NAVSAFECEN TR-1/90
JANUARY 1989

(4)

SYSTEM SAFETY
RISK ASSESSMENT MANUAL

Approved for public release; unlimited distribution.

NAVAL SAFETY CENTER
NAVAL AIR STATION
NORFOLK, VA 23511-5796

NAVSAFECEN TR-90/1
JANUARY 1989

(4)

SYSTEM SAFETY
RISK ASSESSMENT MANUAL

Prepared by:

R. P. Kinzey (CSP)
System Safety Programs Directorate
Naval Safety Center
Norfolk, VA 23511-5796

Approved for public release; unlimited distribution.

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS NONE
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION / AVAILABILITY OF REPORT UNLIMITED
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) NAVSAFECEN TR-90/1	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION NAVAL SAFETY CENTER 6b. OFFICE SYMBOL (*If applicable*) 90	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (*City, State, and ZIP Code*) NAVAL AIR STATION NORFOLK, VA 23511-5796	7b. ADDRESS (*City, State, and ZIP Code*)
8a. NAME OF FUNDING / SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (*If applicable*)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (*City, State, and ZIP Code*)	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO.
11. TITLE (*Include Security Classification*) SYSTEM SAFETY RISK ASSESSMENT MANUAL UNCLASSIFIED	
12. PERSONAL AUTHOR(S) KINZEY, R. P.	
13a. TYPE OF REPORT FINAL 13b. TIME COVERED FROM _____ TO _____	14. DATE OF REPORT (*Year, Month, Day*) 1989, JAN, 19 15. PAGE COUNT 47
16. SUPPLEMENTARY NOTATION	

17. COSATI CODES		
FIELD	GROUP	SUB-GROUP
12	03	
13	12	

18. SUBJECT TERMS (*Continue on reverse if necessary and identify by block number*)
PLEASE USE THE FOLLOWING POSTING TERMS: SYSTEM SAFETY, SYSTEM SAFETY ENGINEERING, SYSTEM SAFETY MANAGEMENT, RISK ASSESSMENT, HAZARD INDEX, AND RELATIVE WORTH.

19 ABSTRACT (*Continue on reverse if necessary and identify by block number*)

This guide was prepared to assist system safety managers in making informed risk management decisions. Additional guidance is available from command system safety instructions and handbooks. The information is drawn from MIL-STD-882B, Navy Safety School Course Material, and other safety information sources.

Successfully managing safety risk is basic to a successful system safety program. Over the years, several tools to manage safety risk have evolved. This guide compiles several of the more common ways of defining safety risk. When managing several systems (e.g., command system safety manager) which are competing for resources, the classical MIL-STD-882B approach is not always fully effective. Therefore, a new management concept referred to as relative worth index and a safety performance baseline are introduced.

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT ☑ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION
22a. NAME OF RESPONSIBLE INDIVIDUAL R. P. KINZEY	22b. TELEPHONE (*Include Area Code*) 804-444-5093 22c. OFFICE SYMBOL 90B

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted. All other editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE

FOREWORD

This guide was prepared to assist system safety managers in making informed risk management decisions. Additional guidance is available from command system safety instructions and handbooks. The information is drawn from MIL-STD-882B, Navy Safety School Course Material, and other safety information sources.

Successfully managing safety risk is basic to a successful system safety program. Over the years, several tools to manage safety risk have evolved. This guide compiles several of the more common ways of defining safety risk. When managing several systems (e.g., command system safety manager) which are competing for resources, the classical MIL-STD-882B approach is not always fully effective. Therefore, a new management concept referred to as relative worth index and a safety performance baseline are introduced.

EXECUTIVE SUMMARY

Risk assessment is the process of assessing the level of risk. Risk management is the process of controlling risk to an acceptable level. Risk can be anything which could interfere with the accomplishment of a task or mission. In system safety, safety risk is the possibility of a mishap with the maximum possible consequences. Mishaps decrease operational readiness and have a major impact on schedules and program resources. With the cost of new systems rapidly increasing, mishaps must be reduced to control costs. For example, the A-7, when in production, cost the Navy roughly $2.8M. Mishaps (CY84-CY88 May) added $200 per flight hour due to 6.28 Class A mishaps per 100,00 flight hours. To achieve the same mishap cost, the F/A-18 ($22.8M each) would have to average less than 1 Strike loss per 100,000 flight hours. Although, the F/A-18 has a better safety record than the A-7 (4.3 Class A mishaps per 100,000 flight hours), mishaps add $1000 per flight hour to the operating cost due to attrition.

Prior to initiating a system safety program, the unacceptable level of safety risk must be specified. The standard practice is to define risk in terms of maximum possible mishap severity (hazard severity) and the probability of occurrence of a hazard. Hazard categories are aligned closely with the DOD definition of a mishap. A hazard is a prerequisite to a mishap. For example, fuel leaking into a space with hot surfaces could be ignited (fire hazard). If the resulting fire could cause loss of the system, the hazard is considered to be potentially catastrophic. If the likelihood of a fuel leak into the compartment is considered high, the combination of the consequence and the high likelihood that the mishap will occur are unacceptable. Safety risk can be reduced to an acceptable level by controlling hazards (eliminating or reducing the probability that a hazard will occur). Control measures could be: (1) totally eliminating the hazard by taking a different design approach, (2) providing protective barriers to contain damage, (3) providing warning devices to alert operators to the need for corrective action, or (4) implementing special procedures. In the example above, rerouting fuel lines or reducing fuel line connections in the compartment would reduce the probability of fuel leak. Risk could be further reduced by providing thermal protection for critical components, reducing the temperature of hot components (ignition source), and installing a fire suppression system.

To ensure program resources are properly allocated to correct hazards, the risk associated with a hazard must be defined. Over a number of years, MIL-STD-882B "System Safety Program Requirements" and the system safety community have developed techniques to describe risk. A major portion of this manual is devoted to describing this process. The other portion of the

manual outlines a process for assessing the safety risk associated with multiple system safety programs typical of a headquarters or command level activity. The Navy operates over 140 different models of aircraft. Therefore, the question that a headquarters System Safety Manager must ask is "With the limited resources available, where do I place the system safety emphasis?". In order to answer this question, the Naval Safety Center attacked the problem two ways. The first approach was to establish a safety performance baseline based on types and models of aircraft. The aircraft baselined were those employed for tactical purposes (Tactical Aircraft or TACAIR) and rotary wing aircraft. The factors considered were:

a. Number of overall losses

b. Dollar losses

c. Number of fatalities

d. Number of losses associated with material failure/malfunction of aircraft subsystems

e. Number of losses associated with pilot error

The data is displayed in graphical format to allow easy comparison. The factors that were considered in developing the baseline criteria were:

a. Class A rate per 100,000 flight hours

b. Percentage of mishaps versus percentage of flight hours

c. Dollar losses by model and as a percentage of flight time

d. Number of fatalities and percentage of fatalities as a percentage of flight time

e. Percentage of involved material component Class A mishaps by major subsystem

f. Percentage of pilot error mishaps due to mismanagement of major subsystems

The above process provides a methodology to establish a safety baseline using a number of factors. Models of aircraft which exceed the baseline probably require additional system safety emphasis. The major objective of this process is to allow System Safety Managers to identify potential problem areas and to provide a basis for establishing safety performance criteria for

contracting purposes. The process to identify basic areas of pilot error could be utilized to improve other non-design support areas such as training.

The second approach was to assess the cost of a Class A mishap in terms of:

a. Loss of operational capability

b. Potential loss of life

c. Loss of expected service life

d. Surplus or shortfall of assets

e. Strike cost or replacement dollar value

The result was a Relative Worth (RW) Index ranking of aircraft models based on subjective weighting factors. By establishing the relative worth of models of aircraft, a System Safety or Program Manager should have a selling point to obtain resources for initiatives that could have a significant safety payoff.

In summary, this manual describes various methods to assess safety risk and to highlight problem areas. The methods are easily implemented using existing data available from the Naval Safety Center. The intended users are system safety and program managers. Other users who might benefit from this approach are command safety managers, safety officers, and analysts.

TABLE OF CONTENTS

DEFINITIONS

a. Hazard. A condition that is a prerequisite to a mishap.

b. Hazard Category. Hazard severity expressed in qualitatative terms (usually Category I - IV).

c. Hazard Index. Qualatative expression of risk in numerical terms.

d. Hazard Probability. The aggregate probability of occurrence of the individual hazardous events that create a specific hazard.

e. Hazard Severity. An assessment of the worst possible mishap that could be caused by a specific hazard.

f. Mishap. An unplanned event or series of events that results in death, injury, occupational illness, or damage to or loss of property.

g. Risk. An expression of the possibility of a mishap in terms of hazard severity and probability.

h. Risk Assessment. An assessment of the level of risk from identified hazards

i. Risk Assessment Code (RAC). A qualitative expression of risk, usually expressed by an alphanumeric code (IA, IIB, etc.).

1.0 Introduction to System Safety

Safe system operation is vital in achieving operational readiness. Through safety awareness in design and operational procedures, a high degree of freedom from mishap potential can be obtained and maintained. A cost effective method for achieving this objective is System Safety Management/Engineering. The impetus for this discipline has been the enormous and needless waste of resources and reduction in combat capability due to mishaps. The high cost of new systems means that fewer systems can be bought. Older systems are being replaced with newer, more expensive systems; therefore, unless the number of mishaps are reduced, operating costs will continue to increase. (See Figure 1). System complexity requires use of a formalized safety analysis approach to ensure all system hazards are identified and corrected.

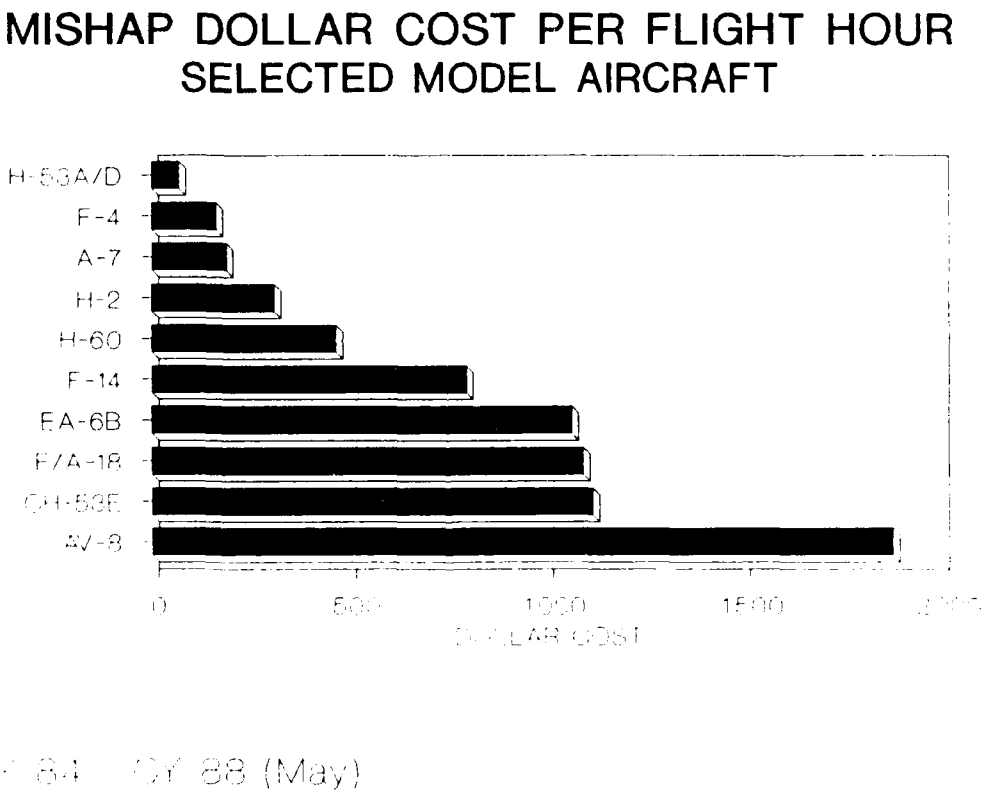


Figure 1

System safety is easily obtained within the constraints of mission performance, schedule, and cost. Maximum effectiveness is obtained by applying system safety principles early and throughout the life cycle of the system.

Specifically, system safety is defined as "the optimum degree of safety within the constraints of operational effectiveness, time, and cost attained through specific application of system

management and engineering principles throughout all life cycle phases of a system". It is an evolved discipline from the past when the safety approach was "fly-fix-fly". The new safety approach is "identify-analyze-control". System safety management is the key to an effective program which ensures significant hazards are identified, analyzed, and controlled. The effort is most effective when applied at program milestone "0". It is further reinforced by the acquisition system safety agencies. These agencies ensure that system safety requirements are in the request for proposal, specifications, and standards. From the conceptual and validation phases, the output of the system safety management team (trade studies and analytical efforts) works to keep risks below a mandated threshold value. This is accomplished by adjusting the design and providing management with an informed appraisal of risk for directed correction or acceptance. Mishap loss control numerical goals can be contractually established. Financial incentives can then motivate a contractor to meet or exceed the system safety goal.

Early attention to engineering considerations minimizes design changes to correct safety deficiencies. Late safety design changes and additions are expensive. Late hardware changes historically add weight, complexity, decrease reliability, and increase maintenance time. More importantly, late changes impact on the primary program resources of time and money.

1.1 Primary Objective and Function

System safety's primary function is to increase operational readiness by designing safety into systems. This is accomplished through a risk management process by identifying and classifying hazards as to safety risk. Preferably, this hazard analysis process takes place before final design decisions are made. However, this process is a life cycle requirement. If the risk is unacceptable (quantitatively or qualitatively), the system safety manager should direct corrective action. Obviously, the earlier an unacceptable hazard is identified and eliminated, the less adverse impact there will be on the project. In fact, early attention to design safety details results in little or no impact on cost or schedule. Overall system performance actually increases due to fewer safety restrictions.

2.0 System Safety Management

System Safety Management consists of several levels. At the primary level is individual program management. At the intermediate level is the administration of contracts and resources to manage a command's system safety program. At the upper level is the policy making area where system safety goals and objectives are established and monitored. MIL-STD-882B risk

assessment guidelines work well at the individual project level. Whenever resource allocation has to be split between projects and programs (intermediate level), the classical 882B approach fails. The purpose of this manual is to provide some guidelines for managing single and multiple projects.

3.0 Risk Assessment

Decisions regarding the resolution of identified hazards (mishap causal factors) are based on an assessment of the safety risk involved. Safety risk is the possibility of a mishap loss in terms of hazard severity and probability. Safety risk can be expressed only in terms of the maximum possible mishap (hazard severity) that could reasonably be expected to occur if the proper conditions are met. However, the usual practice is to try to define risk in both terms of severity and probability. Hazard probability is usually expressed in qualitative or, sometimes, quantitative terms. The standard practice is to express risk in terms of Risk Assessment Codes (RAC) or occasionally a Hazard Index (HI). RAC and HI are explained in paragraph 7.

3.1 Risk Management

Risk management is the process used to control risk once the magnitude of the risk is understood. The purpose of this manual is to provide some guidelines to personnel who have to make risk management decisions. Basic to this process is the defining of unacceptable and acceptable level of safety risk. Risk is measured with a RAC or HI. Therefore, unacceptable hazards can be defined as those hazards with a RAC/HI at or above a certain level. The primary emphasis in this report is directed toward the naval aviation system safety program. However, the same processes could be applied to any system safety program.

3.2 Elements of Risk

The elements of risk from a system safety standpoint are:

a. Potential degradation of mission capability due to equipment destruction/damage/loss of key personnel.

b. Potential loss of life/personnel injury/occupational illness/permanent or partial disability

c. Potential dollar loss.

d. Potential loss of public confidence due to needless and costly mishaps, destruction of private property; cause death injury, or illness to private citizens; generate hazardous waste and pollution

e. Potential schedule and dollar impact from unforeseen safety problems.

MIL-STD-882B risk assessment guidelines work well when applied to single systems (hazard severity and probability). However, this approach has limited application toward managing multiple systems. A Category I hazard could result in a Class A mishap. However, a Class A mishap involving 4 fatalities is more severe than one involving 1 fatality. A Class A mishap costing 30M is more severe than one costing 10M. Losses of certain aircraft can have a far greater impact on operational readiness than other types. An E-2C loss has a much more significant impact on readiness than an F/A-18A. Other aircraft, if lost, could be out-of-production or a one of a kind development test model. Replacement, even when possible, would be difficult, time consuming, and expensive. The same undesired event (hazard) may have different risk factors depending on time and spatial considerations. For example, an engine loss on a multi-engine aircraft will have greater significance during takeoff or landing than it will during cruise. Other considerations involve the reliability of one-time emergency devices such as escape systems.

Every endeavor has some risk, whether safety or mission related. The primary system safety mission is to reduce safety risk associated with the operational mission. Reducing safety risk increases operational readiness. Readiness is increased by:

a. Preserving assets (Materiel/Personnel) needed to support the operational mission

b. Decreasing safety restrictions by an appropriate design for the mission.

4.0 Defined DoD Mishap Categories

DOD mishaps are defined by DODINST 6055.7. Mishaps are classified as class A, B, C, and sometimes, D. A class A mishap is the most severe and D the least severe. The mishap classification standard (proposed for use in FY90) is:

Class A Mishap. The resulting total cost of reportable property damage is $1,000,000 or greater; or a DOD aircraft or spacecraft is destroyed; or an injury/occupational illness results in a fatality or permanent total disability.

Class B Mishap. The resulting total cost of reportable property damage is $200,000 or more, but less than $1,000,000; or an injury/occupational illness results in permanent partial disability; or when five or more personnel are hospitalized.

Class C Mishap. The resulting total cost of reportable property damage is $10,000 or more, but less than $200,000; or an injury/occupational illness results in a lost workday case with one or more days away from work.

Class D Mishap. The resulting total cost of reportable property damage is less than $10,000; or an injury/occupational illness results without a lost workday.

5.0 Hazard Categorization

The existence of a hazard doesn't mean that a mishap will occur. A hazard is a condition that is a prerequisite to a mishap. However, if the hazard did occur, it could result in a mishap of certain severity. Thus, each hazard is assigned a severity code based on the maximum credible mishap that could occur. MIL-STD-882B uses the Table 1 hazard severity codes or categories which have been combined with DODINST 6055.7 mishap categories.

HAZARD SEVERITY CODES/CATEGORIES

Hazard Description	Category	Mishap Definition*
CATASTROPHIC	I	Death, permanent total disability, system loss, or Class A mishap.
CRITICAL	II	Severe injury, severe occupational illness, permanent partial disability, major system damage, or Class B mishap.
MARGINAL	III	Minor injury, minor occupational illness, minor system damage, or Class C or D mishap.
NEGLIGIBLE	IV	Less than minor injury, occupational illness, or death.

*Class A, B, C, & D mishap categories are not used in MIL-STD-882B

Table 1

These hazard severity categories provide guidance to a wide variety of programs. However, adaptation to a particular program is generally required to provide a mutual understanding between the procuring activity and the contractor as to the meaning of

the terms used in the hazard category definitions. The adaptation must define what constitutes system loss, major or minor system damage, and severe and minor injury and occupational illness. The most straightforward approach is to apply DODINST 6055.7 loss, injury, and occupational illness criteria as shown in Table 1.

6.0 Hazard Probability

Hazard probability can be described in qualitative or quantitative terms. Hazard probability can be described in potential occurrences per unit of time, events, population, items, or activity. Assigning a quantitative hazard probability to a potential design or procedural hazard is generally not possible early in the design process. In fact, the usual practice is to exclusively use qualitative probabilities. If required, a quantitative hazard probability may be derived from research, analysis (Fault Tree Analysis, etc.), and evaluation of historical safety data from similar systems. Supporting rationale for assigning a hazard probability (qualitative or quantitative) should be documented in hazard analysis reports.

6.1 Qualitative Hazard Probability

An example of a qualitative hazard probability ranking is provided in Table 2. It is not essential that hazard probabilities be established or used. However, without a hazard probability, no hazard category I or II hazards can be accepted. The hazard must be eliminated by design since the effectiveness of control measures could not be established.

6.2 Quantitative Hazard Probability

Generally speaking, qualitative hazard probabilities are used early in the development phase. As the program progresses, additional data may allow quantitative expression of hazard probability. Management care must be used to ensure that the process of quantifying doesn't overshadow the primary objective. A format for a quantitative hazard probability is listed in Table 3.

The measuring base; i.e., operating hours, must be meaningful for the system under examination. Some systems may be evaluated by numbers of missions or the probability of success, e.g., an escape system. If extended missions (days, weeks, months, or even years) are common, operating hours can accumulate rapidly. Systems that must operate far at sea without access to emergency facilities require careful thought before establishing hazard probability criteria.

QUALITATIVE HAZARD PROBABILITIES

Description*	Level	Specific Individual Item	Fleet or Inventory**
FREQUENT	A	Likely to occur frequently	Continuously experienced
PROBABLE	B	Will occur several times in life of an item	Will occur frequently
OCCASIONAL	C	Likely to occur sometime in life of an item	Will occur several times
REMOTE	D	Unlikely but possible to occur in life of an item	Unlikely but can reasonably be expected to occur
IMPROBABLE	E	So unlikely, it can be assumed occurrence may not be expected	Unlikely to occur, but possible

*Definitions of descriptive words may have to be modified based on quantity involved.

**The size of the fleet or inventory should be defined.

Table 2

QUANTITATIVE HAZARD PROBABILITY*

Descriptive Word	Level	Specific Individual Item	Fleet or Inventory
Frequently	1	Likely to occur frequently a. One or more times per 10,000 operating hours b. One or more times per 100,000 flight hours	Continuously experienced/ One or more times per year
Probable	2	Will occur several times a. 1 to 10 per 100,000 operating hours) b. Less than 1 per 100,000 Flight Hours but 1 or more times per 300,000 Flight Hours	Will occur frequently/ Once every 3 years
Occasional	3	Likely to occur in life of an item a. Less than once per 100,000 operating hours b. Less than once per 300,000 Flight Hours	Will occur several times in system lifetime
Remote	4	Very unlikely to occur	Unlikely, but can reasonably be expected to occur
Extremely Improbable	5	Probability of occurrence cannot be distinguished from zero	Very unlikely to occur
Impossible	6	Physically impossible	Physically impossible

*Quantitative probabilities listed are examples. Specific quantitative probabilities should be tailored to each item.

Table 3

7.0 Risk Assessment Procedures

Risk as used herein refers to safety risk. Risk is defined as the possibility of a mishap in terms of hazard severity and hazard probability. In large system safety programs, such as aviation, it is not unusual to identify several hundred hazards. In order to ensure consistency in processing the disposition of each hazard, an easy to use method of expressing risk is necessary. Many risk assessment procedures have been developed. The usual practice is to use an alphanumeric Risk Assessment Code (RAC) designation such as IA, IVB, etc., or a numerically based Hazard Index. Both RAC and HI are generally qualitative in nature. The most important factor in the success of a system safety program is consistency in assigning a proper level of risk to each hazard and establishing a level of unacceptable or acceptable risk early in the development program. This allows management attention to focus on those hazards with the greatest mishap loss potential.

7.1 Risk Assessment Code (RAC)

A typical safety risk matrix based on RAC's is provided in Table 4.

RISK ASSESSMENT CODE MATRIX

INCREASING SEVERITY ↑				
	IA (UNACCEPTABLE RISK)	IB	IC	ID
	IIA	IIB	IIC	IID
	IIIA	IIIB (ACCEPTABLE RISK)	IIIC	IIID
	IVA	IVB	IVC	IVD

DECREASING PROBABILITY ——————>

Table 4

The Roman numerals portion of the RACs are derived from the hazard severity codes defined in paragraph 6.0. The letter portion is a qualitative assessment of hazard probability based on the coding system provided in paragraph 6.1.

7.1.1 Naval Aviation Risk Assessment Codes

The Naval Aviation Safety Program (OPNAVINST 3750.6P) uses a slightly modified MIL-STD-882 Risk Assessment Code format.

7.1.2 Hazard Severity (Naval Aviation)

Hazard severity is an assessment of the worst potential consequence, defined by degree of injury, aircraft damage, or property damage, which could ultimately occur or recur. Hazard severity categories are assigned by Roman numeral according to the following criteria:

a. Category I: Catastrophic: May cause a fatal injury or loss of an aircraft.

b. Category II: Critical: May cause a defined naval aircraft mishap.

c. Category III: Marginal: May cause injury, aircraft damage, or property damage less than that defined as a naval aircraft mishap.

7.1.3 Hazard Probability (Naval Aviation)

Hazard probability is the likelihood that a hazard of certain severity will occur. Hazard probability subcategories are assigned a letter designation according to the following criteria:

a. Subcategory A: Will occur frequently

b. Subcategory B: Will occur occasionally

c. Subcategory C: Will occur rarely

The number of times (frequency) per 100,000 flight hours is not referenced in OPNAVINST 3750.6P. Probability is usually assessed qualitatively vice quantitatively. Suggested quantitative values are: frequently (one or more times per 100,000 flight hours), occasionally (less than one per 100,000 flight hours, but 1 or more times per 300,000 flight hours), and rarely (less than 1 per 300,000 flight hours).

7.1.4 Risk Assessment Code (Naval Aviation)

A RAC for naval aviation is obtained by combining hazard severity code with hazard probability (IA, IB, etc.). Risk assessment codes of IA, IB, and IIA are considered severe hazards. IC, IIB, IIC, IIIA, IIIB, and IIIC identify routine hazards.

7.2 Hazard Index

The Hazard Index is another method of expressing risk. It is a parallel system to RAC, but is usually more complicated to apply. Instead of alphanumeric codes, the hazard index is numerical. The HI is a relative numerical statement of risk in qualitative terms. The HI can be determined by several means. The simplest method is that of multiplying the numerical values assigned to hazard severity and mishap probability. The HI has no dimensions or significance as an absolute numerical value. It serves only as a tool to rank potentially hazardous conditions. The managing activity may assign threshold HI values for which the contractor is required to take specific actions.

Table 5 is an example of a hazard index matrix. For this example, numbers I through IV are assigned for hazard severity and 1 through 6 for probability. An HI of 3 or less requires the contractor to take action to reduce the hazard probability. These numbers may be adjusted to fit a specific system as long as continuity is maintained.

HAZARD INDEX

	HAZARD PROBABILITY INDEX					
Hazard Severity Index	Frequent 1	Reasonably Probable 2	Occasional 3	Remote 4	Extremely Improbable 5	Impossible 6
Catastrophic I	1	2	3	4	5	6
Critical II	2	4	6	8	10	12
Marginal III	3	6	9	12	15	18
Negligible IV	4	8	12	16	20	24

Table 5

This technique can be used with a weighted HI. A weighted HI is developed by applying the Table 5 severity and probability numbers and the formulas shown below:

$$HI = ((4\text{-Hazard Category})*(6\text{-Hazard Probability Level}))^{1.7}$$

The primary advantage of this system is better separation between high probability Category I and III hazards. Using 1.7 as a weight factor gives a HI of 100 (rounded off) for the highest probability Category I hazard. The risk acceptance criteria could be to correct or control hazards for HI's of 15 and above with priority devoted to the higher numbers.

Historically, HI's are useful as a management tool only if the procuring activity has the ability to evaluate the HI for accuracy. All Category I and II hazards must be reported to the procuring activity regardless of the HI assigned. The procuring activity must reserve the right to accept or reject a contractor's proposed HI.

8.0 Managing Multiple System Safety Programs

Managing multiple system development and systems after deployment presents a major challenge. Limited resources force system safety managers to judiciously allocate resources. In this section two major topics will be discussed:

a. Establishing a safety performance baseline

b. Establishing the relative worth of systems

By establishing a safety performance baseline for classes of systems, two benefits are evident:

a. Performance criteria for new systems can be contractually specified

b. Out of tolerance performance can be detected and corrective action taken sooner

By establishing the relative worth of systems, hard decisions can be made easier. If system A is worth more than system B, system A should receive more attention (resources).

8.1 System Safety Performance Baseline

Establishing a performance baseline should be accomplished two ways:

a. A system baseline for the safety performance for classes of systems as measured by an established baseline; ie., expected mishaps per 100,000 flight hours, X number of mishaps per steaming hour

b. A subsystem baseline for the contribution of subsystem failures/human error to the overall mishap rate

A system baseline is established by reviewing the mishap records for types of systems over a number of years. Types of systems might include Tactical Aircraft (TACAIR) or Rotary Wing. The minimum time base should be 3 years. The following factors should be considered:

a. Number of Class A mishaps

b. Number of fatalities

c. Dollar cost

d. Contribution of major subsystems to Class A mishaps

e. Contribution of pilot error to Class A mishaps

Figures 2 and 3 show the Class A mishap rate by model and as a percentage of mishaps for Tactical Aircraft (TACAIR) from FY84-FY88 (May). Based on this historical data, any model tactical aircraft that exceeded 6 mishaps per 100,000 flight hours would be above the expected norm. Figures 4 and 5 show the Class A rate for Rotary Wing (helicopters) for the same period. Therefore, a model of a rotary winged aircraft should not be expected to exceed 3.5 mishaps per 100,000 flight hours. Excursions in any given year could occur. Over a period of years, a particular model aircraft should be at or below the community mishap rate or expected norm. If it is not, then research into improved control measures such as design, training, and utilization may be warranted and easily justified. Understandably, some aircraft fly a more demanding mission, but acceptance of the mission by itself as a reason for the higher rate should not be permitted. Operational readiness dictates that missions can be successfully executed with minimum risk to mission assets.

If dollar losses are spread over all of naval aviation, it is difficult to identify loss leaders. If, however, dollar losses are associated with the % of flight time in an aircraft community such as TACAIR or Rotary Wing, high dollar loss models stand out. Figures 6 and 7 demonstrate this principle for the A-6 aircraft.

Establishing a baseline for fatalities presents a dilemma. For example, some tactical aircraft carry a crew of one, while others may have 4 to 11 crew members. Fatalities could be counted using

crew hours vice flight hours. This method has some merit. The problem is that it can mask higher than expected numbers of fatalities associated with a particular aircraft. The best way is to look at the percentage of fatalities associated with a particular model aircraft as a percentage of community flight time. Figures 8 and 9 are examples of this concept.

A baseline for aircraft subsystems can be established by breaking down systems along the same lines as those used by Work Unit Codes (WUCs). This would allow an evaluation of aircraft systems by major assemblies (subsystems). The Naval Safety Center has a code for Involved Material Component (IMC) which addresses aircraft material design, failure or malfunction involved as a factor in mishaps. This IMC data was slightly modified to correlate closer with WUC and fixed wing and rotary wing systems. Figures 10 and 11 show the percentage of overall Class A mishaps with at least one or more involved material component(s) by model for TACAIR and Rotary Wing. If the percentage is above average, additional research may be indicated. Care should be taken to ensure that skewed numbers are not the result of a few Class A mishaps with involved material component problems.

Figures 12 and 13 are baselines showing the contribution of involved material component Class A's by subsystem. Generally speaking, the highest percentage of involved material component

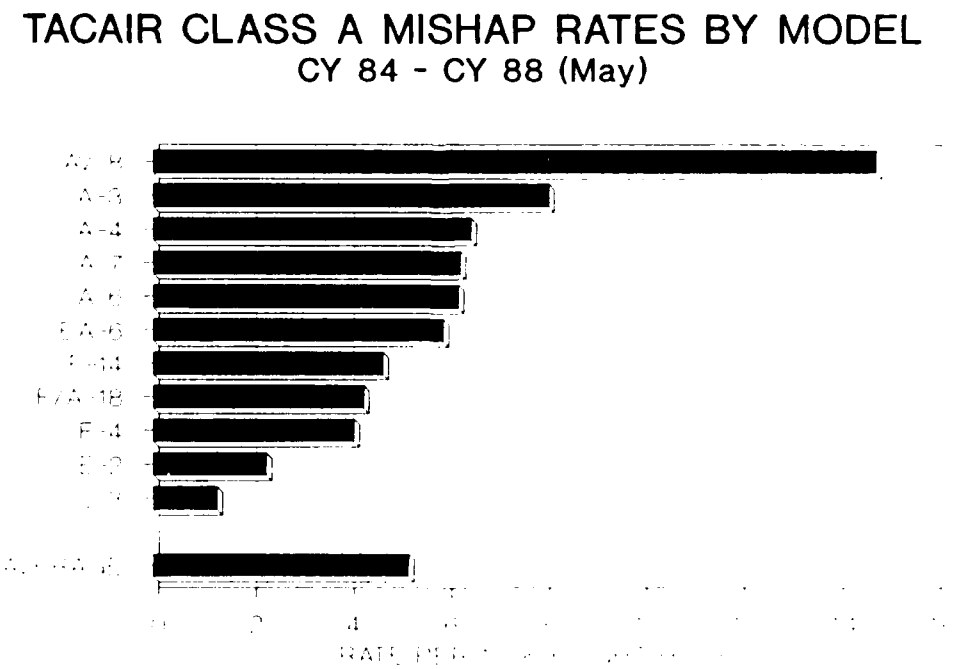


Figure 2

% TACAIR CLASS A MISHAPS BY MODEL
CY 84 - CY 88 (MAY)

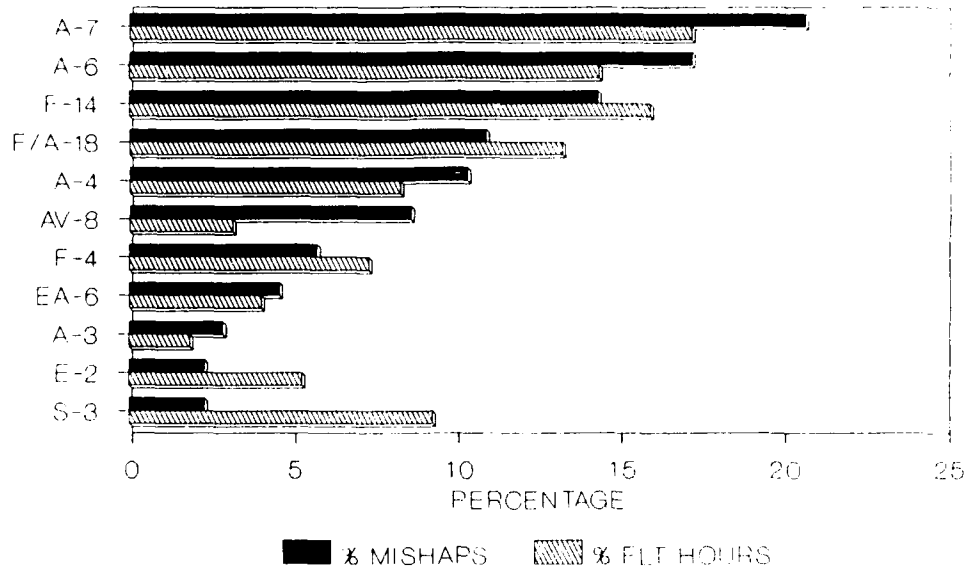


Figure 3

ROTARY WING CLASS A MISHAPS BY MODEL
CY 84 - CY 88 (May)

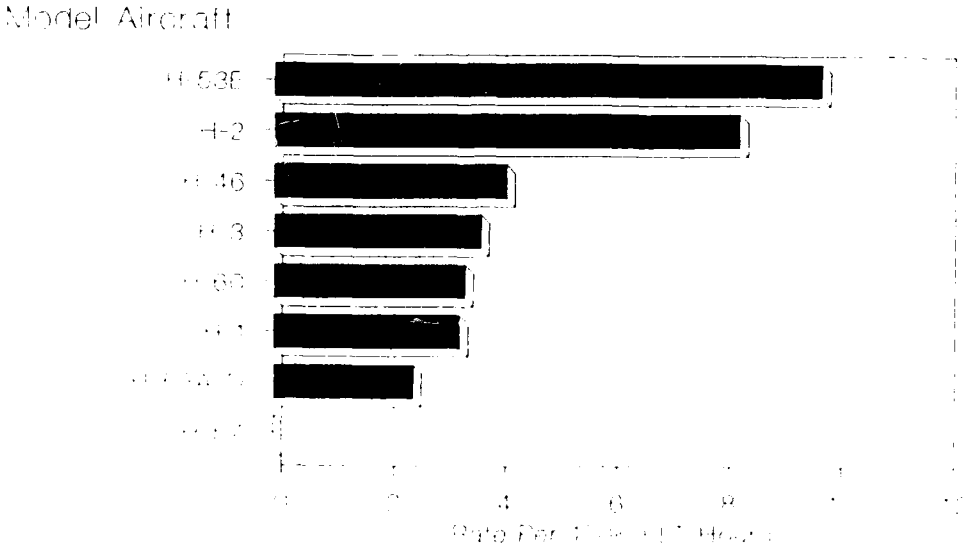


Figure 4

% ROTARY WING CLASS A MISHAPS BY MODEL
CY 84 - CY 88 (May)

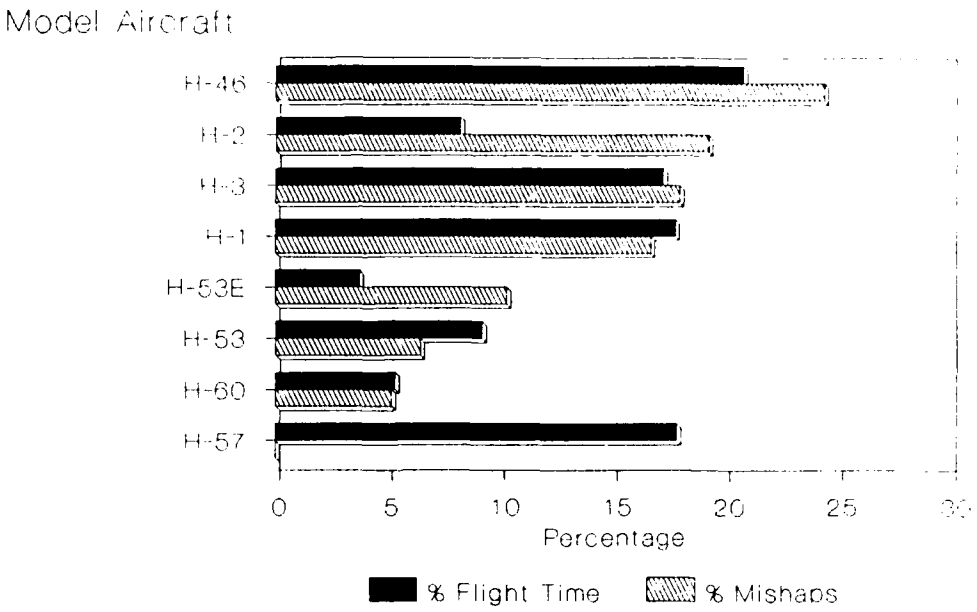


Figure 5

A-6 CLASS A DOLLAR LOSSES VS TACAIR
CY 84 - CY 88 (May)

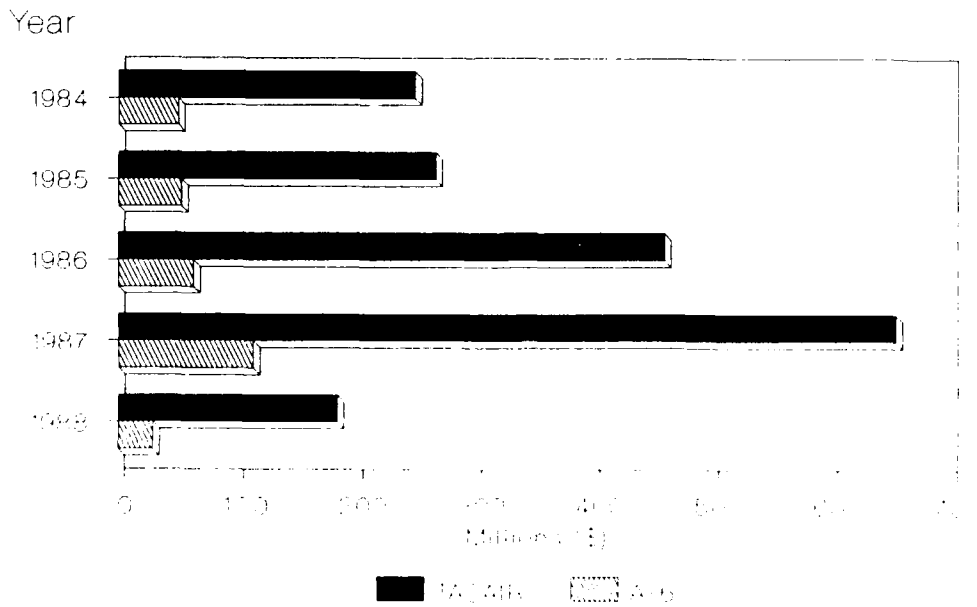


Figure 6

% A-6 DOLLAR LOSSES VS TACAIR
CY 84 - CY 88 (May)

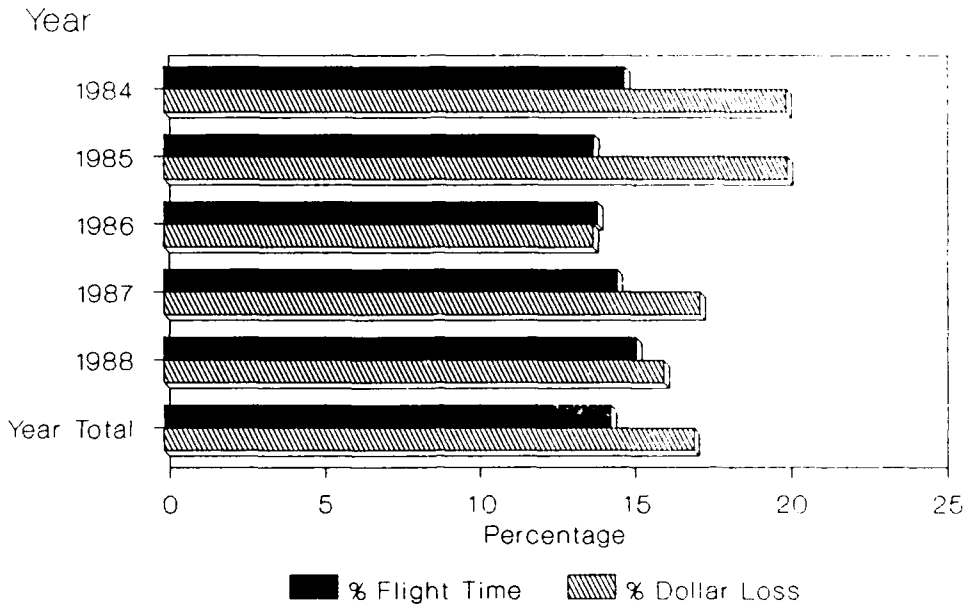


Figure 7

No. A-6 FATALITIES VS. TACAIR
CY 84 - CY 88 (May)

Figure 8

% A-6 FATALITIES VS TACAIR
CY 84 - CY 88 (May)

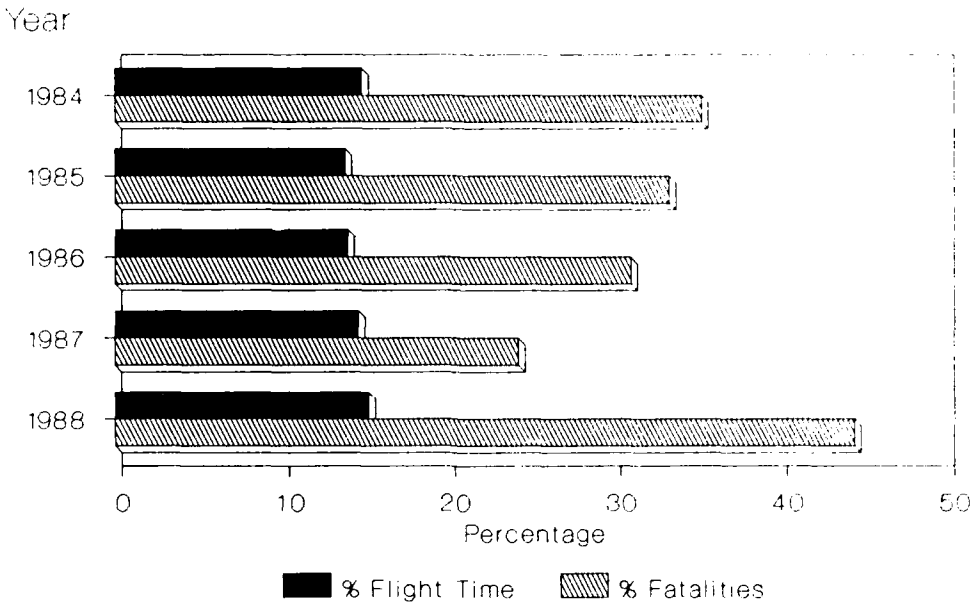
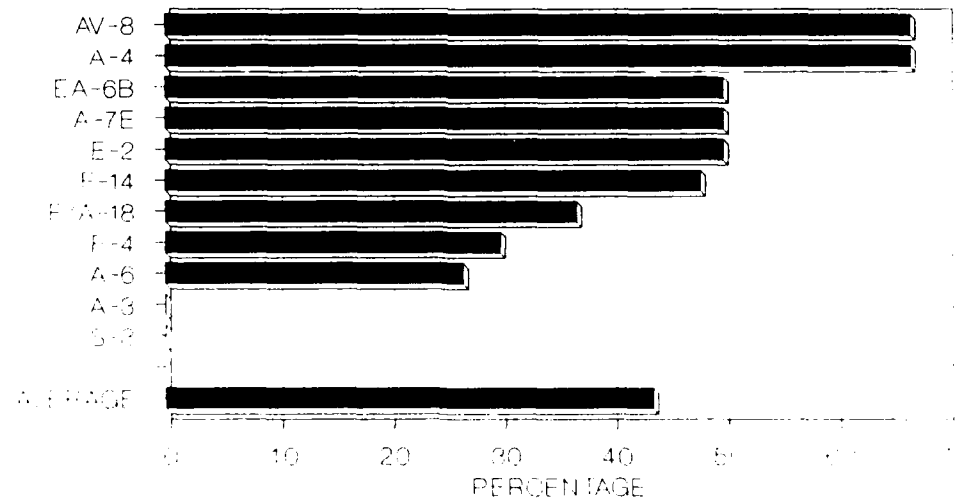


Figure 9

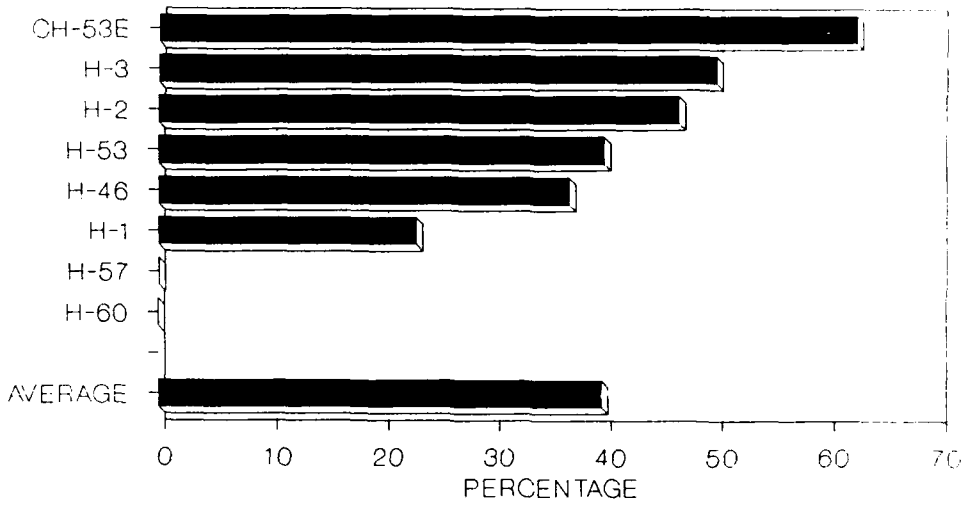
TACAIR CLASS A MISHAPS
% WITH INVOLVED MATERIAL COMPONENT



(May)

Figure 10

ROTARY WING CLASS A MISHAPS
% WITH INVOLVED MATERIAL COMPONENT



CY 84 - CY 88 (May)

Figure 11

TACAIR CLASS A MISHAPS
RANKING BY INVOLVED MATERIAL COMPONENT

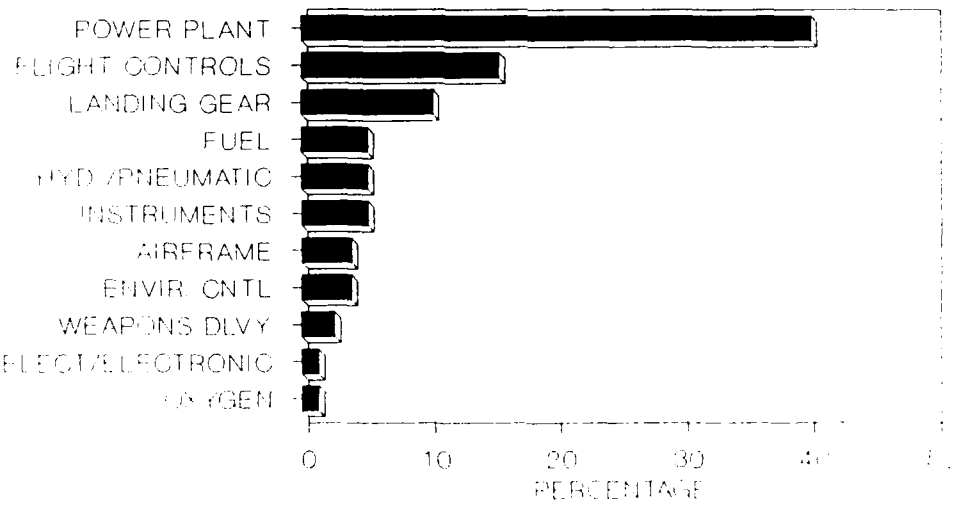
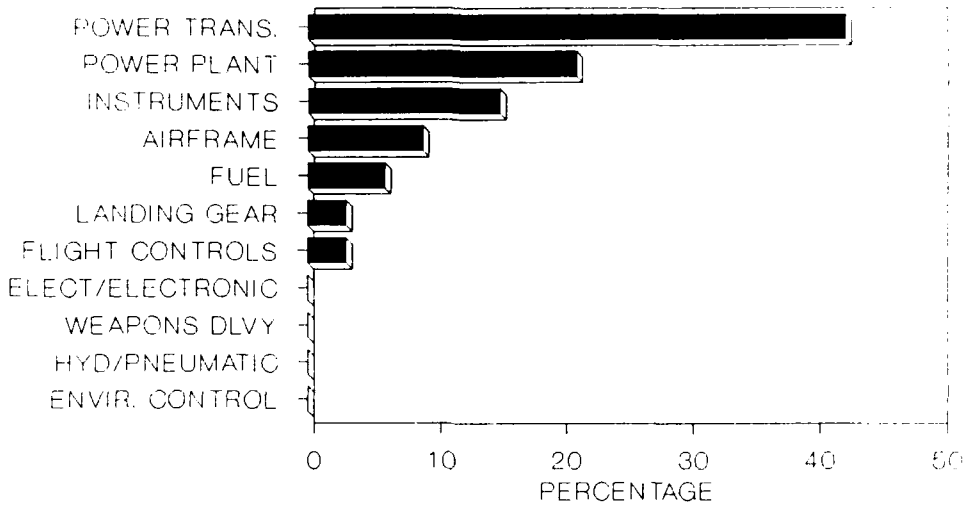


Figure 12

CY 84 - CY 88 (May)

ROTARY WING CLASS A MISHAPS
RANKING BY INVOLVED MATERIAL COMPONENT



CY 84 - CY 88 (MAY)

Figure 13

Class A's are the result of power plant failure/malfunction for TACAIR and power transmissions for rotary wing systems. Powerplants were the number two factor in rotary wing. After establishing a baseline, subsystems in models of aircraft can be compared with the baseline. Figures 14 and 15 show comparisons with the baseline. If a particular subsystem is above an expected norm, additional research is indicated to better understand why and what corrective action is needed.

Aircrew error is difficult to evaluate with existing mishap data storage and retrieval systems. It is possible that a human error baseline could be established using processes similar to those applied to Involved Material Components. That is, a mishap could be caused by the aircrew mismanaging flight controls, landing gear, fuel, etc. Thus, if an aircrew performance baseline is established for a particular aircraft community, deviations from the norm could be detected. The particular reason such as inadequate or improper design, NATOPS, training, utilization, etc., would require further research. Figure 16 shows the most frequent pilot error mishap causal factors. This data is based on existing Naval Safety Center mishap coding and retrieval practices. Aircrew coordination problems and violation of existing procedures are the major contributors to naval aviation mishaps. Unfortunately, this data coding approach does not lend itself to engineering analysis. A possible approach to this end is to view pilot error as mismanagement of major subsystems; i.e., flight controls, engines, weapon control, etc. Figures 17 and 18 show this approach as

applied to the F/A-18 and H-53 aircraft. The baseline used in this measurement is for all Navy/Marine vice TACAIR or Rotary Wing. Unfortunately, the current aviation mishap data must be manually reviewed to obtain pilot error by major system. This procedure provides too great an opportunity for misinterpretation. Advances in the Naval Safety Center SHAIMS (Safety and Hazard Abatement Information Management System) project should allow for easier analysis of human performance data.

Contracting for system safety performance could be achieved by using the IMC baseline for a particular type of aircraft (TACAIR, Rotary Wing, etc.). Thus, a contractual requirement could be imposed such that Class A mishaps due to a particular subsystem (flight controls, landing gear, etc.) shall not exceed the norm for that subsystem. If human performance data is available by subsystem, this could also be imposed. Other factors such as preventi..g TFOA (Things Falling Off Aircraft) could also form part of the contract if a baseline is established. One major problem area is how to handle GFE (Government Furnished Equipment). GFE could be anything from radios to engines. Safety requirements could be imposed on individual vendors for safety critical factors involving quality. If a design factor needs improving, the managing activity and the program office will have to determine if the basic problem is installation sensitive or basic design sensitive. Another approach might be to require the GFE supplier

F/A-18 CLASS A MISHAPS
Ranking By Involved Material Component

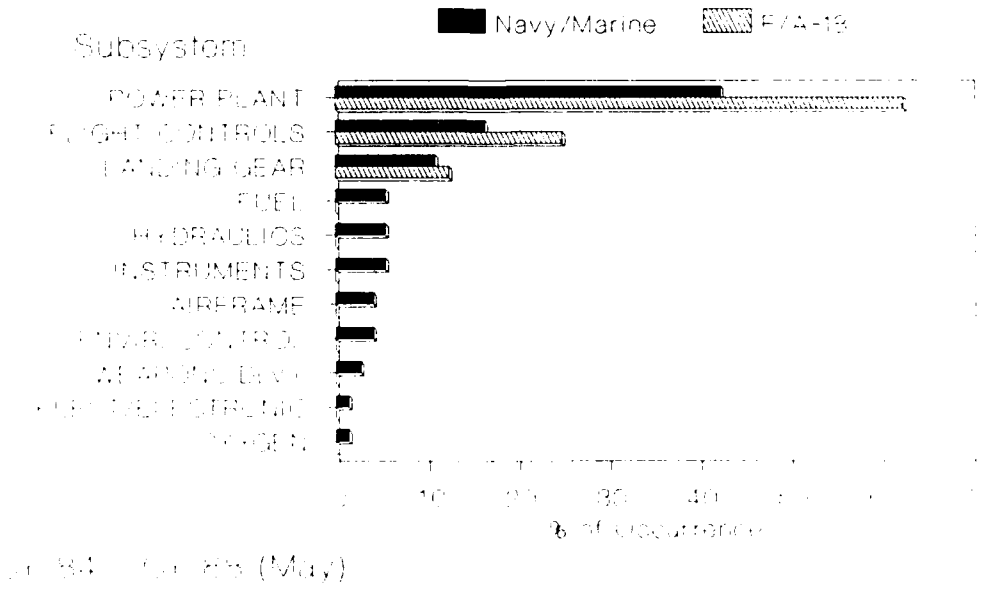
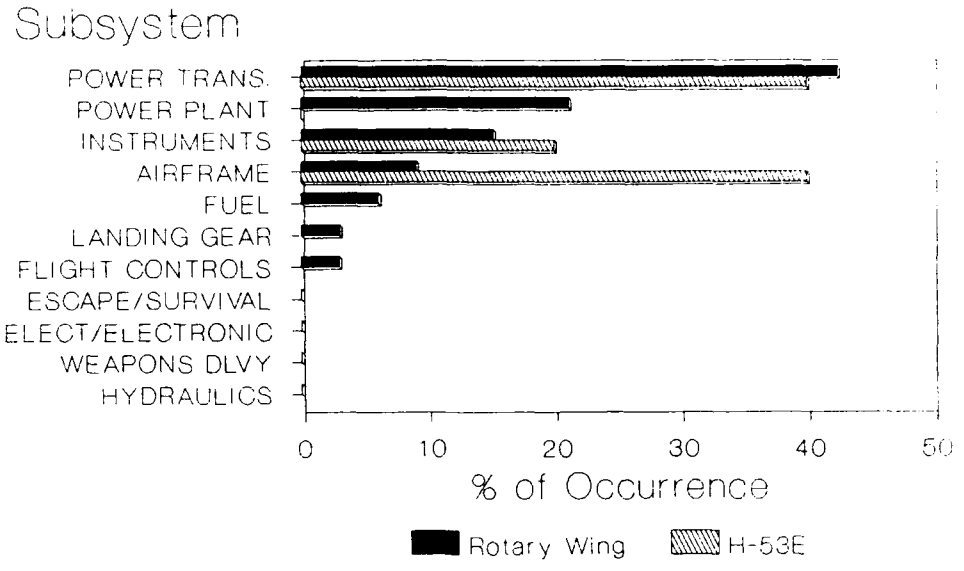


Figure 14

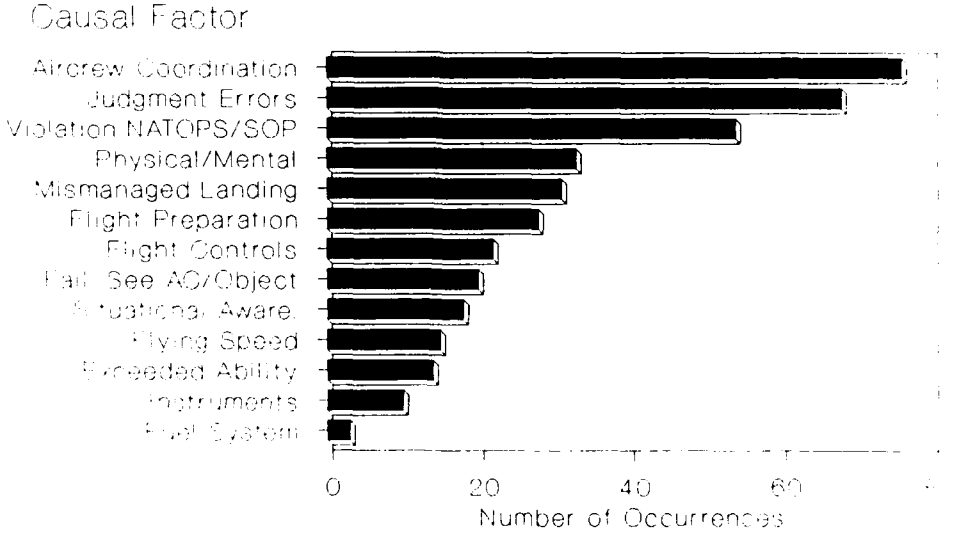
CH-53E CLASS A MISHAPS
Ranking By Involved Material Component



CY 84 - CY 88 (May)

Figure 15

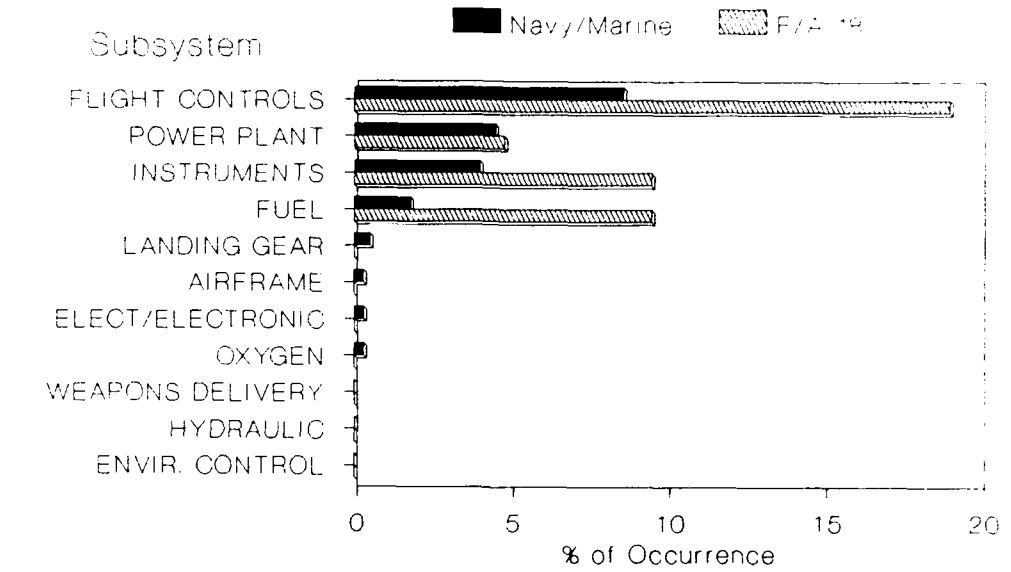
PILOT ERROR CLASS A/B MISHAPS
RANKING BY CAUSAL FACTORS



CY 85 - CY 89 (30 September)

Figure 16

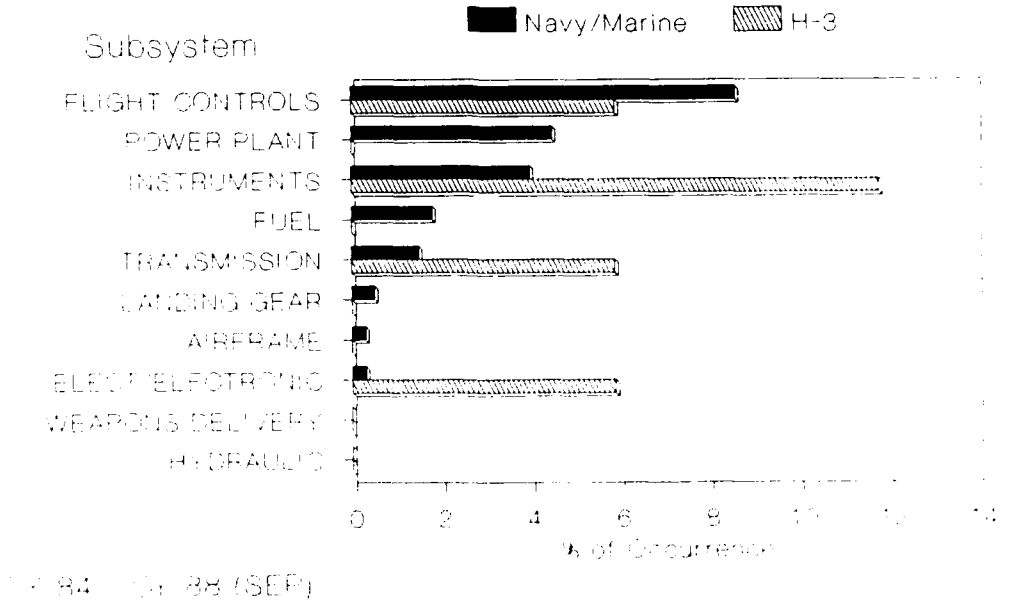
% F/A-18 PILOT ERROR CLASS A MISHAPS
BY SUBSYSTEM VS ALL NAVY/MARINE



CY 84 - CY 88 (SEP)

Figure 17

% H-3 PILOT ERROR CLASS A MISHAPS
BY SUBSYSTEM VS ALL NAVY/MARINE



CY 84 - CY 88 (SEP)

Figure 18

and airframe manufacturer to share responsibility for safety performance. For example, if an engine losses turbine blades, the engine blades should be self-contained. As a backup, safety critical items in the airframe should be located out of the turbine and compressor arcs. The engine compartment should also provide an effective fire containment zone to limit damage and allow a "Get Home" capability. In summary, if one supplier is allowed to point a finger at the other supplier, nothing will be accomplished. They must work together as a team.

8.2 Relative Worth (RW) Index

The Relative Worth (RW) concept is useful for the relative ranking of multiple systems. For example, the Navy operates over 140 different models of aircraft. Loss of certain of these systems would have a far greater impact on readiness, higher potential for multiple fatalities, greater dollar loss, etc. This difference in impact can be handled on a relative basis by using relative worth. Systems with a higher relative worth should receive increased system safety emphasis. When hazards of similar risk occur, the majority of resources should be directed toward correcting the hazard associated with the higher worth system. That is not to say that Category I & II hazards should be ignored for the lower value system. What it could mean is that quality fixes or retrofit actions could be applied to one system and less effective, but less costly, procedural control measures to the other. Relative worth is not strictly based on dollar value or replacement cost. It and airframe manufacturer to share responsibility for safety performance. For example, if an engine losses turbine blades, the engine blades should be self-contained. As a backup, safety critical items in the airframe should be located out of the turbine should be based on a number of factors:

a. Loss of operational capability (M)

b. Potential loss of life (PLL) as a result of a Class A mishap (crew value)

c. Loss of expected service life (ESL)

d. Surplus or shortfall of assets (S)

e. Strike cost or replacement dollar value (D)

The Relative Worth (RW) is determined by assigning weighting factors and Relative Worth (RW) Indices to each of the above categories. The weighting factor and relative worth indices are plugged into a simple mathematical formula. The RW does not give an actual value. Instead, it provides a means of ranking two or more systems by relative importance. RW aids decision making when used in conjunction with other factors such as mishap rate or Risk Assessment Codes. From a command safety manager standpoint, the

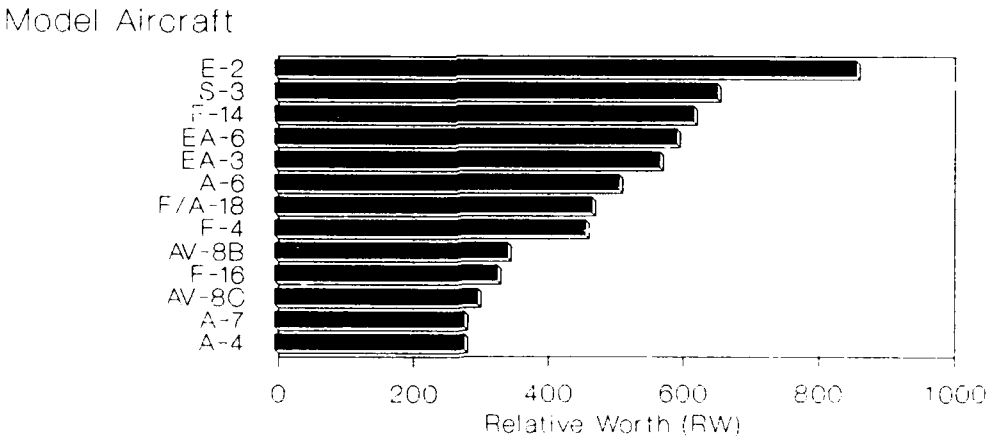
relative worth could be established for each type of aircraft (F/A-18A, etc.) or other assigned systems. The major consideration is to have command directors and safety managers agree on common factors. Unless a command establishes uniform ground rules, the results for this technique would, at best, be suspect.

Examples of weighting factors and Relative Worth Indices (RWI) are provided in Appendices A - E. The RW is determined by assigning the appropriate weighting factor (relative worth indices) from each of the tables. Then, the weighting factors are multiplied together to give the relative worth (RW).

$$RW = W_m*M + W_l*PLL + W_e*ESL + W_s*S + W_d*D$$

Figures 19 and 20 are examples of a relative worth ranking for TACAIR and Rotary Wing. It must be remembered that this system is highly subjective. However, if the ground rules are uniformly applied, the result will be a consistent ranking. The weighting factors are slanted heavily toward potential fatalities. Therefore, transport helicopters are ranked high due to the greater potential for multiple loss of life. RWI should help to direct design improvement factors such as crashworthiness features, improved NAVAIDs, Ground Collision Avoidance Systems, and Maintenance Monitors.

RELATIVE WORTH RANKING
TACTICAL AIRCRAFT



RW reflects magnitude of risk from an aircraft loss

Figure 19

APPENDIX A

LOSS OF OPERATIONAL CAPABILITY (M)

WEIGHTING FACTOR (W_m) = 30

BASIC MISSION	RELATIVE WORTH INDICES (M) **
Attack (A)	
Light Attack	5
Medium Attack (all weather)	8
Transport (C)	
Carrier On-Deck Delivery (COD)	5
Heavy Transport	5
Medium Transport	5
Special Electronics Installation (E)	
Airborne Early Warning Radar	10
Electronic Countermeasures	6
Airborne Command and Control	10
Tactical Data Communications Link	5
Fighter (F)	
Air Superiority	10
Interdiction & Close Air Support	8
Observation (O)	5
Patrol	8
Reconnaissance (R)	5
Antisubmarine (S)	8
Trainer (T)	5
Utility (U)	5
Research (X)	5

** Aircraft which provide a self protect or defensive capability are given the highest ranking (10).

APPENDIX A

LOSS OF OPERATIONAL CAPABILITY (M)

WEIGHTING FACTOR (W_m) = 30

BASIC MISSION	RELATIVE WORTH INDICES (M) **
Attack (A)	
Light Attack	5
Medium Attack (all weather)	8
Transport (C)	
Carrier On-Deck Delivery (COD)	5
Heavy Transport	5
Medium Transport	5
Special Electronics Installation (E)	
Airborne Early Warning Radar	10
Electronic Countermeasures	6
Airborne Command and Control	10
Tactical Data Communications Link	5
Fighter (F)	
Air Superiority	10
Interdiction & Close Air Support	8
Observation (O)	5
Patrol	8
Reconnaissance (R)	5
Antisubmarine (S)	8
Trainer (T)	5
Utility (U)	5
Research (X)	5

** Aircraft which provide a self protect or defensive capability are given the highest ranking (10).

APPENDIX B

POTENTIAL LOSS OF LIFE (PLL)

WEIGHTING FACTOR (W_1) = 30

MAXIMUM POSSIBLE LOSS OF AIRCREW LIFE (EXCLUDING SPECIAL CIRCUMSTANCES) (PLL)	RELATIVE WORTH INDICES
More than 10 lives	20
More than 5 lives	10
3 to 5 lives	8
2 lives	5
1 lives	2

APPENDIX C

DOLLAR VALUE (D)

WEIGHTING FACTOR (W_d) = 15

STRIKE COST (NOW DOLLARS)	RELATIVE WORTH INDICES (D)
More than $30M	10
More than $25M & less than $30M	8
More than $20M & less than $25M	6
More than $15M & less than $20M	5
More than $10M & less than $15M	4
More than $5M & less than $10M	3
$5M or less	2

APPENDIX D

EXPECTED SERVICE LIFE (ESL)

WEIGHTING FACTOR (W_e) = 10

Expected Service Life	Relative Worth Indices
20 years	10
15-20 years	8
10-15 years	6
5-10 years	4
1-5 years	2

APPENDIX E

SHORTFALL OF ASSETS (S)

WEIGHTING FACTOR (W_S) = 10 Shortfall	Relative Worth (S)
More than 20% shortfall	10
More than 15% and less than 20%	8
More than 10% and less than 15%	6
More than 5% and less than 10%	4
Less than 5%	2