AD-A052 384 DEFENSE SYSTEMS MANAGEMENT COLL FORT BELVOIR VA F/G 13/12
A GUIDE TO DOD SYSTEM SAFETY PROCESSES AND ORGANIZATIONS.(U)
NOV 77 J E HORMUTH

UNCLASSIFIED NL

| OF |
AD
AD52384

END
DATE
FILMED
5-78
DDC

1

DEFENSE SYSTEMS MANAGEMENT COLLEGE

PROGRAM MANAGEMENT COURSE
INDIVIDUAL STUDY PROGRAM

A GUIDE TO DOD SYSTEM SAFETY
PROCESSES AND ORGANIZATIONS

STUDY PROJECT REPORT
PMC 77-2

John E. Hormuth
Major USAF

FORT BELVOIR, VIRGINIA 22060

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE *(and Subtitle)* A GUIDE TO DOD SYSTEM SAFETY PROCESSES AND ORGANIZATIONS		5. TYPE OF REPORT & PERIOD COVERED Study Project Report 77-2 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) JOHN E. HORMUTH		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS DEFENSE SYSTEMS MANAGEMENT COLLEGE FT. BELVOIR, VA 22060		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS DEFENSE SYSTEMS MANAGEMENT COLLEGE FT. BELVOIR, VA 22060		12. REPORT DATE 1977-2 13. NUMBER OF PAGES 59
14. MONITORING AGENCY NAME & ADDRESS*(if different from Controlling Office)*		15. SECURITY CLASS. *(of this report)* UNCLASSIFIED 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT *(of this Report)*

UNLIMITED

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

17. DISTRIBUTION STATEMENT *(of the abstract entered in Block 20, if different from Report)*

18. SUPPLEMENTARY NOTES

19. KEY WORDS *(Continue on reverse side if necessary and identify by block number)*

SEE ATTACHED SHEET

20. ABSTRACT *(Continue on reverse side if necessary and identify by block number)*

SEE ATTACHED SHEET

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

DEFENSE SYSTEMS MANAGEMENT COLLEGE

STUDY TITLE: A GUIDE TO DOD SYSTEM SAFETY PROCESSES AND ORGANIZATIONS

STUDY PROJECT GOALS:

To introduce acquisition program office personnel to the terminology, techniques and organizations for System Safety in the DOD.

STUDY REPORT ABSTRACT:

This report is written to provide DOD system acquisition personnel with an overview of the System Safety function. It assumes no prior knowledge of the subject.

This study introduces the language of System Safety and describes some of the more common System Safety analyses types and techniques used in the acquisition process.

Using this information as background, a System Safety program is traced through the acquisition cycle. The roles and functions of System Safety personnel in relation to other program functions are outlined for a typical program.

To aid personnel new to the acquisition business, the organization and functions of System Safety are described for the major Army, Air Force and Navy acquisition organizations.

SUBJECT DESCRIPTOR: System Safety (10.05.06.04)

NAME, RANK, SERVICE	CLASS	DATE
John E. Hormuth, Major, USAF	PMC 77-2	November 1977

A GUIDE TO DOD SYSTEM SAFETY PROCESSES AND ORGANIZATIONS

Individual Study Program

Study Project Report

Prepared as a Formal Report

Defense Systems Management College

Program Management Course

Class 77-2

by

John E. Hormuth
Major USAF

November 1977

Study Project Advisor
CDR Jerry Chasko, USN

EXECUTIVE SUMMARY

System Safety is the function which strives to obtain the optimum degree of safety within the constraints of operational effectiveness, time and cost through specific application of System Safety management and engineering principles whereby hazards are identified and risk minimized throughout all phases of the system life cycle (4:3)[1]. The requirement that System Safety be considered in all research, development and acquisition programs stems from guidance given in DODD 1000.3 (1).

To assist the Program Manager in understanding his System Safety program this report presents and discusses System Safety terminology, techniques and functions as used in a typical acquisition process. It also outlines the key elements of DOD and service System Safety organizations which a Program Manager may call upon for assistance on his program.

The information presented in this paper reflects the author's experience as the System Safety Engineer on the Advanced Airborne Command Post (E-4) project and as the System Safety Officer on the Advanced Tanker/Cargo Aircraft (ATCA) project plus a composite of the information gathered in some 18 interviews (Appendix A) with System Safety personnel from the DOD and each of the services.

---

[1] This notation will be used throughout the report for major references. The first number is the source listed in the bibliography; the second number is the page. General references have only one number which indicates the document. Superscripts refer to the Footnotes on Page VI-1.

TABLE OF CONTENTS

LIST OF TABLES

SECTION I

INTRODUCTION

Purpose of the Study Project

The primary purpose of this study project is to acquaint the Program Manager with the language, functions, techniques and products of System Safety and how it interfaces with other program elements during the acquisition life cycle. A guide to the services' System Safety organizations is also provided.

Specific Goals of the Project

A successful Program Manager must make decisions in many areas which impact on his program without having specific expertise in the area itself. To do this he must have some knowledge of the language of the discipline and sufficient understanding of the techniques employed to ask the proper questions concerning the discipline's utility in his acquisition program. This study project will attempt to assist the Program Manager to achieve such knowledge and understanding of System Safety.

Scope of the Study Project

During the life cycle of a program, environmental and occupational safety, nuclear safety and System Safety must all be addressed. Usually different organizational groups operating with somewhat different but related goals handle these three aspects of safety. To address all three areas of safety

would be beyond the scope of this paper, therefore, this study will include only the System Safety tasks as directed in DODD 1000.3 and detailed in MIL-STD-882A.

SECTION II

THE SYSTEM SAFETY PROCESS

Introduction

To say that a system is safe is to say that it is free from those conditions that can cause death, injury, occupational illness or damage to or loss of equipment or property (4:2). Obviously, by this definition, no system that performs any function can be designed to be absolutely "safe". Therefore, safety becomes a relative term. This means that the objective of a safety program becomes one of identifying hazards where the combination of the consequences and the frequency of the undesired event is unacceptable to the user or to the environment in which the system is to be operated.

This sytem will identify and briefly explain some of the tools and techniques that are used in the System Safety discipline to identify, analyze and quantify such hazards.

Definitions

The following definitions are basic to understanding System Safety concepts (4:2-3):

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

b. Risk - An expression of possible loss in terms of hazard severity and hazard probability.

c. Hazard - An existing or potential condition thatcan result in a mishap (e.g., the presence of fuel in an undesired location is a hazard whereas the fuel itself is not).

d. Hazard probability - The likelihood, expressed in quantitative or qualitative terms, that a hazard will occur.

e. Hazard severity - A qualitative assessment of the worst potential consequence, defined by the degree of injury, occupational illness, property damage, or equipment damage that could ultimately occur.

Tables 1, 2 and 3 contain additional definitions of hazard classifications, hazard probabilities and risk levels.

Table 1

Hazard Classifications (4:11)

Category	Descriptive Word	Effect
I	Catastrophic	May cause death or system loss.
II	Critical	May cause severe injury, severe occupational illness, or major system damage.
III	Marginal	May cause minor injury, minor occupational illness, or minor system damage.
IV	Negligible	Will not result in injury, occupational illness, or system damage.

Table 2

Hazard Probabilities (4:12)[1]

Descriptive Word	Level	Specific Individual Item	Fleet or Inventory
Frequent	A	Likely to occur frequently	Continuously experienced
Reasonably 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	So unlikely, it can be assumed that this hazard will not be experienced	Unlikely to occur but possible
Extremely Improbable	E	Probability of occurrence cannot be distinguished from zero	So unlikely, it can be assumed that this hazard will not be experienced
Impossible	F	Physically impossible to occur	Physically impossible to occur

Table 3

Risk Levels

Hazard Category	Largest Acceptable Probability Undesired Event Taking Place*
I Catastrophic	10^{-6}
II Critical	10^{-5}
III Marginal	10^{-2}
IV Negligible	1

Some maximum allowable hazard probabilities for certain hazard classifications are specified by each service. [2,3]

*Failures per hour for continously operating systems (e.g., a radio) and per operation for discretely operating systems (e.g., a switch).

Analyses Types

There are many hazard analysis techniques available for use ranging from qualitative techniques which may be no more than "wild guesses" to sophisticated techniques which yield precise quantified risk data. The technique chosen is a function of two things:

a. The intended use of the information.

b. The resources and data available to develop and use the appropriate technique or model.

Normally, during the acquisition cycle, initial analyses are qualitative. Then, as the system design becomes more definitized, they are quantified.

The following analyses are those most commonly performed during the system acquisition process.

Preliminary Hazard Analysis (PHA) - A PHA is a qualitative technique normally performed early in an acquisition process to identify safety-critical areas, evaluate hazards and identify the safety design critera to be used. To the extent possible, the following information is developed (25:6-6):

a. A description of the system, subsystem or component.

b. A description of the hazard.

c. The effect of the hazard on other components and the system as a whole.

d. The hazard classification (Table 1).

e. Recommended action to eliminate or control the hazard.

f. Probability of occurrence (Table 2). May be qualitative early in a program. Critical items will be quantified as data become available.

The PHA is the framework for the whole System Safety Program. It identifies areas of concern where major system development effort may need to be focused.

Some representative PHA entries are shown in Table 4.

Subsystem Hazard Analysis (SSHA) - An SSHA (4:14) is performed to identify hazards associated with the actual or proposed design of a subsystem. The failure modes of components and the interactions of failed components within the subsystem with other unfailed or failed components are examined to determine types and frequencies of hazards. An SSHA may be either qualitative or quantitative depending on the detail of design available and on the planned use of the analysis. On simple systems an update of the PHA may be adequate.

Typical SSHA entries are shown in Table 5.

System Hazard Analysis (SHA) - An SHA (4:14) is performed to identify hazards introduced through the integration of subsystems into a system. This includes, not only identifying failures of individual subsystems and determining the effects on other subsystems, but also determining hazardous effects induced in the system and other subsystems by a properly working subsystem. An SHA may be either qualitative or quantitative depending on its purpose and on the level of detail available on the system/subsystems.

Typical SHA entries are shown in Table 6.

Operating and Support Hazard Analysis (O/SHA) - An O/SHA (4:15) identifies hazards to personnel and equipment associated with operation, maintenance, testing, modification, transportation, storage, egress, rescue, training and disposal

TABLE 4

Typical PHA Entries

Item Nomenclature	Operation and/or Energy Source	Undesired Event	Triggering Event	Effects	Probability	Hazard Category	Recommended Control	Amplifying Remarks
Hydraulic Pump	Normal	Leaking Seals	Age	Hydraulic Fluid in Wrong Area. Possible Fire.	Unknown	III	Periodic inspection or Non-Flammable Fluid.	
Bomb Production Melt/Pour Operations	Melting Explosives	Explosives Temperature of 176° F	a. Operator sets steam pressure above 10 psi b. Steam pressure fails allowing pressure to exceed 10 psi.	TNT Separation during pouring operation.	a. Medium b. Unknown	I I	a. Automatic control system with fail safe control b. Operator control limit to less than 10 psi.	Provide criticality inspection point for explosives separation.
Shipboard Weapon Warhead Explosive	a. Shock b. Heat	a. Cracking, Powerizing b. Melting, Exudation	a. Drop While Loading b. Fire	a&b. Detonation, deflagration, burning of explosive prior to safe separation from launch vessel.	a. Low b. 10^{-3}	I	Qualify explosive for service application. Use only approved explosives for intended application.	Use of sensitive primary explosives is forbidden. Use of secondary (Booster) Explosives for main charge applications is highly hazardous.

TABLE 4

Typical PHA Entries

Item Nomenclature	Operation and/or Energy Source	Undesired Event	Triggering Event	Effects	Probability	Hazard Category	Recommended Control	Amplifying Remarks
Aircraft Liquid Oxygen (LOX) System	Landing and Take Off	Leakage of LOX resulting from Nose Gear Collapse	Failure of Nose Gear	Rupture of LOX Container or Lines	Low	III	Do not place LOX system in lower forward Cargo area.	LOX system & lines should not be installed where may be ruptured during minor accident such as nose gear collapse.
Artillery Shells	Transporation & Storage; Manufacturing facility to Army	Detonation of Round	a. Fire b. Drop	Destruction of Round	a. Low b. Unknown	I I	a&b. Mark vehicles with warning/hazard placards. a. Design round to permit burning of explosive filler. a. Design packaging of noncombustible material. b. Conduct drop tests.	Rail/Truck accidents have high incidence of associated fire environment. Loading & unloading functions have greatest incidence of drop events.

TABLE 5

Typical SSHA Entries

Hazardous Element	Hazard Event	Hazard Condition (Exposure)	Triggering Event	Accident/Incident Description	Hazardous Event Effects	Hazard Category	Recommended Corrective Action/ Remarks
Refueling Boom	Hook-up with Receiver	Receiver exposed to boom strike	a. Operator error. b. False boom extension	a&b. Boom strikes receiver aircraft.	Structural damage to receiver aircraft. Possible broken canopy.	II, III I, II	a. Ensure training standards & crew operating procedures met. b. Redundant command channels.
Shipboard Missile Launcher Elevation Subsystem	Raising or lowering missile	Personnel exposed to gears.	Raise or lower missile	Personnel caught in gears	Injury or death to personnel	II	Guard gears.
Rack mounted equipment, mobile communications center	Servicing equipment	No bumper stops or extension locks on on equipment.	Pulling equipment out of rack.	Equipment falls from rack.	Injury to personnel.	III	Install bumper stops so equipment will not fall from rack when partially pulled out for servicing
Landing Gear	Inadvertent Gear Retraction	Gear retracted while aircraft on ground	Gear retraction handle activated	Gear retracts	Damage to aircraft	II, III	Place sensing switch on gear to deactivate handle while aircraft on ground.
Tank Engine	Tank engine noise	Crew exposure to excess noise	Tank operation	Crew has prolonged exposure to excessive engine noise.	Permanent hearing impairment.	III	Increase accoustic shielding & individual crew ear protection.

TABLE 6

Typical SHA Entries

Hazardous Element	Hazard Event	Hazard Condition (Exposure)	Triggering Event	Accident/Incident Description	Hazardous Event Effects	Hazard Category	Recommended Corrective Action/ Remarks
Bomb	Transfer of bombs from cart to final preparation table.	a. Bomb exposed to 5 ft drop while explosve is molten. b. Operator exposed to falling bomb.	Hoist fails or operator fails to properly attach hoist to bomb.	a. Bomb falls to floor. b. Operator struck by bomb	a. Detonation or deflagration of bomb. b. Disabling injury	I III	Redesign hoist.
Ship Gun Turret	Turret travel beyond safe angle	Narrow Personnel Clearance	Operator inattention to turret travel	Personnel trapped in narrow space	Death or severe injury	I, II	Install mechanical stops to prevent excess turret travel.
Wing Fuel Tanks	Static Discharge in fuel cells	Fuel-air mixture exposed to static discharge	Lightning strike	Fuel-air mixture explodes	Aircraft lost. Crew probably lost.	I	Install adequate grounding system or nitrogen inerting system in fuel cells.
Portable Bridge	Extension of Bridge	Vehicle unstable when bridge in pre-extend position	Bridge moves from stowed to pre-extend postion	Vehicle Overturns	Vehicle Damaged. Personnel Injured.	II	Stabilize vehicle before bridge deployment.

during all phases of acquisition, operation and disposal of the system. It must take into account human errors possible when various operational and maintenance tasks are being performed. An O/SHA can result in safety precautions, procedures, warnings and placards being included in maintenance and operating manuals and on the equipment. An O/SHA is usually partially qualitative and partially quantitative.

Sample O/SHA entries are shown in Table 7.

Accident Risk Assessment (17:7-1) - When the Government or the contractor chooses a particular design alternative over another there is the implicit willingness to accept certain operational or performance restrictions in order to avoid an accident. An Accident Risk Assessment evaluates the risk being assumed during test or operation by defining the design and operating limits imposed on each system element to preclude an accident or mishaps and the consequences of design or operation outside those limits. With this information a Program Manager can decide whether to accept or reject the risk by making appropriate design/operation limit decisions.

A typical Accident Risk Assessment is shown in Table 8.

Safety Statement (25:8-19) - Prior to release to the Government of a system for testing, the contractor provides safety information to the testing organization either by participating in Safety Review Board activities or by providing a Safety Statement. Concentration is on inapparent or ill-defined hazards, reactions or by-products which may be injurious to operating, maintenance or test personnel.

TABLE 7

Typical O/SHA Entries

Work Station	Function	Operation	Effect		Hazard Category	Safety Features Recommended Control	Recommendations and/or Remarks
			Normal	Hazard			
Flight Engineer Station	Oxygen Control Switch	Turn Oxygen Control Switch to desired setting.	Provides either normal or 100% oxygen flow	Switch located below table top so operator cannot see setting. May select normal when 100% required.	II	Relocate oxygen control switch to flight engineers panel	
FPQ-XX Radar Control Room	Antenna Activation	Activate Radar Traverse Switch	Radar turns on pedestal	Personnel on pedestal may be injured by moving equipment	II	Provide horn and light to warn personnel that equipment to be operated	A system similar to that used on the FXZ-13 radar is recommended.
X-14 Test Equipment	Electric Curcuit Continuity Check	Connect two Test Cables to Proper Terminals	Provides continuity Check	If cables reversed operator may receive shock and equipment damaged	III	Color code the tester cables so they are less likely to be reversed	Best solution to use different connectors on each cable. Would require mod of the entire fleet.
Work Stand Anti-Tank Vehicle	Facilitate Access to TOW Hardware	Placed on Left Side of Vehicle	Provides Correct Work Height	Personnel may fall from stand while working on equipment.	III	Use larger stand or a stand with a safety rail on three sides	Such a stand is in the Navy inventory for use on the A-7 Aircraft.

TABLE 8

Sample Accident Risk Assessment*

Flight Test - Modified Aerial Refueling Boom

Ref: XYZ Co. Drawings 76-347-B and 76-348-B.

Test Description: Modified Boom installed on 4950th Test Wing KC-135 (62-346) for purpose of determining compatibility with following receivers B-52, C-5, F-15 and A-10. No actual hook-ups will be made. Boom will be dry. Receiver aircraft will fly in contact position while boom is maneuvered to simulate hookup.

Identified Potential Hazards:

a. At speeds greater than 325 KEAS the boom is subject to flutter when deployed to its full length (XYZ Report 76-107).

b. At speeds below 190 KEAS the boom loses aerodynamic stability when deployed (XYZ Tech Note 76-3).

Since this boom is to be used for test purposes only, no changes are anticipated. Hazards will be controlled by restricting the flight envelope (boom deployed) to 200-315 KEAS with no receiver and 210-305 KEAS with a receiver. Further flights with the boom deployed will be restricted to test zones C-2 and C-3 and must be accompanied by a chase plane. The boom operator's manual and the pilot's partial flight manual will contain warnings and the appropriate flight restrictions. Should any irregularity occur during compatibility testing, the boom operator's manual indicates that a "breakaway" shall be called.

No unacceptable hazard to the KC-135 or its crew is anticipated should the boom flutter, lose stability or separate from the aircraft (XYZ Report 76-107).

XYZ Company Report 76-107 indicates that there are no other hazards not usually associated with an aerial refueling mission.

---

* /The system listed is hypothetical. It does not represent an actual system. This report is a summary - an actual report would be longer and more detailed. This sample is meant to illustrate the technique.

Some of the techniques which are used to prepare these analyses types are discussed below. More details on these analyses types may be found in references 6, 25 and 38.

Analysis Techniques

The results of any analysis can be no better than the data and models which are used to prepare them. A quantitative model cannot produce precise answers from imprecise or wrong data. Thus, when a quantitative analysis is prepared it should be accompanied by a statement of the accuracy of the input data, the validity of the model used to manipulate the data, the assumptions made and the relative accuracy of the output from the model.

Likewise, qualitative analyses should be examined to determine whether they considered all possible modes of failure and hazardous consequences.

Both quantitative and qualitative analyses must be continually updated to reflect the latest system design.

There are many analyses techniques. Some of the more commonly used are briefly explained below.

Failure Mode and Effect Analysis (FMEA) (25:6-9) - An FMEA is a qualitative technique using as its basis the reliability FMEA. However, instead of focusing on successful operation of the system, a safety FEMA evaluates the effects of various failure modes on the safety of the system. Data examined for the failed component include all of its failure modes, the effects on other components and the system, a hazard category and relative frequency (Tables 1, 2 and 3) and remarks on preventing or

controlling the undesired effect. FEMA's are often performed to support SHA's and SSHA's (see FMECA below).

Failure Mode, Effects and Criticality Analysis (FMECA) (25:6-13) - An FMECA is a quantitative expansion of an FMEA. As information becomes available specific failure rates are applied to components. FMECA's are often used to support an SHA or SSHA in evaluating the safety effects of piece part selection.

Typical FMECA data are shown in Table 9.

Fault Tree Analysis (FTA) (38C:7-66) - A FTA looks at undesired events rather than system failures. An undesired event, e.g., fire in a weapon storage area, is selected and then the analysis proceeds through the system to identify the event or chain of events that must occur for the undesired event to occur. Outputs of particular concern are critical paths containing only one event or paths containing events with relatively high frequencies of occurrence. These paths could become prime candidates for designing out of a system. A FTA analysis, because of the amount of detail required, is often expensive and time consuming, particularly on a complex system. For this reason care must be taken to select only the most critical systems/subsystems for analysis.

Symbols and a portion of a typical Fault Tree Analysis are shown in Table 10.

Fault Hazard Analysis (FHA) (38C:7-56) - An FHA considers component, subassembly or subsystem failures or design deficiencies. It goes beyond the FMEA and FMECA in that it considers

TABLE 9

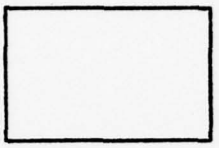
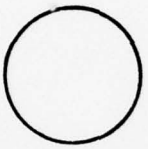
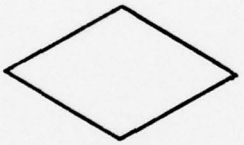
Typical FMECA Data

Equipment Component	Function	Failure Mode	Possible Cause	Failure Effects		Criticality		Recommendations and/or Remarks
				Local	System	Failure Probability	Hazard Category	
Inertial Navigation System (INS)	Provide Position Update for Aircraft	Excessive Drift Rate	Electronic Component Failure	Error in Aircraft position	Bad targeting update information for SRAM air-ground missile. Possible impact out of test area.	10^{-4}	IV	Install dual INS.
5" MK36 Bomb	Fuse Removal	Detonation	a. Friction of base on explosive during base fuse removal. b. Adaptor assembly and cavity not staked sufficiently during nose fuse removal.	a&b. Detonation of weapon	a&b. Death or injury to arming personnel	a. $3x10^{-5}$ b. 10^{-4}	I I	a. Operations to be conducted in accordance with local operating instructions. b. 1. Nose fuses to be removed remotely. 2. Adaptor inserted. 3. Adaptor restaked.
Directional Finding (DF) Equipment at airfield	Provide relative bearing for aircraft.	Short in transmitter/ receiver	Corrosion in transmitter/ receiver section	Inability to determine relative bearing for aircraft	Excessive noise in UHF radios preventing ground-air communications	$5x10^{-4}$	II	If excessive noise occurs in UHF radios cycle DF off to see if problem disappears.
Incoming fire detection system	Provide position source data on incoming artillery & mortar fire	Bad position data	Bad computer output data	Failure to accurately determine incoming fire source	Possible strikes against friendly forces due to bad position data	$6x10^{-3}$	I	Built in self check in computer

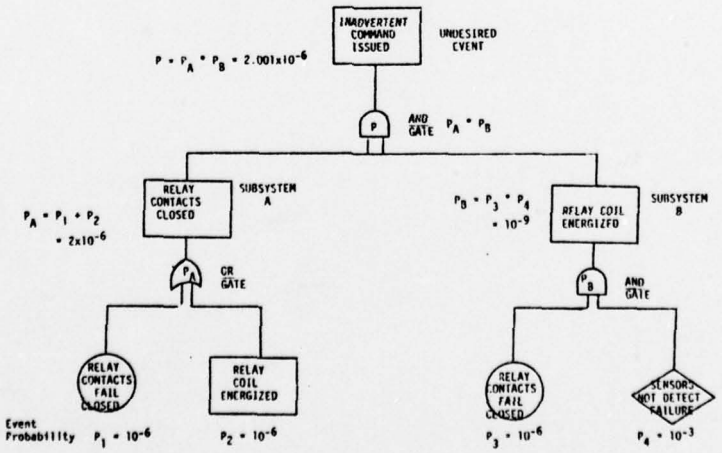
TABLE 10

Fault Tree Analysis

Symbols

Common Symbols		Used To Represent
Rectangle		1. Top Undesired Event. 2. Command Event.
Circle		1. Basic fault event. Probability of Occurrence derived from generic rate of the component. 2. An input or independent event.
House		An event that must occur due to normal operating conditions in the system. Not a fault event. Probability is the reliability of the component.
Diamond		Secondary fault event. Occurs outside of design, e.g., high winds, water damage.
<u>And</u> Gate		Coexistence of <u>all</u> input events is required to produce the output event.
<u>Or</u> Gate		Situation exists if one of more of the input events exist.

FTA Example



human error, procedural deficiencies, abnormal environments and other components that may cause normal operation at undesired times if such operation would then create a hazard. An FHA is often done to support an O/SHA.

Typical FHA entries are shown in Table 11.

There are numerous other specialized hazard analyses which may be performed. A few are listed below. Details of these and other techniques may be found in references 25 and 38.

Sneak Circuit Analysis - Computer aided technique for examining software and hardware to identify latent (sneak) circuits and conditions that inhibit desired functions or cause undesired functions to occur without a component having failed.

Energy Transfer Analysis - A series of probability computations to determine how various energy inputs to the system will react during a catastrophic accident.

Safety Check List Analysis (SCLA) - Uses checklists derived from established design practices, safety requirments and constraints to identify common hazards associated with poor design practice. In some cases these checklists have been formalized for common systems, e.g., AFSC Design Handbook 1-X (15). Other organizations have developed checklists peculiar to their own needs.

Maintenance Hazard Analysis (MHA) - Determines hazards inherent in or introduced by maintenance procedures, equipment or substances.

Radiation Hazard Analysis (RADHAZ) - Examines areas where electromagnetic and ionizing radiations present hazards to

TABLE 11

Typical Fault Hazards Analysis Entries

Item Component	Hazard	Undesired Event	Conditions Necessary: Item Fault State	Conditions Necessary: Energy Source	Hazard Category	Possible Energy Sources in Environment	Recommendations and/or Remarks
5" MK 36	Blast Fragmentation	a. Exposure of operators to detonation of round during base fuse removal	a&b. Sensitive ammonium picrate compound present at base fuse	a. Friction on base of explosive	I	Fuse removal Operations	Operations to be conducted remotely in cell in accord with operating instructions
		b. Detonation of round during nose fuse removal		b. Adaptor assembly and cavity not staked sufficiently	I	Torque Wrench Removal of Nose Fuse	1. Nose fuses to be removed remotely. 2. Adapter reseated. 3. Adapter Restaked.
Aircraft Engine	Dropped Engine	a. Exposure of personnel to Falling Engine b. Damage to Engine due to Fall	Engine falls from Lifting Device	a&b. Failure of Lifting Device or of personnel to follow proper procedures	a. I b. II	a&b. Movement of Engine from stand to pylon	Verify adequacy of Lifting Device via System Test. Ensure Only Qualified Personnel Participate on Installation Team
Parachute	Excessive Descent Rate	Exposure of personnel to parachutes which fail to deploy or Improperly deploy	a. Parachute fails to deploy	a. D-Ring or ripcord failure	a&b. I (IV if reserve parachute deploys successfully)	a. Deployment Procedure	a. Visual Inspection During Rigging.
			b. Parachute Deploys Improperly	b. Improper Rigging		b. Rigging Procedure	b. Follow Training and Inspection Procedure per unit regulations.
Anti-Submarine Mine	High Energy Projectile	Exposure of crew to inadvertant deployment	a. Deployment ejection device failure to operate	a. Failure of Propelling device	III	a. Improper or Incomplete inspection	a&b. Ensure training for inspections, repair & operations meets required standards.
			b. Inadvertant Operation	b. Inadvertant Deployment signal		b. Faulty operational Procedure	

personnel.

All of the above analyses techniques are only tools for the decision-maker. They do not provide final answers, but rather allow the decision-maker to become aware of consequences of design and performance choices.

The worth of any safety analysis is in its timeliness and appropriateness to the situation. These factors are discussed in more detail in Section III.

The formats of the tables in this Section were chosen from reference 38. There are any number of formats, the appropriate format being the one which displays the information desired for a particular project.

SECTION III

SYSTEM SAFETY IN THE ACQUISITION PROCESS

Introduction

System Safety - the elimination or control to an acceptable level of hazards throughout the entire life cycle of a system in a timely and cost effective manner - is an integral part of every acquisition process. Although the basic elements of most System Safety programs are the same, the details will be determined by the type of system being acquired, the method of acquisition, and the competence of the contractor as well as the amount and type of System Safety resources available to the Program Manager. For these reasons the System Safety tasks, functions and organizations described in this Section should be taken as a generic description of a System Safety effort.

It should be emphasized that System Safety is not a discipline that stands alone. It cuts across all functional areas including engineering, test and evaluation, logistics and maintenance support, training, operations, configuration control and cost. It involves the participation of all Program Office members, the user and the contractor.

Organization in the Program Office

To illustrate the role of System Safety in the life cycle of a system this study will look at a "typical" Program Office and the System Safety effort during each phase of the acquisition cycle.

To simplify the vocabulary, the following terms will be used instead of the individual service designations: Program Office, Program Manager, Development Command (AFSC, DARCOM, NMC), Acquisition Division (AFSC System Divisions, DARCOM Research and Development Commands, NMC SYSCOM's) and Support Commands (AFLC, DARCOM Readiness Commands, Navy Field Activities). These titles are descriptive enough to be self explanatory. The general statements concerning these elements apply to all three services unless otherwise specified.

Principal Participants

The individual responsible for System Safety in any project is the Program Manager. It is his responsibility to appoint a focal point for System Safety within the office and to provide sufficient resources to perform the System Safety task. All significant safety matters which cannot be resolved at lower levels are brought to his attention for a decision.

Each Program Office has a designated focal point for safety - the System Safety Officer (SSO). This individual is responsible for the accomplishment of the System Safety tasks to achieve effective and timely realization of the System Safety objectives. The SSO does this by ensuring that all areas of design, maintenance, support and operations are examined for safety imlications. The SSO's job is coordination of the safety effort - not necessarily the performance of the safety tasks. On major projects this position might be a full time duty, but in most cases it is an added duty for one of the full time program office personnel.

The System Safety Engineer (SSE) coordinates the engineering review of the system for System Safety. The SSE draws upon the efforts of personnel in various engineering disciplines to identify and evaluate system hazards and to recommend safety changes. The SSE, in cooperation with the SSO and other engineering disciplines, performs in-house System Safety analyses. Like the SSO, this position on a major program may be a full time duty, but more often the Program Office shares the time of an SSE or safety staff.

All of the services provide for, but not all require, the formation of System Safety Groups (SSG) for each program (13). A SSG, chaired by or reporting to the Program Manager, is a formally chartered group organized to assist the Program Manager in achieving System Safety objectives. It consists of members appropriate to the task at hand, e.g., SSO, SSE, Program Office representatives from Test, Logistics and Engineering, the user and representatives from the services' independent test and evaluation organization, laboratories and other participating organizations. Meetings of the SSG usually coincide with significant project milestones like source selection, design reviews and major test events or are called to consider a specific significant safety problem. A SSG can levy safety related tasks on participating organizations or recommend that additional System Safety effort be initiated by the contractor, Government laboratories or development commands. Formal minutes over the Program Manager's signature are usually required of all SSG meetings.

Day to day System Safety efforts are handled by informal ad hoc groups which include participation by representatives from all concerned organizations - usually various engineering disciplines, test and logistics. In some cases these groups are referred to as System Safety Working Groups (SSWG).

Milestone 0

The system often receives its first "safety review" when the services' Development Command safety staff reviews the initial requirement document (AFSC Form 56 (USAF), TRADOC/DARCOM Letter of Agreement (USA) or Tentative Specific Operational Requirement (USN)). Usually no comment is made unless exceptional hazards are identified. Comments could also be expected if a MIL-STD-882A System Safety program was not to be required. In the absence of any specific guidance to delete a safety program both the DOD and Service regulations (1) (7) (18) (28) require that a MIL-STD-882 safety program be carried out.

Conceptual Phase

Early in the Conceptual Phase the SSO should identify and document the approach to System Safety to be used on the program. Since each program and each phase of a program have unique safety requirements, it is desirable that MIL-STD-882A be tailored to suit the technical and fiscal constraints provided by the Program Manager. Documentation of the tailoring effort will facilitate coordination of the safety effort with higher headquarters.

During the Conceptual Phase safety emphasis should be placed on assessment of the hazards associated with the proposed operating environment and characteristics of alternative systems, possible exposure to hazardous material, interface problems and special areas of safety concern, e.g., man-rating requirements. This information is sually documented by the contractor or SSE in the form of a Preliminary Hazard Analysis (PHA) for each alternative (see Section II for descriptions of safety analyses). Additional information on hazards identified on past and present systems may be obtained from each service's accident data files (Section IV) and in some cases from other Government or commercial sources like the Deparment of Transportation or the Electronic Industries Association.

Proper safety input at this stage can have considerable impact on life cycle costs through identification of critical hazard areas which need to be called to the attention of designers and users as early as possible in the program.

Demonstration/Validation Phase

During this phase subsystem/system prototypes or large scale models are often produced by a contractor for the Government. This process tends to "lock-in" many design details of the final product. For this reason, it is very important that a strong System Safety program be applied during this phase.

The following safety tasks are normally performed by the SSO and SSE:

a. Develop safety requirements for the solicitation

document - RFP, SOW.

b. Participate in source selection activities with emphasis on technology, design, test, training, production and operation and support risks having an impact on safety.

c. Review contractor's proposed System Safety Program Plan (SSPP) to ensure that the contractor has adequately addressed the areas of hazard analyses, hazard identification, tracking and resolution, safety participation in the design and testing processes, safety design reviews, and system interface hazards.

d. Evaluate the portions of the development specification pertinent to System Safety.

e. Participate in design reviews, test meetings and reviews, support and maintenance concept meetings and demonstrations, training meetings and System Safety Group meetings.

f. Review submitted safety analyses.

g. Prepare System Safety input for the Program Management Plan (PMP).

h. Provide safety support for (S)SARC/DSARC II.

The principal safety analyses prepared during this phase of the program will be the Subsystem and System Hazard Analyses (SSHA/SHA), an update of the PHA and in some cases an Operating and Support Hazard Analysis (O/SHA). These analyses are normally done by the contractor. In addition, certain critical subsystems may be further analyzed using Fault Tree Analysis (FTA), Failure Mode and Effect Criticality Analysis (FMECA) and other techniques identified in Section II and references 4, 17, 25 and 38.

Critical safety issues which are not resolvable at the working level will be documented by the SSO for the Program Manager's consideration and decision. The more complete the system development during Demonstration/Validation, the more important that a thorough System Safety effort be accomplished since many of the basic system parameters are being finalized. If System Safety is not persued aggressively during this phase, i.e., significant hazards identified and corrected, safety may become a matter of retrofit and modification after the system is built - both of which are usually more expensive and less satisfactory than if safety is designed in from system conception.

Full Scale Engineering Development (FSED)

The System Safety tasks performed during FSED are very similar to those performed in the Demonstration/Validation Phase, especially if a prototype was developed. These tasks include:

a. Preparing System Safety inputs for the RFP.

b. Participation in source selection.

c. Ensuring the SSPP is adequately updated.

d. Reviewing newly prepared or updated analyses.

e. Participating in design, test, training, maintenance and operations reviews and SSG meetings.

f. Supporting the Configuration Review Board.

g. Providing safety support for (S)SARC/DSARC III.

Special emphasis should be placed on operations and maintenance safety using as a baseline information developed in the Demonstration/Validation phase and updating it with data obtained

during development and operational suitability testing conducted during FSED.

The system should also be examined to determine whether there are any peculiar hazards being designed in which will be a problem during the ultimate disposal of the system.

During FSED most of the analyses described in Section II are updated and used to validate the safety of the system.

While most safety issues will be resolved without major expense or system changes, there is always the chance that an unanticipated critical issue will arise which requires major resources to resolve. The best way to avoid these late surprises is to require a strong, thorough System Safety program during the Conceptual and Demonstration/Validation phases so that as many unknowns as possible can be surfaced early.

Production

The primary System Safety efforts during Production are assuring that the safety issues brought to light earlier have been resolved and are reflected in the Production Specification and the operations, maintenance and training courses and manuals. If source selection is required for production or logistics support, the SSO will prepare RFP input and participate in proposal evaluations. Testing will be monitored to determine whether latent hazards are identified. Safety will also support the Configuration Review Board to ensure that ECP's do not degrade safety. Accident/Incident Review Boards will also be supported.

In addition, the SSO and SSE must document their safety

efforts to include all anlayses and the supporting rationale for decisions made. This material must be ready to transfer when the system transitions to the Support Command.

During Production safety mainly concentrates on validating the system as it enters the operational force. Major safety tasks this late in the program tend to result from changes in operational concepts, e.g., a desire to hot pit refuel fighter aircraft, rather than from latent safety failures. A good safety program will have eliminated most of the minor failures, but some can always be expected as the system matures in the field and some design parameters, e.g., reliability and maintainability, are found not to meet system specifications. In these cases some safety retrofits may be required.

Cost[4]

The prime cost driver for the System Safety function is the level of technology being used in the system. Those systems using low level technology or building on or modifying systems previously developed will expend relatively little on a System Safety Program. Conversely, programs pushing the state-of-the-art will have to spend considerably more on System Safety tests and analyses to validate the same level of safety.

Program System Safety costs typically are small in the Conceptual Phase when mostly qualitative analyses are done, but grow rapidly in Demonstration/Validation - particularly if the system is prototyped. System Safety costs usually peak during Full Scale Engineering Development as the system design is

finalized and safety tests and quantified analyses are performed. Costs during Production are limited to accident/incident analysis and change proposal evaluations. Costs can be large if major safety problems surface after the system is in the field.

On a large program System Safety costs are typically 1-3% of R&D costs, somewhat higher (3-5%) on intermediate cost programs and as high as 5-10% on lower cost programs (assuming all are using the same state-of-the-art technology). This is because much of the same levels of effort on safety analyses and tests are required on all programs regardless of their size.

System Safety costs can be minimized by tailoring the safety requirements, taking advantage of similar efforts expended on other programs and by starting the safety effort early to avoid costly redesigns and retrofits.

SECTION IV

ORGANIZATION FOR SYSTEM SAFETY

Introduction

There is no regulation or guidance concerning System Safety organization in the Department of Defense, thus each service has selected its own safety organization. In addition, in major commands within each service there are differences in organization and function depending upon the resources allocated by the command.

This Section is not meant to comment on the relative merits of different System Safety organizations within the DOD, but rather to give the reader an idea of the scope and setting of System Safety within his own organization. Hopefully this information will be useful to the reader in determining the assets which he might utilize for his safety program.

This Section was compiled largely as a result of some 18 interviews (see Appendix A) conducted with DOD System Safety personnel. The organizations described are current as of the writing of this report. They are subject to change beyond the control of the author.

DOD

The responsibility for System Safety at the DOD level lies within the office of the Deputy Assistant Secretary of Defense for Energy, Environment and Safety (DASD (EE&S)). Their charter for System Safety is DOD Directive 1000.3 (1). DASD (EE&S) is

responsible for determining and issuing policy for both System Safety and Occupational safety. System Safety guidance is presently being revised through the issuance of DODD 5000.XX, System Safety Program Requirements (2), and the updating of the Armed Forces Procurement Regulations (ASPR's) to reflect the requirements of the proposed DODD 5000.XX. This detailed guidance will supplement the general guidance presently contained in DODD 1000.3. It is anticipated that these changes will require more resources and effort on safety throughout the life of a system than are presently required.

Air Force

Air Force Inspection & Safety Center (AFISC)

The focal point for safety in the Air Force is the Air Force Inspection and Safety Center (AFISC) at Norton AFB, California. AFISC, which reports directly to the Air Force Inspector General, determines, documents and issues guidance on safety through the 127 series of AF regulations. AFR 127-8 (9) is the main implementing instrument for System Safety.

AFISC is also the AF Inspector General (IG) for safety. As part of this function it performs inspections, reviews program safety requirements (RFP's, SOW's, etc.), collects, analyzes and disseminates accident/incident data, reviews Program Office safety efforts (contractor and in-house documentation), participates in program safety reviews and directs the AF safety education program.

AFISC also coordinates safety data exchanges with interested parties outside the Air Force, e.g., the National Transportation Safety Board, Federal Aviation Agency and the other services.

The principal offices within the Directorate of Aerospace Safety at AFISC are: Policy and Programs (SEP), Education (SED), System Safety and Engineering (SES), Life Sciences and Human Factors (SEL), Reports and Analysis (SER), Weapon Safety (SEW), Ground Safety (SEG) and Flight Safety (SEF).

Accident/incident data may be obtained by writing AFISC/SER, Norton AFB, California 92409.

Air Force System Command (AFSC)

The AFSC is responsible for the development and production of aerospace vehicles and support equipment for the Air Force. The focal point for System Safety within the AFSC is in the Inspector General's office (IGF). This office provides the following safety functions for the AFSC: policy and guidance formulation, safety inspections and program review and assistance.

AFSC policy and guidance for organizing and implementing System Safety programs are contained in AFSCR 127-8 (12). In general all research, development and test programs are required to have a tailored MIL-STD-882 System Safety Program. In addition, programs are required to form a System Safety Group (Section III) which acts as a safety coordinating group for development, test and integration of the new system into the Air Force inventory.

AFSC Subordinate Commands

Each Systems Division (ASD, ESD, SAMSO, ADTC) has a staff safety office (SE) which reports to the commander and is responsible for safety policy and doctrine. Safety offices provide inspection, information and staff assistance functions for individual programs.

The Engineering Directorates of the Systems Divisions provide System Safety engineering support in the form of System Safety Engieers (SSE) (See Section III) who are drawn from engineering assets. Major programs usually have a full time SSE; small projects usually share an SSE with on or more other programs.

Also, within each Program Office, there is designated a System Safety Officer (SSO) (Section III) who is responsible for coordinating the System Safety effort for the program. Usually only major programs have a full time SSO.

AFSC Systems Divisions make extensive use of System Safety Groups (SSG) (See ASDP 127-1 (13)) to review program safety efforts and to ensure that the using command is brought into the program early to coordinate on operational and support safety problems.

Logistics and Using Commands

The Logistics (AFLC) and Using commands (MAC, TAC, SAC, ATC) have safety staff functions at Headquarters level which participate in the acquisition process to ensure that support and operational safety considerations are included in the development

process. Participation usually takes the form of membership on the SSG and review of System Safety documentation.

AFLC System Safety responsibility transfers from the Headquarters to the Air Logistics Center (ALC) once the ALC which will support the system is designated. This usually takes place during the Full Scale Engineering Development phase of the program. ALC participation on the SSG and their review of program documentation during acquisition helps facilitate transfer of the program to the ALC from the System Division once acquisition has been completed.

Test Organizations

The test organizations (AFTEC, SAMTEC, 6550 ABWG, AFFTC, Arnold Engineering Development Center) have flying, range and test safety functions which review all programs to ensure that safety requirements are met before any significant new phase of testing is approved. For those test organizations which employ civilian contractors, the safety function is written into the support contract.

Army

The Office of the Inspector General (DAIG-SD) provides policy and guidance for the Army System Safety program. The principal implementing documents are AR 70-17, System/Project Management (19), and AR 385-16, System Safety (22). This office also has IG responsibility for safety. The Army safety program is largely decentralized, therefore, the effectiveness of the Army

safety program is determined by the resources allocated at the major command level.

Development and Readiness Command (DARCOM)

Safety activity in DARCOM is split into three functions - policy and guidance, safety program evaluation and safety implementation. Each is the responsibility of a different organization.

Headquarters, DARCOM

The policy and guidance function is provided by the HQ, DARCOM Safety Office (DARCOM/SF) which provides overall direction to the DARCOM System Safety program. The Safety Office maintains general cognizance over subordinate commands by reviewing requirements documents, e.g., Required Operational Capability (ROC) and Letters of Agreement (LOA), to determine that system Safety is properly addressed. They also provide a channel for access to the DARCOM Command Section for System Safety matters which cannot be resolved at a lower level.

Field Safety Activity

The DARCOM Field Safety Activity (FSA), Charlestown, Indiana 47111, provides evaluations of the effectivness of the System Safety programs in the DARCOM subordinate commands by performing staff visits and reviewing program test reports and Safety Statements (see Section II, p. 12).

Staff visit reports for major activities, e.g., Main Battle

Tank Project Office, are forwarded through the DARCOM Safety Office to keep Headquarters aware of field problems; those for subordinate commands go directly to the commands. While these reports are not officially IG reports they are generally treated in a similar manner and do require an answer in writing.

The Field Safety Activity also writes and publishes DARCOM System Safety documents and regulations to implement DARCOM safety policies.

Another function of the FSA is to provide safety training for both System and Occupational Safety personnel. This training ranges from one week short courses to degree granting programs at major universities.

In general safety personnel in DARCOM are recruited from college engineering schools and are then trained in and remain in the safety field in the Command thus providing professional continuity for the Army's safety program.

Research and Development (R&D) Commands

In accordance with the Army's concept of decentralized safety responsibility, the R&D Commands and the Project Office commanders (approximately one quarter of all Army Project Offices report directly to the Commander, DARCOM) are responsible for establishing their own System Safety program. Usually the R&D Command's safety function reports to the commander or his deputy while the Project Office safety function reports to the Project Manager. This provides high visibility at top levels for the safety program.

System Safety is handled in generally the same way in all of the R&D Commands. Major programs are staffed, when possible, with a full time System Safety specialist. When resources do not permit, or the program is too small to warrant a full time effort, part time assistance is provided by the Safety Office to support safety and design reviews and for general system overview. Those programs not having a safety specialist have a full time person in the office who acts as a focal point for safety. He ensures that the Safety Office is provided with program safety documentation and that they are made aware of design reviews when System Safety participation is desirable.

Readiness Commands

Each Readiness Command has a Safety Office which is responsible for safety on systems which have transitioned from the Development Commands.

Safety transition includes the transfer of all safety documentation produced during system development and acquisition by the R&D Command. This transition is facilitated by the fact that most Army Development Commands and Readiness Commands are collocated.

The Readiness Commands rely to a great exgent on data collected in the field to provide System Safety feedback which is the basis for recommending changes to the system.

US Army Agency for Aviation Safety (USAAAVS)

The Aviation Safety Center at Fort Rucker, Alabama provides

the accident/incident data collection and dissemination service for the Army and also acts as the source for System Safety policy for Army aviation*.

USAAAVS's role in aviation safety includes co-chairing System Safety Group (Section III) meetings with the Project Office on major aviation programs, e.g., UTTAS and the Attack Helicopter. The Center also reviews Safety Statements, hazard analyses and system specifications. The principal emphasis in on crash-worthiness - the ability of the aircraft and its passengers to survive a crash.

To facilitate its aviation safety function USAAAVS maintains a liaison office at the Aviation Research and Development Command in St. Louis.

USAAAVS provides some data analysis for aviation systems. However, the responsibility for analysis of non-aviation data which is collected and disseminated by USAAAVS is left solely to the appropriate Research and Development or Readiness Command.

Information stored in the USAAAVS data bank may be obtained by making a written request to: USAAAVS Data Bank, ATTN: IGAR-TS (HICKS), Fort Rucker, Alabama 36362. Information on the data system may be obtained by calling Autovon 558-4812.

The USAAAVS also publishes quarterly the System Safety Newsletter which stresses items of interest to the aviation safety community.

---

*Policy for non-aviation systems is handled by HQ, Army (DAIG-SD).

Test Organizations

The Army's test ranges/facilities and the independent test organization (OTEA) require safety reviews before each significant phase of testing. The basis for these reviews is the Safety Statement (Section II) which is provided by the developer.

Navy

System Safety policy and guidance for the Navy are provided by the Chief of Naval Operations. This policy for System Safety is disseminated to the operating and acquisition commands in SECNAVINST 5100.10C (28) and OPNAVINST 5100.8C (29).

Naval Safety Center (NSC)

The NSC is responsible to the Chief of Naval Operations for assisting in formulating System Safety policy and guidance for the Navy (30).

The NSC also collects, stores and disseminates accident, incident and unsatisfactory material information for all Navy systems except ordnance*. The NSC staff, which ranges from medical personnel to statisticians, reviews this data to identify safety problems. This information, as well as studies of general interest, e.g., cockpit design, are forwarded to SYSCOM's and Field Activities for use in future system designs and for inputs to changes for systems in the fleet.

---

*Ordnance accident/incident information is collected by the Naval Weapons Surface Center at Dahlgren, Virginia. Information may be obtained by writing SAFEORD, Naval Weapons Lab (ES), Dahlgren, VA 22448.

NSC personnel also support accident/incident investigations and perform safety surveys of operational units and Field Activities. They also participate on interservice safety panels in areas such as aviation safety.

Information on individual classes of accidents/incidents as well as periodic publications on flying safety, operational safety, shipboard safety and other safety related information, may be obtained by writing the Naval Safety Center, Naval Air Station, Norfolk, Virginia 23511.

Navy Material Command (NMC)

The responsibility for safety in the NMC rests in NAVMAT-04F (Logistics). This Safety Office, which prepares and disseminates System Safety policy and guidance to the SYSCOM's and Field Activities, reports directly to the Office of the Commander, NMC. Only general guidance is provided in NAVMATINST 5100.6 (31) thus each SYSCOM and Field Activity is responsible for the details of its own System Safety effort.

System Commands (SYSCOM's)

The SYSCOM's and those major Project Offices which report directly to the Commander, NMC, e.g., TRIDENT, have taken advantage of the broad guidance given in reference 31 to develop several different types of System Safety programs. Some of the more interesting points are listed below.

NAVAIR

In NAVAIR each program tailors its safety program to meet its own objectives with emphasis placed on the risk analysis technique which results in a list of hazards in decreasing order of severity (a combination of category and frequency of occurrence). The Project Manager then determines which risks are unacceptable and must be eliminated.

Safety engineering support is obtained from the Engineering Safety Office (05). These trained System Safety personnel support the System Safety Working Groups (Section III) which each program is required to have. These groups provide safety review and guidance for each program.

NAVSEA

In NAVSEA the System Safety function is divided into two areas of responsibility - ship systems and weapon systems. This approach is taken mostly because of the different technologies used in the two areas.

Ship hull technology tends to be mature and ships also tend to closely resemble floating cities with living quarters, shops, boiler rooms, etc. Thus the main safety effort tends to be on occupational safety with System Safety applied to modification or the introduction of new technologies, e.g., HALON fire suppression systems.

Ship weapon systems, on the other hand, use advanced technology subsystems and are often replaced (up to five times in the life cycle of a hull). Thus weapon system development

concentrates more on System Safety with System Safety Groups (optional), safety analyses tailored to the program and staffing at least part time by a System Safety Officer/Engineer.

NAVELEX

When NAVELEX is procuring commercial or modified commercial equipment the safety function is usually limited to the generation of a Hazard List or a Safety Statement (Section II). This effort is aimed at eliminating obvious hazards and identifying hazards associated with integration of the equipment into the Navy system.

On development programs a more extensive System Safety program is required concentrating on electromagnetic, radiological, hazardous materials and hardware hazards.

The System Safety function is tied closely to the Quality Assurance function with common tests often required to satisfy both specialties.

NAVSUP

Most items procured by NAVSUP deal with material handling, storage and retrieval and most are derivatives of commercial products. Therefore, most programs require only an Operational Hazard Analysis which concentrates on the operational environment where it differs from the commercial environment.

Field Activities

Safety in Navy Field Activities concentrates on tracking incident/accident information from the fleet and supporting

changes to the system when the data warrants.

R&D Centers and Laboratories

The Navy's research facilities provide much of the Navy's System Safety expertise. This expertise, in the form of trained System Safety engineers, is available to the SYSCOM's for use during the development and acquisition of Navy systems. This assistance is normally obtained by the Program Office through the Safety Office of the SYSCOM.

Weapon System Explosives Safety Review Board (WSESRB)

NAVSEAINST 8020.6 (34), responding to NAVMATINST 8020.1D (33), established the WSESRB under the chairmanship of NAVSEA. The board also has members from the other SYSCOM's (NAVAIR, NAVELEX, NAVSUP and NAVFAC) as well as the Naval Safety Center which represents the users. The Naval Weapons Laboratory, Dahlgren, provides technical advice to the WSESRB.

Each program must present to the WSESRB details of the design, operation and safety features of any explosive device which is contained within the system regardless of its function, e.g., propellants are included under this instruction. An explosives safety certification must be obtained from the WSESRB before moving to each new stage of system development and before deployment.

Navy Test Organizations

Navy test organizations are concerned with the safe use of

their ranges/facilities. Therefore system test plans and parameters are reviewed for safety by the testing organizations at all significant test milestones.

Plant Representatives

The Plant Representative's office, whether staffed by the services (AFPRO, NAVPRO, Army Plant Representative) or by the Defense Contracting Agency (DCASPRO), designates a safety representative for each program in the plant. This individual provides an "on the spot" presence during system development and production. Close contact between the plant safety representative and the Program Office safety manager can result in on the spot monitoring of the contractor's safety program on a far more frequent basis than could be provided by Program Office personnel.

SECTION V

SUMMARY

System Safety does not attempt to eliminate all hazards. To do so would be impractical, too expensive and too time consuming to say nothing of performance limiting. Rather the aim is to reduce identified hazards to an acceptable level. The definition of "acceptable" is left to the Program Manager to define based on trade-offs between cost, schedule and performance.

A safety program is most effective if it is started early in the program - during the Conceptual Phase. Most major safety impacts are made during the development of the first full scale system. After that time safety retrofits often become prohibitively expensive or too politically sensitive to make. The system then often must be derated, e.g., C-5A, if it is used safely.

System Safety must report directly to the Program Manager and not to a functional director. Otherwise it may not get the Program Office wide support it requires to be most effective.

The responsibility for a strong, effective System Safety program lies with the Program Manager and it's success is a direct function of how much support he gives to his System Safety effort.

Interviews with System Safety personnel from all of the services revealed that each service and major command tailors the structure of its safety program to compliment the technology

being developed and the resources on hand. Thus there are almost as many different types of System Safety programs in the DOD as there are acquisition organizations. However, without exception, the interviewees stated that the success of their efforts was directly related to the support given to the safety program by the Program Manager.

SECTION VI

FOOTNOTES

1. Numeric values are suggested in reference 6 as follows:

   Frequent - Up to one failure in 1000 hours.

   Reasonably Probable - Up to one failure in 10,000 hours.

   Occasional - Up to one failure in 100,000 hours.

   Remote - Up to one failure in 1,000,000 hours.

   Extemely Improbable - Less than one failure in 1,000,000 hours.

   Impossible - No failures.

2. Reference 38C, p. 2-8, lists unacceptable loss rates for DD type (10^{-9}) and CV Type (10^{-11}) ships.

3. Reference 25, p. 6-4, contains discussions of considerations that may lead to a lowering of acceptable probabilities.

4. Reference 38a, Chapter 5, contains a discussion of System Safety program costs.

APPENDIX A

Interviews

DOD

26 Aug 77 LTC Les White, USAF, Office of Deputy Assistant Secretary of Defense (Energy, Environment & Safety), DASD (EES), Pentagon, Washington, D. C.

Navy

12 Aug 77 CDR Ritchey, Naval Materiel Command (MAT-04F3), Safety Office, Washington, D. C.

12 Aug 77 Mr. Ed Dougherty & Mr. John Sharockman, Naval Materiel Command (NAVSEA-04H) Safety Office, Washington, D. C.

18 Aug 77 Mr. Leo Schroeder, Naval Materiel Command (NAVELEX-4703), Safety Office, Washington, D. C.

18 Aug 77 Mr. Jim Gibble, Naval Materiel Command (NAVAIR-09E3), Safety Office, Washington, D. C.

18 Aug 77 Mr. Paul Chaen Kwok, Naval Materiel Command (NAVSUP-0322), Safety Office, Washington, D. C.

20 Sep 77 Mr. Bill Titus, Naval Materiel Command (NAVSEA-04H), Safety Office, Washington, D. C.

23 Sep 77 Mr. George Stewart, Naval Safety Center, Naval Air Station, Norfolk, VA (Phone).

Army

10 Aug 77 Mr. Pete Rutledge, DARCOM (DRC/SF), Safety Office, Alexandria, Virginia.

26 Aug 77 Mr. Craig Schilder, HQ, Department of the Army (DAIG-SD), Safety Office, Pentagon, Washington, D. C.

8 Sep 77 Mr. Jim Johnson, DARCOM Field Safety Center, Charleston, Indiana (Phone).

8 Sep 77 Mr. Jim Hicks, US Army Agency for Aviation Safety (USAAAVS/IGAR-TS), Fort Rucker, Alabama (Phone).

13 Sep 77 Mr. Ron Larch, DARCOM Mobility Equipment Research and Development Command (MERADCOM) Safety Office, Fort Belvoir, Virginia.

29 Sep 77 Mr. Jim Elliott, DARCOM Aviation Systems Command (AVSCOM/DRSAV-X), Safety Office, St. Louis. Missouri (Phone).

Air Force

9 Aug 77 Mrs. Joyce McDevitt, HQ, Air Force Systems Command (AFSC/IGF), Andrews AFB, MD.

9 Aug 77 Mr. Don Chislaghi, Aeronautical Systems Division, ASD/ENEST, Wright-Patterson AFB, Ohio (Phone).

12 Aug 77 Mr. Dick Olsen, Space and Missile Systems Office (SAMSO/SE). Los Angeles, California (Phone).

15 Aug 77 Major Bob Sweginnis, Air Force Inspection and Safety Center (AFISC/SES), Norton AFB, California (Phone).

BIBLIOGRAPHY

DOD

1. DODD 1000.3, Accident Prevention, Safety and Occupational Health Policy for the Department of Defense, 15 Jun 1976.

2. DODD 5000.XX, System Safety Program Requirements (Draft), May 1977.

3. MIL-STD-721B, Definitions of Terms for Reliability, Maintainability, Human Factors and Safety, 10 March 1970.

4. MIL-STD-882A, System Safety Program Requirements, 28 June 1977.

5. MIL-STD-1574, System Safety Program for Space and Missile Systems, 15 March 1977.

6. DI-H-3278, System Safety Hazard Analysis Report (Draft), undated.

Air Force

7. AFR 127-1, Accident Prevention, Responsibilities for USAF Aerospace Programs, 16 March 1972.

8. AFR 127-4, Investigating and Reporting US Air Force Mishaps, 24 Oct 1975.

9. AFR 127-8, Responsibilities for USAF System Safety Engineering Programs, 19 April 1976.

10. AFR 127-101, Ground Accident Prevention Handbook, 4 Sep 1974.

11. AFSCR 127-4, Investigating and Reporting USAF Air Force Mishaps, 15 June 1976.

12. AFSCR 127-8, Responsibilities for USAF System Safety Engineering Programs, 27 Aug 1976.

13. ASDP 127-1 System Safety Programs, 23 Aug 1977.

14. AFSC DH 1-6, System Safety.

15. AFSC DH 1-X, Checklist of General Design Criteria, August 1974.

16. AFETRM 127-1, Range Safety Manual, August 1975.

17. SAMSOR 127-8, System Safety Engineering, 30 April 1976.

Army

18. AR 70-1, Army Research, Development and Acquisition, 1 May 1975.

19. AR 70-17, System/Program/Project/Product Management, 11 November 1976.

20. AR 70-27, Advanced Development Plans/System Development Plans, 17 March 1975.

21. AR 385-10, Army Safety Program, 17 February 1970.

22. AR 385-16, System Safety, 22 September 1972.

23. AMCR 385-12, Life Cycle Verification of Materiel Safety, 29 June 1972.

24. AMCR 385-24, Development of Army Range Safety Requirements, 11 April 1974.

25. DARCOM P385-23, System Safety, 1 June 1977.

26. USAAAVS TR72-8, Prepration of an SSPP for Aviation System Development, April 1972.

Navy

27. SECNAVINST 5000.1, System Acquisition in the Department of the Navy, 13 March 1972.

28. SECNAVINST 5100.10C, Accident Prevention, Safety and Occupational Health Policy; Implementation of, 21 October 1976.

29. OPNAVINST 5100.8C, Department of the Navy Safety Program; Implementation of, 8 September 1976.

30. OPNAVINST 5450.180, Naval Safety Center; Mission and Functions, 8 April 1970.

31. NAVMATINST 5100.6, System Safety Program; Implementation of, 2 April 1970.

32. NAVMATINST 5100.10, Safety Responsibility in Designated Project Management Offices within the Naval Materiel Command, 20 August 1976.

33. NAVMATINST 8020.1D, Naval Explosives Safety Program, 12 January 1971.

34. NAVSEAINST 8020.6, Naval Explosives Safety Program; Responsibilities, Policies and Procedures for, 27 May 1976.

35. NAVELEXINST 5100.5, System Safety Program; Implementation of, 7 July 1971.

36. NAVAIRINST 5100.3A, System Safety Policies, Objectives and Responsibilities, 15 October 1976.

37. NAVFACINST 5100.11A, Safety; Command Policy and Program for, 15 July 1971.

38. NAVORD OD 44942, Weapon System Safety Guidelines Handbook, Navy Ordnance System Command.

    a. Part I; System Manager's Guide to System Safety 1 May 1973.

    b. Part II; System Safety Management Guidelines, 1 May 1973.

    c. Part III; System Safety Engineering Guidelines, 1 May 1973.

    d. Part IV; Hazard Control for Explosive Ordnance Production, 15 January 1974.

39. Minutes: Weapons Systems Safety Symposium, Naval Weapons Laboratory, Dahlgren, Virginia, May 1972.

Miscellaneous

40. Proceedings of Second International System Safety Conference, 21-25 July 1975, San Diego, CA.

41. Safety Enginering Bulletin No. 2; System Safety: Bibliography, Electronic Industries Association, Washington, D. C., August 1970.

42. Safety Engineering Bulletin No. 3; System Safety: Analytical Techniques, Electronic Industries Association, Washington, D. C., May 1971.

43. Sneak Analysis: An Effective Air Force Tool; The Boeing Company, Houston, TX, undated.