tasks-is simplified" (1998, p.52). What makes this successful and beneficial is the ability to streamline your work and eliminate errors as well as the increase of efficiency. According to Phil Sinclair-Harry, vice president of product marketing for Cimlinc, a company which has been designing software for CAD/CAM environment since 1974, "estimates that mistakes involving scrap, rework, and non-conformance and compliance issues can cost a maintenance operation anywhere from 20 to 25 percent of annual revenues" (Stroud, p.52). The whole objective to software design for the maintenance environment is to eliminate those cumbersome paper manuals and make use of computer software that will make the job faster and easier. The old format of "dry text with an occasional sketchy black and white illustration, is replaced with specific 'graphically rich' instructions with detailed, annotated color photographs of the part or item being repaired" (1998, p.52). There are also different types of software that

do different jobs; there are software applications for manufacturing, service, management, invoicing, and operations and others that encompass all these functions. That means software can be specifically designed to meet your needs and objectives. It is very important to make this transition, as aircraft are becoming more computerized and complicated. This means that our technicians need to be prepared to handle this new type of maintenance and overcome problems that develop. The only way to merge them is through technology integration and computer based-training; not only through the use of portable maintenance aids (PMA's).

CHAPTER III

THE INTRODUCTION OF PORTABLE MAINTENANCE AIDS

"The Portable Maintenance Aid (PMA) is an interactive maintenance tool that allows mechanics and engineers to analyze and solve airplane problems at the work site- in the hangar, on the shop floor, or at the line" (Boeing, p.4). It basically consists of an "entire technical library of key maintenance information in a laptop computer that a mechanic can carry directly to the airplane" (Smith, 1999, p.1). This is the new age of technology for the aircraft technician. It will not only allow him to perform his job safely but it will also give him the advantage of obtaining the latest information in the industry and at the same time being able to use the newest technology in aircraft maintenance to obtain that information. The use of PMA's has many advantages:

- Instant access to custom airline information
- Powerful customization features that allow you to add your own documents, add or edit tasks, and insert bookmarks and notes
- Extensive electronic links between related tasks, both within a document as well as between documents
- Intelligent graphics that facilitate navigation and text searches from illustrations
- Easy navigation and advanced search capability, including searches for words or numbers in titles, text, and graphics (Boeing, p.4).

Besides its portability to the maintenance site, today's PMA's offer a great deal in terms of increased productivity, increased profits, and time utilization. It can reduce schedule delays and cancellations by providing instant information. It can allow the possibility of working a problem before aircraft arrival. It also offers the ability to reduce costs due to its timeliness of information and precise research tools. "The Federal Aviation Regulation's (FAR) Part 43 specifies that an AMT must have in his/her possession the current maintenance manual, pertinent to the procedure that he/she is performing" (Rivera, 1996, p.3). Therefore the system must be easy to use and provide accurate information because in today's growing aviation community, time is money. Aircraft today are different than twenty years ago in term of automation. Consequently the new aircraft technicians of today need to be well versed on the use of computerization, yet there are still many who are not. It is important that the PMA be a useable tool and can easily be integrated into the organizational structure.

Usability is traditionally associated with five parameters:

- Easy to learn: The user can quickly become comfortable with the system
- Efficient to use: Once the user has learned the system, a higher level of productivity is possible
- Easy to remember: The user is to return to the system after a period of time and work with the system without retraining
- Few errors: Users do not make any errors; if they do, they can easily recover from them

- Pleasant to use: Users are satisfied by using the system (Rivera, 1996, p.5)

The basis for a successful system not only lies within its integration into the business, but also its practicality and acceptance among the work force. If employees feel it delivers what it promised, then it will be successful among the work force.

CHAPTER IV

COMPUTER BASED TRAINING

In the early days aircraft maintenance technicians worked on aircraft mostly through trial and error, as time has progressed, more and more of them were introduced to a more structured program which included classroom and hands on training. This included countless hours of lectures, which evolved into tapes and then films and videotapes. Although these phases were all important in getting where it is today, nothing can come close to the technological; changes that computer-based training (CBT) has brought to the classroom. CBT involves using computers with specifically designed software that resembles one-on-one training within a classroom setting. "From an educators point of view, the biggest advantage of CBT is that students can access information and learn at their own pace" (Smith, 1998, p.28). CBT can offer a lot of things that other types of training cannot, such as the use of high tech graphics, demonstrations, and the most important, a self paced individual paced program. "Along with making it easy to demonstrate the ways the different subsystems of an aircraft operate, it has proven especially valuable in teaching the logical progression of the troubleshooting process, including the paths of influence" (1998, p.28). This training really gives the student a realistic look into the task at hand through multi-media software, to visual schematics, component systems, and the option to choose appropriate testing equipment and perform tests as necessary.

CBT will never totally replace all facets of training, but it will become more widespread as the technology becomes more economical and our economy continues on its progression. There will also be an integration of different variations of CBT training such as Computer-Aided Instruction (CAI). With this type of training "There is an instructor always on hand to assist in the learning process, rather than leaving the student to work his way through a totally CBT-based course" (1998, p.29). Some people prefer the face-to-face interaction, which CAI has to offer. As PMA's become more a part of the aviation maintenance's profession, it will also bring CBT more into the mainstream as far as training is concerned. In order to use PMA's effectively, it would be a natural transition to incorporate CBT into your training curriculum. Both offer the same type of problem solving and troubleshooting scenarios and they both require interaction on the part of the user.

Other factors of CBT are its ability to offer unbiased education and up to date information. In a typical classroom there is always the natural tendency for the curriculum of the course to be biased towards the instructors area of expertise or towards the needs of the majority of the class. In addition, the course information is always up to date with the latest and greatest procedures and requirements within the industry. This could be advantageous in initial and recurrent training, as it would prevent re-training due to changes in particular areas. There is also the advantage of CBT offering the ability to be tailored to your specific company's needs and/or individual needs. This can prove to be cost efficient by preventing rework, which will keep the aircraft in the air. CBT, with

its ability to offer the latest in information, can save time and money in the instance that new equipment will be upgraded into the fleet. It would provide the training before the equipment arrives and in the long run saves money due to the jump-start in the familiarization process. The beauty of this is the instructor and the student can be hundreds or thousands of miles apart from each other. Many colleges and universities are now offering CBT as part of their course catalog reaching new areas throughout the world as well as the aviation industry.

CHAPTER V

TYPES OF AVIATION MAINTENANCE SOFTWARE

In today's growing computer industry, there are a variety of software applications, and the maintenance industry is not any different. There are "integrated maintenance management software programs that generate, manage, and/or track work orders, and inventory" (Decker, 1998, p.66). This can also come with options to transmit this information to accounting and also use bar coding capabilities. The technician that is directly involved with the task directly inputs this information, and this provides the most accurate information. There is also "bar coding for parts, components, and tasks" software, which is used by many operators because of the timesaving and accuracy advantages. One of the great benefits for all maintenance documentation is the use of the CD-ROM. This information can be put onto a server for everyone within the company to access. This also is a timesaving application as well, not only in terms of searching for information but also in the reduction of countless pages of revisions that constantly need updated. The only requirement now would be to throw away the old CD and install the new one, versus replacing each page at a time in a manual. Some software currently on the market incorporates troubleshooting techniques, which some aircraft can be downloaded to provide system status and fault information.

Oracle Service Resource Planning is one type of software that has been put onto the market to "automate the maintenance and repair service for airlines" (Stroud, 1998, p.55). This software was developed to allow for quick access to information, which

causes a reduced efficiency due to the amount of time it takes to make decisions. This software gives opportunities to access manuals, inventory, IPC, and parts ordering. It also allows a one stop transaction, and increased accuracy due to the access to parts and inventory through the IPC, which gives quick response to parts orders instead of the days of delay time that is normal. It also eliminates the amount of time the technician is in the library searching through volumes of manuals, instead of working on the aircraft.

Visibility creates and markets software called VisAer, which is "specifically designed for the maintenance, overhaul and repair market" (Stroud, 1998, p.55). It came about due to the need to differentiate a manufacturing setting of tracking inventory to a service setting of tracking projects. Within the service industry it is extremely important to be able to have the "ability to promptly respond to customers, to track rotables, man hours, and to issue timely invoices" (1998, p.55). Employees are able to access VisAer from their Personal Computers (PC's) through a window-based system.

Airline Technical Publishers (ATP) has also hit the market with their variations of software. Their software includes "huge amounts of technical data, maintenance manuals, parts, catalogs, Airworthiness Directives (AD's), service bulletins, and other information-from hard copy into a user friendly electronic format" (Stroud, 1998, p.55). This company also offers numerous databases for different manufactured aircraft, engine, and avionics systems. They also have introduced "ATP Maintenance Director, which is a Windows-based electronic logbook system that tracks just about everything that is part of the maintenance process: times and cycles on powerplants, life-limited parts, scheduled

maintenance, and component status and history" (1998, p.55). ATP also offers "maintenance schedules for different manufactured aircraft, including AD's, service bulletins, and type certificate data" (1998, p.55). This company, along with others, offers detailed training to implement the software within any company.

There are many aviation maintenance applications that are currently on the market that can prove to be an intricate part of the solution for success. The ones mentioned previously were just a few of the many that are available. Some of them can be purchased right off the shelf and integrated immediately and others offer the option of being tailored to your specific companies needs and requirements.

CHAPTER VI

INTEGRATION OF SOFTWARE APPLICATION INTO THE MAINTENANCE STRUCTURE

Computers with Internet access have proven to be a great working tool for not only maintenance but also all facets of business. The Internet had offered us access to all types of information and connected us globally to our suppliers, vendors, and customers. Many software applications today use the Internet as a way to connect people throughout the aviation industry to retrieve and offer up to date information. Yet integration of the software and the Internet capabilities is no small task. Before deciding on what software is right for your company, there is one aspect many companies forget, that is the user. "Managers should get feedback from their maintenance personnel as to what software and hardware are important" (Garetson, 1999, p.58). This is a very important step because Information Technology (IT) personnel are not well versed in the needs of aircraft maintenance software applications. Maintenance personnel know what they want to see in their computer systems. They should become involved in the designing process as United Airlines and Delta Airlines did with their in-house system. Maintenance personnel can be your best resource; they work with the information everyday and can offer good advice to how the format should be laid out and the processes and procedures for that application. Most of all to make it successful it should be user-friendly-if it is a system that is totally foreign or hard to work with it will be very difficult to implement. In addition to the design aspects, there are also the training aspects. There has to be a

formal structure to train the personnel and most important to train the trainers. The initial implementation of this project will come from trainers, so providing them proper training and access to information is very important.

The most important thing is senior management commitment to spend the time and money to do it right. Without this commitment, you won't get the right equipment, the software that meets your needs, or the training needed to make it work. Once you have their commitment you can look for software to meet your corporate needs, preferably one that is Windows 95 or Unix based. This will make it very familiar and easy to work with. You will also want to "look for a vendor that has been around for a while and has a good reputation for support" (Decker, 1998, p.66). When buying your hardware and computer equipment be sure to allow room, via memory and RAM, for expansion as the system changes and progresses. Most important to the operation of this new system is to have a knowledgeable person in charge of it to ensure its proper implementation and to validate its time and money savings to the company. These systems are very costly and time consuming upon initial start up but they can return a great deal to the company in task timesaving, information access, and real time and accurate data.

CHAPTER VII

CONCLUSION

Aircraft are becoming more complex everyday and the use of computerization is a necessity if we are to survive as an industry. Although other industries have seen the uses of computerization, it is just the beginning to become not only popular but also cost effective for aircraft maintenance.

In order to integrate a successful system, there has to be several key issues worked out. First, there must be management support, second, there must be financial backing of the project, third, there must be a strong participation within the Information Technologies departments within the company, and fourth, the system chosen must meet corporate objectives and procedures. Management approval and financial backing for implementation are the most important. As project manager, you must be able to demonstrate the possible savings in time and accuracy and how it will result in cost savings in order for management to jump on board. A strong project proposal of what system will be integrated, how it will be integrated, and why is very important. For instance, there will be less time in going to and from the library, timesaving in looking for materials in massive manuals, and timesaving in revision insertion due to the CD-ROM. There will be increased accuracy due to variations of search tools and the immediate access to all information and any possible variations that could occur within the problem at hand. This would be especially important in highly complex avionics systems evaluations. There will also be the savings in space. Manuals take up a lot of

space and CD-ROM's are no comparison in space requirements. This will allow for better space planning and growth.

Information Technologies must be able to be a project partner due to the fact it will take a great deal of incorporation into the existing system and if the system is going to be networked it will require their expertise as well. You want to ensure that the system meets all corporate requirements for software and it can be integrated on a timely schedule. There will also be the need for hardware as well. PMA's will require more laptops for use by the technicians and computers for any computer based training that might take place. This in turn will require that there be technical support in case of computer malfunctions and other like problems. In addition, you want the software to meet company objectives and procedures. Will it integrate into the formal procedures you now have in place? Is it going to give a return that meets corporate objectives? Those are all very important questions.

A good plan is your most important tool when integrating such a massive project. Proper communication with management, proper documentation, and thorough research will be necessities within the implementation process. As aviation grows so will the technological advancements, therefore creating room for growth within the new system and being a major factor for its future success.

REFERENCES

Bahr, Nicholas J. (1997). Software Safety. System Safety Engineering and Risk Assessment: A Practical Approach, pp 161.

Chandler, J.G. (1998, January). Software Solutions. Aviation Maintenance, pp.16-19.

Decker, B.D. (1998, May). Is There a Laptop in Your Future? Aircraft Maintenance Technology, p. 66.

Boeing Website. [On-Line] http://www.boeing.com/assocproducts/digital/faq.html (1999, November 28).

Geretson, M. (1999, September). E*-nable your Shop Floor. Aircraft Maintenance Technology, pp. 58-61.

Laudon, K.C., & Laudon, J.P. (1998). Management Information Systems New Jersey: Prentice-Hall, Inc.

Rivera, G. (1996, March). Human factor issues in interactive electronic technical manuals for aircraft maintenance [On-Line]. Available: http://members.aol.com/geo13/ietm.htm.

Smith, D. (1998, April). Welcome to the Future of Training. Aviation Maintenance, pp. 28-34.

Smith, S. (1999, February 16). Airline demand for Boeing's portable maintenance aid grown 100 percent---new, more powerful version on the way. Boeing News. [On-Line].

Available: http://www/boeing.com/news/releases/1999/news-release/9902kea.html.

Stroud, C. (1998, September). Software For Maintenance Firms. Aircraft Maintenance Technology, pp. 52-57.

TRAFFIC ALERT AND COLLISION AVOIDANCE SYSTEM

BY

James L. McCarthy

A Term Paper Submitted in Partial Fulfillment of the
Requirements of ASCI 611 System Safety for
Aviation/Aerospace

Embry-Riddle Aeronautical University
Fort Worth Resident Center
February 2003

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

As far back as the 1950's government and airlines began searching for a viable collision avoidance system for Aircraft. In 1956, the Civil Aeronautics Administration Technical Development Center reported that "results of tests that had been conducted over the last four years indicate that only general use of proximity warning devices would substantially reduce the steadily increasing threat of mid-air collisions" (ALLSTAR, 2000, p. 1). The general interest in developing traffic avoidance systems for aircraft was brought about by the ever-increasing growth in air traffic. Research and development was slow to evolve at first. However this was spurred on by the collision between two airliners over the Grand Canyon on June 30, 1956. In 1978 when a light aircraft collided with an airliner over San Diego U.S. pilots began to warm up to the idea of a collision avoidance system. In took 30 years of research and several systems were developed before one was considered acceptable.

In 1981, the Federal Aviation Administration (FAA) finally announced that it had decided to proceed with the

development and implementation of the Traffic Alert and Collision Avoidance System (TCAS). This paper will explore the evolution of TCAS, examine the pros and cons and take a look at the future.

CHAPTER II

THE BIRTH OF TCAS

In the wake of airborne disasters, airlines realized that they needed a system that could help prevent similar accidents. Companies soon began designing collision avoidance systems, but two problems hampered their efforts. First, many systems would require the airlines to equip their aircraft with expensive new hardware. Second, there was still a lot of development left to do before an adequate system would become available.

Because of these two problems research efforts since the mid 1970's have concentrated on the use of hardware already installed on most aircraft, namely the transponder of the Air Traffic Control Radar Beacon System (ATCRBS). Using transponders already installed in many aircraft for communication with the ground based ATCRB system developers could take advantage of existing hardware and technology to significantly move forward on the development and implementation of a viable collision avoidance system. This system became know as the Beacon Collision Avoidance System or BCAS.

The BCAS system worked basically the same way the Air Traffic Controller Radar System dose. Aircraft would be equipped with airborne interrogators that would be able to interpret data from nearby aircraft transponders to learn the location, speed and course of each plane and determine whether there is a potential threat.

In 1981, the FAA chose to pursue the onboard design approach used in BCAS rather than a ground-based collision avoidance system, which they were also looking into at the time. At this point BCAS was renamed TCAS. The FAA had now committed itself to TCAS, however, progress in implementing the system was slow. It would take a 1986 midair collision involving a Aeromexico DC-9 and light civil aircraft over Cerritos, California to prompt congressional legislation. This legislation required the FAA to implement the use of TCAS for all passenger carrying aircraft operating in the U.S. and a time schedule for the certification of a newer version of TCAS, called TCAS II.

CHAPTER III

THE EVOLUTION OF TCAS

TCAS and other similar devices have been in various stages of research and development since the early 1950's. Research studies have shown that the greatest danger of a collision lies in one aircraft overtaking another and in high aircraft density areas. The research also found that a warning to a pilot that a collision danger exists is not sufficient information to prevent the collision and that relative bearing of an existing collision threat must be known to the pilot to give him enough time to see the other aircraft and execute an avoidance maneuver.

TCAS is a sophisticated system of antennas, computer processors, cockpit displays and voice warnings, all carried onboard the aircraft. It includes a cockpit display which shows the pilot transponder equipped aircraft that are nearby. The system is totally independent of ground-based air traffic control.

There are basically three versions of TCAS. TCAS I is the first and is designed primarily for general aviation use. It can only indicate the bearing and relative

altitude of other aircraft within a selected range. It warns the pilot of an impending conflict but dose not give instructions on how to avoid the traffic. Pilots must visually identify the traffic to determine if the best course of action is to climb or descend. The second, TCAS II is intended for large commercial aircraft. It not only warns the pilot of an impending collision but also advises the pilot to go either up or down to avoid the collision. And, lastly a new system called the Airborne Collision Avoidance System or ACAS II is really TCAS II with an additional software upgrade called Change seven.

CHAPTER III

HOW TCAS WORKS

TCAS I uses information from transponders installed in other aircraft to provide Traffic Advisories (TAs) to the pilot. It detects and displays range and the approximate bearing of other aircraft if the aircraft is within a selected range, generally 10 to 20 miles. The system uses color-coded dots on a display to indicate which aircraft in the area poses a potential threat. This is referred to as a

Traffic Advisory (TA). When the pilot receives a TA it is up to him/her to maintain separation visually. TCAS I dose not tell the pilot what to do to avoid a collision. TCAS I can also report the altitude of nearby aircraft if that aircraft is equipped with a Mode c or Mode s transponder.

TCAS II dose everything that TCAS I dose but with greater range and bearing accuracy. In addition, this system also instructs the pilot with a visual and aural Resolution Advisory (RA) on which way to climb or descend to avoid a collision, provided the other aircraft is Mode C or S equipped. If both aircraft are equipped with TCAS II,

then the two computers offer deconflicting resolution advisories (RAs) so the pilots do not receive advisories that would cancel each other out and maintain the potential for a collision. This system doesn't just show the other planes on a display like a radar screen, but offers warnings and solutions in the form of traffic advisories (TAs) and resolution advisories (RAs).

TCAS II Change 7 (now called ACAS II) will be virtually the same as TCAS II but with many improvements to the software that makes the system more accurate and user friendly.

Needless to say, there were a few problems that occurred in the development of TCAS. One problem was with the directional capabilities of the antenna used with the system. Another problem was signal clutter. Additionally, software upgrades had to be developed to reduce the number of false alarms. However, the biggest initial problem was getting the pilots and controllers to use the system.

CHAPTER IV

THE FUTURE OF ACAS/TCAS II

As long as there are airplanes flying there will be a system developed to help assist pilot in avoiding mid-air collisions. ACAS/TCAS II is that system and with continued software upgrades at a much lower cost than an initial installation ($200,000 per aircraft) the system will continue to evolve long into the future.

The time is fast approaching when the system can help to relieve congestion and expedite the flow of air traffic. An example of this was tested in 1993 called the In-Trail Climb (ITC). It is intended to reduce fuel consumption and reduce separation criteria for transoceanic flights. This maneuver permits a trailing aircraft at a lower altitude to climb through the altitude of a preceding aircraft using ACAS/TCAS II as a separation aid. This would allow aircraft to save thousands of pounds of fuel. Other prospects for ACAS/TCAS include reduced separation on transoceanic routes, reduced spacing for departures in instrument conditions and could permit aircraft to establish and maintain separation intervals on final

approaches.

Another prospect for the use of ACAS/TCAS II is being able to transmit Global Positioning System (GPS) coordinates and altitude via a Mode-S data-link called the Automated Dependent Surveillance Broadcast, or ADS-B. This technology will be used to greatly extend the range and accuracy of the collision avoidance system to within a foot. Although basic elements of ADS-B have been defined, practical use by commercial airlines is still years away.

CHAPTER V

CONCLUSION

The Traffic Alert and Collision Avoidance System has become a standard for safety in the United States and abroad. Its impact and value is clear, no airline mid-air collisions have occurred in the U.S. since 1990, when airliners began equipping their aircraft with TCAS.

From the beginning, TCAS has dramatically improved pilots chances of successfully avoiding the chance of a mid-air collision. Pilots have come to rely on TCAS to give them the critical data they need to avoid collisions. It gives pilots the edge they need to ensure that their crew and passengers have the safest flight possible.

REFERENCES

MITRE's Center for Advanced Aviation System Development. (2002, January 08). Traffic Alert and Collision Avoidance System. www.mitre.org/pubs/showcase/tcas.html

HONEYWELL. TCAS – The Best Airborne Collision Avoidance Protection Available. (2002, May 16). Change 7, Improvements for the 21st Century. www.honeywelltcas/whitepapers.htm

Summary of the Fifty-Fifth Meeting, Special Committee 147. (2000, March 21). Minimum Operational Performance Standards for Traffic Alert and Collision Avoidance Systems Airborne Equipment. www.rtca.org/comm/sc147sum.asp

ALLSTAR Network. (2002, February 04). Traffic Alert/Collision Avoidance System. www.allstar.fiu.edu/aero/tcas.htm

MITRE's Center for Advanced Aviation System Development. (1998, December 31). TCAS In the Beginning. www.mitre.org/pubs/showcase/tcas.html