1970

NATIONAL TRANSPORTATION SAFETY BOARD

Report Number: NTSB-RSS-70-1

NATIONAL TRANSPORTATION SAFETY BOARD

STUDY OF WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY'S SAFETY PROCEDURES FOR THE PROPOSED METRO SYSTEM

NATIONAL TRANSPORTATION SAFETY BOARD
Bureau of Surface Transportation Safety
Washington, D. C. 20591

NATIONAL TRANSPORTATION SAFETY BOARD

STUDY OF WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY'S SAFETY PROCEDURES FOR THE PROPOSED METRO SYSTEM

NATIONAL TRANSPORTATION SAFETY BOARD
Bureau of Surface Transportation Safety
Washington, D. C. 20591

For sale by U.S. Department of Commerce, CLEARINGHOUSE for Federal Scientific and Technical Information, Springfield, Va., 22151. Single copy $3.00; Microfiche $0.65.
Report Number: NTSB-RSS-70-1

DEPARTMENT OF TRANSPORTATION
NATIONAL TRANSPORTATION SAFETY BOARD
WASHINGTON, D.C. 20591

OFFICE OF
THE CHAIRMAN

September 28, 1970

Mr. Jackson Graham
Washington Metropolitan Area Transit Authority
950 South L'Enfant Plaza, S. W.
Washington, D. C. 20024

Dear Mr. Graham:

The National Transportation Safety Board has a continuing interest in improving safety in the Nation's transportation network. In fulfilling one phase of our objective in this respect, we are reviewing safety management procedures in mass transit systems.

Several months ago, Members of this Board and staff personnel reviewed proposed designs of the Metro System. On May 18, 1970, you were advised of our continuing interest in the proposed Metro System, and arranged for staff conferences to assist us in developing information relative to the status of safety management of WMATA's proposed system. You were advised we would consider some detailed matters of the proposed Metro System; however, no technical review was contemplated. Since that time, members of my staff have received complete cooperation from your assistants in determining how WMATA has approached safety in the development of the proposed Metro System.

A review of available materials and conversations with your staff revealed that the WMATA approach to safety in the development of Metro consists mainly of reliance on the counsel and advice of consultants, with periodic review of the consultants' decisions by WMATA engineering staff. We believe that a more systematic approach to the question of safety could result in a safer subway system.

In the attached study, we have outlined some of the identifiable high-risk areas of Metro that we believe would benefit from a system safety review of the proposed system. Additionally, we have recommended a program that will assist you in identifying predictable hazards in the development stage of the Metro System.

If you desire it, we would welcome the opportunity to discuss the attached study with you or your staff.

Sincerely yours,

John H. Reed

John H. Reed
Chairman

Attachment

A STUDY OF

WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY'S

SAFETY PROCEDURES

FOR THE

PROPOSED METRO SYSTEM

BY

THE NATIONAL TRANSPORTATION SAFETY BOARD

WASHINGTON, D. C. 20591

NATIONAL TRANSPORTATION SAFETY BOARD
STUDY OF
WASHINGTON METROPOLITAN AREA
TRANSIT AUTHORITY'S SAFETY PROCEDURES
FOR THE PROPOSED METRO SYSTEM

I. BACKGROUND

Under the authority of Title III of the National Capital Transportation Act of 1960, the District of Columbia negotiated an interstate compact with Maryland and Virginia to establish an organization to provide necessary regional transit facilities. As a result, the Washington Metropolitan Area Transit Authority (WMATA) was created. WMATA is governed by a Board of six Directors, consisting of two Directors from each signatory. One of the purposes of this Authority is to plan, develop, finance, and cause to be operated improved transit facilities in coordination with transportation and general development planning by others for the Washington Metropolitan Area Transit Zone, as part of a balanced system of transportation. The zone embraces the District of Columbia; the cities of Alexandria, Fairfax, and Falls Church; and the counties of Arlington and Fairfax in Virginia; and the counties of Montgomery and Prince George's in Maryland.

In 1969, the Congress of the United States authorized construction of a regional system consisting of 97.96 miles of rapid rail transit routes, serving the central core area of the National Capital region. Approximately 47.47 miles will be underground line and stations, and 50.49 miles will be above ground.

The Metro System will have double-track, standard gauge, steel rails, and dual-truck cars with steel wheels. Trains will be 2-, 4-, 6-, or 8-car operated by an automatic train control system. Underground stations will be 600 feet long, generally 64 feet wide with a 30-foot high, arched, coffered roof of structural concrete with side or center platforms. The stations will have floating mezzanines, escalators from street to mezzanine and mezzanine to platforms, air conditioning, indirect lighting, automatic fare collection, and auxiliary rooms for maintenance and operation facilities. Tunnels will be single-track and double-track horseshoe in rock, single-track bore in earth, and some mixed-face, double-track horseshoe. Tunnel bores will normally provide 16 feet 6 inches finished inside diameter for single track. A third rail will furnish 600- to 750-volt d.c. power to trains. Telephone and radio communications will be provided throughout the system.

The cost of the adopted Metro System was estimated in December 1969 to be $2,494.6 million. This capital cost is to be met by a combination of Federal and local grants and the issuance of revenue bonds. Of the net project cost of $1,720.5 million, the two-thirds Federal share of $1,147.0 million includes a $100 million Federal grant, authorized in 1965. 1/

1/ See Appendix A, Metro Fact Sheet, Adopted Regional Rapid Rail Transit System (Revised), December, 1969.

For construction and operational reasons, the Metro System will be built and put into operation in six phases. The construction period will span 10 years as follows:

Phase I	- Completion in 1973
Phase II	- Completion in 1974
Phase III	- Completion in 1974
Phase IV	- Completion in 1976
Phase V	- Completion in 1978
Phase VI	- Completion in 1979

The first trains will go into service on the "Phase I" segment from Dupont Circle Station through downtown Washington to Rhode Island Avenue Station. The WMATA Board of Directors approved the first Metro construction contract on December 9, 1969, for about three-quarters of a mile of cut-and-cover construction from 10th and G Streets to Third and D Streets, N. W., as well as work on two underground stations at Gallery Place and Judiciary Square.

In January 1966, WMATA's predecessor, the National Capital Transit Agency, appointed a general engineering consultant for conceptual engineering. The statement of work in the contract with the general engineering consultant did not specify that safety be given consideration in the development of concepts, specifications, and design of the components of the Metro System. According to WMATA, the Manual of Design Criteria is the document that established the basic criteria to be used in the design of the Metro System. WMATA's Manual of Design Criteria does not specify the level of safety required in any engineering phase of system design. The responsibility for including safety requirements in all engineering phases has been left to the judgments of the engineers and architects.

While there was no specific requirement for safety in the contract for the development of the design criteria, WMATA placed the responsibility upon its engineers to consider safety as a prime factor in the development of the engineering aspects of the proposed system. There has been a continuing review by the engineering personnel in WMATA of the decisions reached by the consultants.

The resultant interreaction and exchange of ideas represent, to a large extent, WMATA's approach to safety in the proposed Metro System. A general recognition of the need for the development of a safe system exists; however, it appears that no procedure has been developed by WMATA to insure it.

In the development of the Metro System, WMATA has not subjected all phases of planning and development to a disciplined analysis for safety purposes. Decisions made by the consultants and WMATA personnel are not subjected to a critical systematic safety engineering review. The approach to safety utilized by the consultants and WMATA personnel has resulted in the proposal of a system with potentially serious identifiable hazards.

II. IDENTIFIABLE SAFETY PROBLEMS

A. Location of Metro tracks adjacent to tracks of conventional railroads.

According to proposed plans, the distance between the Metro tracks and the railroad tracks will not be sufficient to prevent interference in cases of derailment or shifted loads on freight trains. There are no plans for means or devices to prevent excursion of Metro trains or conventional trains from their tracks in cases of derailment.

B. Location of Metro tracks adjacent to public highways.

The proposed highway guard rails and chain-link fencing will not prevent a loaded truck from encroaching upon the Metro tracks.

C. Metro trains operating on double-track sections in tunnels.

There will be no support columns or other structures separating trains moving in opposite directions. The absence of any means of preventing the excursion of Metro trains from their tracks make a collision with an opposing train almost inevitable in case of derailment.

D. In-station separation of passengers from track and Metro trains.

The proposed Metro System provides for 86 stations, with access to the trains from platforms located between the tracks or adjacent to the sides of the tracks. No positive means have been proposed to prevent users from being pushed, jumping, or falling from the platforms onto the tracks in front of rapidly approaching trains.

E. In-tunnel emergency procedures for crowd control of passengers under panic conditions.

While there will be narrow safety walkways along the sides of the tunnels, there are no provisions for emergency exits from the tunnels.

F. Design of the cars.

The preliminary design criteria for the cars does not provide for protection of the passengers in cases of collision, derailment, or emergencies requiring immediate evacuation of the occupants.

The foregoing citations are a few examples of potential hazards observed by the Safety Board. The Safety Board's analysis was not a complete technical review of the entire proposed Metro System, but rather observations of obvious factors which contain the potential for catastrophe unless they are identified and assessed.

III. NEED FOR SYSTEM SAFETY

In view of the foregoing, a system safety engineering approach in analyzing the proposed Metro System appears warranted. The Safety Board continuously reviews the use being made of advanced concepts of accident prevention and risk management through the use of system safety. The National Aeronautics and Space Administration (NASA), the U. S. Air Force (USAF), and the U. S. Atomic Energy Commission (USAEC) apply system safety engineering principles to the analysis of each of their projects. The application of system safety principles to all phases of WMATA's proposed Metro System can serve as a useful tool in furthering present efforts to create a safe, rail rapid-transit system for the Washington area.

Reference is made to MIL-STD-882 issued by the Department of Defense on July 15, 1969. This document is attached for information and use as a proven guideline in establishing system safety programs. (See Appendix B.)

Particular reference is made to paragraphs 3.14, 5.5, and 5.8 of MIL-STD-882. Paragraph 3.14 defines qualitative risk levels of hazards under four categories, extending from negligible to catastrophic. Paragraph 5.5 describes the determination of the levels of safety that are acceptable in a system. Paragraph 5.8 specifies that analyses are to be performed which will insure that hazardous conditions are identified for the purpose of their elimination or control. This paragraph also requires analyses to determine that the qualitative levels of safety decided upon have been accomplished.

In paragraph 5.8.1.2 of MIL-STD-882, it is specified that a quantitative analysis provides a numerical assessment of the relative safety of system design. After a cost-benefit assessment to determine the level of safety to be provided, the decision by management will furnish a basis for review by funding agencies and other reviews by public authorities.

The basic objective of system safety is to identify safety questions in the early stages of the development of a project. If system safety had been employed during the conceptual stage of the Metro's development, and carried through as an analysis of the entire life cycle including design, development, and operation of the project, safety questions would have been raised in a formal way. Through this process, safety receives primary attention throughout all stages of the development of a new system.

IV. APPLICATION OF SYSTEM SAFETY APPROACH TO IDENTIFIABLE HAZARDS

Some of the hazards that system safety would have identified in the Metro System follow:

A. Location of Metro tracks adjacent to tracks of conventional railroads.

The absence of a positive means of preventing derailed trains from leaving the track structure will increase the damage caused by derailments. With Metro tracks lying adjacent to railroad tracks without means of preventing interference

between the two systems, in cases of derailments, the potential for disaster becomes a foreseeable possibility. In Dunreith, Indiana, on January 1, 1968, a simple derailment of a car in a westbound freight train, which diverged into an eastbound freight train going in the opposite direction, resulted in fires and explosions which destroyed the major industry of the community, demolished and/or damaged many homes and businesses, and contaminated nearby streams with poisonous chemicals.2/

On September 15, 1968, an undesired emergency brake application on a westbound freight train jackknifed cars into the path of a westbound passenger train on an adjacent track. When the passenger train struck the freight cars, the locomotive and first car derailed and overturned, and the remaining cars derailed, injuring 78 persons. If the passenger train had consisted of conventional commuter-type equipment instead of the massive GG-1 locomotive and coaches, the damage probably would have been much greater.

Shifted loads, loose boxcar doors, and off-center cars on railroad trackage could cause interference with a loaded Metro train that could result in death or injury to numerous persons. The proposed chain-link fence would prevent employees of one system from flagging the trains of the adjoining system if the track becomes obstructed. Possible elimination of these hazards lies in physically separating the systems horizontally or vertically.

B. Location of Metro tracks adjacent to public highways.

The problem of maintaining integrity of the Metro tracks when they are adjacent to public highways can be handled more easily. While derailment of a Metro train is a distinct possibility, the probability of its happening is much less than the probability of an out-of-control truck violating the track. The needed protection could be afforded by a concrete wall, similar to the one which separates the opposing lanes of traffic on the Woodrow Wilson Bridge where I-495 crosses the Potomac River.

C. Metro Trains operating on double-track sections in tunnels.

System safety would have identified the risk of collision when derailment occurs in a double-track tunnel and would have allowed for an assessment of the problem. A possible determent to collision would be some form of guardrail to keep the derailed train in line with the track.

2/ NTSB Railroad Accident Report No. SS-R-2, adopted December 18, 1968.

D. In-station separation of passengers from tracks and Metro trains.

A review of the latest accident statistics for rail rapid-transit operations reveals that a significant number of accidents to passengers occur on platforms and tracks in stations. In the major cities of the United States having rail rapid-transit, there were 9,194 reported station accidents in 1969; 848 of these accidents occurred on station platforms, and 564 occurred on tracks in stations. In addition, there were 5,263 reported accidents to persons in stations while on trains or while boarding and/or alighting from trains.[3/] The proposed stations for the Metro System have open platforms adjacent to tracks without physical controls to prevent passengers from falling, being pushed, or jumping onto tracks in front of moving trains. With trains which can be stopped automatically within a few feet of a predetermined spot, it appears that an arrangement could be developed to separate waiting passengers from incoming trains. A pattern of discharging passengers from one door and taking on passengers at another door would facilitate the loading and unloading of passengers. If waiting passengers are separated by a barrier wall from incoming trains until the trains stop, the opportunity for falling onto the track or between cars is minimized.

E. In-tunnel emergency procedures for crowd control under panic conditions.

The problem of handling large numbers of people under emergency conditions without panic or serious personal injury is one of the most vexing ones facing mass transit operations. Identifying possible emergencies and developing plans and physical facilities to cope with them would result from a system safety approach. Emergency exits from tunnels with well-marked and lighted access walks is a must if frightened people are to be evacuated safely from a subway. The operating personnel must be well trained before the fact and provided with good communications if serious situations are to be avoided.

Electrical fires on subway vehicles are not unusual; however, the means of evacuating passengers under these conditions are not obvious. On May 27, 1969, near the North Bergen portal of the North River Tunnel near Newark, New Jersey, an electrical fire on one unit of a Penn Central multiple-unit commuter train filled the tunnel with dense smoke. One off-duty employee lost his life, and a number of passengers were injured in the unorganized evacuation.[4/]

3/ National Safety Council Rapid Transit Accident Data Exchange, Comparative Operating Accident Rates.

4/ Federal Railroad Administration Railroad Accident Investigation Report No. 4150.

F. Design of Cars.

Without a technical analysis of the preliminary design of the car, its safety qualifications and crash-worthiness cannot be assessed completely. It is obvious, however, that the front-end design represents a potential hazard to the operator and passengers. In overturn of high-speed locomotives on railroads, dirt, gravel, and other debris often are scooped into the operator's compartment causing death or injury. This phenomon occurred May 15, 1968, at Edgerton, Ohio, when the lead unit of Penn Central passenger train No. 63 derailed and overturned. The mud and debris entered the cab of the lead diesel unit and forced the fireman against the top of the cab, causing serious injury.

The preliminary design of the Metro car indicates that there would be little protection from foreign material if the car overturns at high speed. Furthermore, the large windows will be more vulnerable to impact and will be a factor in damage to passengers. Obviously, the car is not designed to maintain its structural integrity in collision situations.

The inward-swinging doors in the ends of the cars create a serious problem under panic conditions when passengers are attempting to get out. On December 28, 1966, 13 persons perished from smoke and fire because they could not get out of an inward-swinging door of a Boston and Maine commuter car which had struck a fuel oil truck.[5/] There is a definite need for means of evacuating passengers other than through regular doors. Emergency removal of windows in a manner comparable to those in aircraft or buses should be considered. Some type of a ladder should be available to get people from car floor level to the invert of the tunnel.

V. CONCLUSION

The Safety Board concludes from the foregoing that although the proposed Metro System was conceived by competent, safety-conscious professionals, the absence of provisions for a disciplined, systematic review of the entire project has resulted in a system with identifiable hazards which could lead to disaster in the future operations. It is not too late to analyze the entire proposed Metro System and to identify those safety problems that could be corrected within the economic boundaries of the proposed system.

5/ NTSB Railroad Accident Report, Boston and Maine Corporation, Single Diesel-Powered Passenger Car 563, Collision with Oxbow Transport Company Tank Truck at Second Street Railroad-Highway Grade Crossing, Everett, Massachusetts, December 28, 1966.

VI. RECOMMENDATIONS

The Safety Board recommends that WMATA develop the capability within its organization for system safety engineering and apply system safety principles to all aspects of the proposed Metro System to identify, assess, and correct those deficiencies identified by the analysis.

Attachments

METRO FACT SHEET
ADOPTED REGIONAL RAPID RAIL TRANSIT SYSTEM (REVISED)

Washington Metropolitan Area Transit Authority; 950 S. L'Enfant Plaza, S. W., Wash., D. C.

ROUTE MILES	97.7 Total; 37.7 in District of Columbia; 30.1 in Virginia; 29.9 in Maryland
MILES IN SUBWAY	47.2
MILES ON SURFACE	50.5
NUMBER OF STATIONS	86 (including 53 underground); 44 in District of Columbia, 20 in Virginia, 22 in Maryland
ESTIMATED 1990 ANNUAL PATRONAGE	292,610,000 passengers
VEHICLES	556 air-conditioned cars; 75 feet long, 10 feet wide; seating 81 passengers with 94 standees; capable of operating in 8-car trains
OPERATION	Automatic train control system will regulate train speed and spacing, start and stop trains, operate doors, and monitor train performance. Attendant can override electronics.
SPEED	Maximum 75 mph; average system speed, including stops, about 35 mph
PROPOSED SERVICE	2-minute, rush-hour headways on main routes; 4 to 8 minutes on branch lines. Operation daily from 5 A.M. to 1 A.M.
COORDINATION	Feeder bus network, auto and taxi drop-off lanes at stations; 30,100 parking spaces.
ESTIMATED COMPLETION DATE	Initial operation in 1972; completion by 1980
ESTIMATED CAPITAL COST	$2,494.6 million
REVENUE BONDING CAPACITY	$835 million
NET PROJECT COST	$1,720.5 million
Assuming: 2/3 federal share	$1,147.0 million (Including $100 million Federal Grant authorized in 1965)
1/3 local share	$573.5 million
ALLOCATION OF LOCAL GRANTS *	
District of Columbia	$208.7 million (Including $50 million grant authorized in 1965)
Virginia	$149.9 million
Alexandria 30.6	
Arlington County 54.0	
Fairfax City 2.6	
Fairfax County 61.9	
Falls Church 0.8	
Maryland	$197.0 million
Montgomery County 110.4	
Prince George's C. 86.6	

*Remaining $17.9 million will be allocated in 1974

December, 1969

APPENDIX B

MIL-STD-882

15 JULY 1969

Superseding
MIL-S-38130A
6 June 1966

MILITARY STANDARD

SYSTEM SAFETY PROGRAM FOR SYSTEMS AND ASSOCIATED SUBSYSTEMS AND EQUIPMENT: REQUIREMENTS FOR

FSC MISC

FOREWORD

The Department of Defense System Safety Program's principal objective is the protection of the public and the individual. This is closely followed by its concern to conserve the other national resources.

To insure that these receive due consideration, this military standard has been written and approved by the Department of Defense and is mandatory for use by all departments and agencies of the Department of Defense effective 15 JULY 1969.

The degree of safety achieved in a military system is directly dependent upon management emphasis. Management emphasis on safety must be applied by the Government and contractors during the conception, development, production, and operation of each military system.

The results of the system safety effort is dependent upon the procuring agency clearly stating safety objectives and requirements, and the Contractor's ability to translate these into functional hardware.

Recommended corrections, additions, or deletions should be addressed to the Air Force Systems Command (SCIZ), Andrews AFB, Washington, D.C. 20331.

CONTENTS

Paragraph		Page
	FOREWORD	i
1.	SCOPE	1
	1.1 Purpose	1
	1.2 Application	1
	1.3 Implementation	1
2.	REFERENCED DOCUMENTS	1
3.	DEFINITIONS	2
	3.1 Safety	2
	3.2 System	2
	3.3 System safety	2
	3.4 System safety management	2
	3.5 System safety engineering	2
	3.6 Contractor	2
	3.7 Prime contractor	2
	3.8 Integrating contractor	2
	3.9 Associate contractor	2
	3.10 Subordinate (sub)contractor	3
	3.11 Crash safety	3
	3.12 Crashworthiness	3
	3.13 Hazard	3
	3.14 Hazard level	3
	3.14(a) Category I - Negligible	3
	3.14(b) Category II - Marginal	3
	3.14(c) Category III - Critical	3
	3.14(D) Category IV - Catastrophic	3
4.	GENERAL REQUIREMENTS	3
	4.1 System safety program	3
	4.2 System safety program activities and sequences	4
	4.2.1 Concept formulation phase	4
	4.2.2 Contract definition phase	5
	4.2.2.1 Contract Definition Phase (CDP) (Phase A)	5
	4.2.2.2 Contract Definition Phase (Phase B)	6
	4.2.3 Engingeering development phase	6
	4.2.4 Production phase	7
	4.2.5 Operational phase (including disposal)	7
	4.3 System safety organization	8
	4.4 System safety program milestones	8
5.	DETAILED REQUIREMENTS	8
	5.1 General	8
	5.2 System safety program plan (SSPP)	8
	5.3 Reviews	9
	5.3.1 Program and Design reviews	9
	5.4 System safety criteria and considerations	10
	5.4.1 General	10
	5.5 Hazard levels	10
	5.6 System safety precedence	10

CONTENTS

Paragraph		Page
5.7	Design criteria/specifications	11
5.8	Analyses	11
5.8.1	Qualitative or quantitative analysis	11
5.8.1.1	Qualitative analysis	11
5.8.1.2	Quantitative analysis	12
5.8.2	System hazard analyses	12
5.8.2.1	Preliminary hazard analysis	12
5.8.2.2	Subsystem hazard analysis	13
5.8.2.3	System hazard analysis	13
5.8.2.4	Operating hazard analyses	13
5.9	Action on identified hazards	14
5.10	Supplier and subcontractor system safety program	14
6.	DATA	
6.1	Data requirements	14
6.2	Data acceptance	14
6.3	Acquisition and use of safety data	14
7.	SAFETY TESTING	14
8.	TRAINING	15
8.1	Safety training for operator and maintenance personnel	15
9.	EFFECTS OF STORAGE, SHELF-LIFE, PACKAGING, TRANSPORTATION, HANDLING AND MAINTENANCE	15
10.	INTEGRATION OF ASSOCIATED DISCIPLINES	15
10.1	Relationship to system engineering	

APPENDIX

APPENDIX A	SYSTEM SAFETY PROGRAM PLAN OUTLINE	16
APPENDIX B	SYSTEM LIFE CYCLE - SAFETY ACTIVITIES	18

1. SCOPE

1.1 Purpose. The purpose of this standard is to provide uniform requirements and criteria for establishing and implementing system safety programs and to provide guidelines for preparing System Safety Program Plans (SSPP).

1.2 Application. This standard is applicable to Department of Defense procurement of military systems, subsystems, and equipment, such as aeronautical, nautical, vehicular, missile, space, electronics, weapons and munitions. This standard will be used during concept formulation, contract definition, engineering development, production, and operational phases.

1.3 Implementation. This standard will be used in preparing safety requirements for inclusion in contract work statements, system safety program plans, and other contractual documents.

1.3.1 Each provision of this standard shall be considered for the extent of applicability, deviations, or supplementary requirements. Where the paragraph or subparagraph of this standard would require duplication, wholly or in part, of design, analysis, test, demonstration, or organizational requirements already specified by the procuring activity, those requirements, functions and efforts shall be identified and utilized in the plan rather than be duplicated. This standard applies to those activities through which a contractor manages his system safety effort to the extent specified in the contract statement of work and approved SSPP. The SSPP shall be incorporated or referenced in contractual documents as necessary to define the safety program.

1.3.2 When the scope and magnitude of a program does not warrant the requirement for a comprehensive system safety program, the procuring activity shall specify to the contractor the minimum acceptable safety program requirements.

1.3.3 The safety life cycle as described herein (see 4.2) is for a system program which includes all phases: concept formulation, contract definition, development, production, and operational. Since all system programs do not follow the phases as distinctly as stated, each system safety program plan and activity must be tailored to the specific requirements and peculiarities of the system or project. The sequence of activities described in the safety life cycle, however, shall be accomplished at some time during the life cycle to insure that a balanced, effective system is developed. Accordingly, when a system program does not require a formal contract definition phase, the essential safety activities for that phase shall be accomplished early in the development phase.

2. REFERENCED DOCUMENTS

None applicable to this standard.

3. DEFINITIONS. The following definitions apply to this standard.

3.1 Safety. Freedom from those conditions that can cause injury or death to personnel, damage to or loss of equipment or property.

3.2 System. A composite, at any level of complexity, of operational and support equipment, personnel, facilities, and software which are used together as an entity and capable of performing and/or supporting an operational role.

3.3 System safety. The optimum degree of safety within the constraints of operational effectiveness, time and cost, attained through specific application of system safety management and engineering principles throughout all phases of a system's life cycle.

3.4 System safety management. An element of program management which insures the accomplishment of the system safety tasks including identification of the system safety requirements; planning, organizing, and controlling those efforts which are directed toward achieving the safety goals; coordinating with other (system) program elements; and analyzing, reviewing, and evaluating the program to insure effective and timely realization of the system safety objectives.

3.5 System safety engineering. An element of systems engineering involving the application of scientific and engineering principles for the timely identification of hazards and initiation of those actions necessary to prevent or control hazards within the system. It draws upon professional knowledge and specialized skills in the mathematical, physical, and related scientific disciplines, together with the principles and methods of engineering design and analysis to specify, predict, and evaluate the safety of the system.

3.6 Contractor. An industrial or governmental agency engaged to provide services or products within agreed limits.

3.7 Prime contractor. One who enters into agreement directly with the Government to provide a product or service.

3.8 Integrating contractor. The contractor assigned responsibility by the procuring activity for overall scheduling and system interface of associate contractor activities and equipment, and for the furnishing of specified support services which are common to two or more of the contractors.

3.9 Associate contractor. A prime contractor for the development or production of subsystems, equipments, or components meeting specifications furnished or approved by the procuring activity. An associate contractor can be one member of a group of contractors developing and producing a complete system.

3.10 Subordinate (sub)contractor. One who enters into agreement with a prime contractor or other subordinate contractor to provide a product or a service.

3.11 Crash safety. A manned-system characteristic that allows the system occupants to survive the impact and evacuate the vehicle in potentially survivable accidents. Crash safety implies:

(a) Crashworthiness
(b) Provisions for timely evacuation

3.12 Crashworthiness. The capacity of a vehicle to act as a protective container and energy absorber during potentially survivable impact conditions.

3.13 Hazard. Any real or potential condition that can cause injury or death to personnel, or damage to or loss of equipment or property.

3.14 Hazard level. A qualitative measure of hazards stated in relative terms. For purposes of this standard the following hazard levels are defined and established: Conditions such that personnel error, environment, design characteristics, procedural deficiencies, or subsystem or component failure or malfunction:

(a) Category I - Negligible

.... will not result in personnel injury or system damage.

(b) Category II - Marginal

.... can be counteracted or controlled without injury to personnel or major system damage.

(c) Category III - Critical

.... will cause personnel injury or major system damage, or will require immediate corrective action for personnel or system survival.

(d) Category IV - Catastrophic

.... will cause death or severe injury to personnel, or system loss.

4. GENERAL REQUIREMENTS

4.1 System safety program. The contractor shall establish and maintain an effective system safety program that is planned and integrated into all phases of system development, production,

and operation. The system safety program shall provide a disciplined approach to methodically control safety aspects and evaluate the system's design; identify hazards and prescribe corrective action in a timely, cost effective manner. The system safety program activities shall be specified in a formal plan (see 5.2) which must describe an integrated effort within the total program. The system safety program shall be based upon such factors as the system objectives, criticality of the safety requirements, the complexity of design, and total cost. The system safety program objectives are to insure that:

(a) Safety consistent with mission requirements is designed into the system.

(b) Hazards associated with each system, subsystem, and equipment are identified and evaluated, and eliminated or controlled to an acceptable level.

(c) Control over hazards that cannot be eliminated is established to protect personnel, equipment, and property.

(d) Minimum risk is involved in the acceptance and use of new materials and new production and testing techniques.

(e) Retrofit actions required to improve safety are minimized through the timely inclusion of safety factors during the acquisition of a system.

(f) The historical safety data generated by similar system programs are considered and used where appropriate.

4.2 System safety program activities and sequences. The application of this military standard to a specific contract requires a complete review of the standard to determine the degree of applicability of each paragraph to the contract. The safety requirements will vary depending on the amount of research, development, test, and engineering, and the intended use of the contract end item. The following paragraphs will give a general *indication of when the requirements of this standard should be* met during the development of a system for the Department of Defense when the formal DOD development process is applied. (See Appendix B).

4.2.1 Concept Formulation Phase. A formal SSPP is not required in the concept formulation phase. As system concepts and functions are identified, safety studies shall be performed to determine the adequacy of design concepts to meet the essential safety characteristics of the system. These studies also shall:

(a) Evaluate technical approaches to system safety design features.

(b) Identify possible safety interface problems.

(c) Highlight special areas of safety consideration, such as system limitations, risks, man-rating requirements.

(d) Define areas requiring further safety investigation and describe safety tests or data needed from exploratory or advanced development activities.

4.2.1.1 A preliminary hazard analysis (see 5.8.2.1) shall be performed as an integral part of the system concept studies to identify inherent hazards, or risks, associated with each design.

4.2.1.2 The contractor shall submit a summary statement of any additional safety design analysis, test, and demonstration requirements and recommendations resulting from these studies and analyses which are not already specified by the procuring activity.

4.2.2 Contract Definition

4.2.2.1 Contract Definition Phase (CDP) (Phase A). In his response to a Request for Proposal (RFP) for CDP, the contractor:

(a) Shall submit a preliminary SSPP (as a separate entity prepared in accordance with the requirements of the RFP. The SSPP shall describe the proposed integrated effort of how the contractor plans to conduct his system safety program to meet the requirements of the RFP, specifically:

(1) A firm proposal on the contractor's efforts and activities during the Contract Definition Phase (Phase B).

(2) A planning purpose proposal for evaluating the contractor's program for the Engineering Development Phase.

(b) Shall, in addition to preparing the SSPP:

(1) Perform necessary studies and analyses to define the system's safety technical specifications, performance requirements, and its operating safety characteristics. A preliminary hazard analysis (see 5.8.2.1) of the system in its intended operating environment shall be performed or revised to identify potential hazards and inherent risks. A system/subsystem/equipment safety interface study shall be performed to insure that compatibility between subsystem-equipment is maintained and safety is not degraded.

(2) Make tradeoff studies as necessary to reflect the impact on system safety requirements, and the identification of inherent risks and the required safety decisions.

(3) Identify and include in the appropriate specifications any resulting qualitative and quantitative requirements for the system, and subsystems including Government Furnished Equipment (GFE), and the proposed test plans to demonstrate their achievement.

(4) Submit a preliminary hazard analysis summary report which:

a. Identifies potential hazards and methods planned to eliminate or control them.

b. Outlines undefined areas requiring guidance or decisions.

c. Describes technical risks or problems in design. The contractor shall delineate the subsystem and component safety requirements for subcontractors and suppliers in order to meet the overall essential system safety requirements. The safety requirements for GFE and related data will be defined at this time and be submitted to the procuring activity for necessary action.

4.2.2.2 Contract Definition Phase (CDP) (Phase B). The contractor shall implement the SSPP as accepted or approved by the procuring activity. System safety studies shall be performed during system engineering, tradeoff studies and formulation of data requirements to insure that safety design requirements as identified in CDP Phase A are refined, updated and further expanded as necessary. Specifically the contractor will:

(a) Submit a firm SSPP for the Engineering Development Phase. This plan shall update the preliminary SSPP with a detailed description of activities, reviews, safety studies, analyses, and tests to be accomplished during the Engineering Development Phase. Also, the SSPP shall include the projected activities anticipated during the production and operational phases to accomplish the objectives of 4.2.4 and 4.2.5.

(b) Update the system safety studies, analyses, and test plans to define safety design requirements and criteria. System safety personnel shall participate in system tradeoff studies to insure that the highest degree of safety is achieved consistent with performance and system requirements.

(c) Update safety requirements in the system specifications and criteria.

(d) Submit a system safety work breakdown statement for the engineering development program.

4.2.3 Engineering Development Phase. The system safety program during this phase is an amplification and the implementation of the program defined in the previous phases. The action is predominantly on the part of the contractor with the responsible Department of Defense organization monitoring the program. System and subsystem hazards, and operating hazard analyses shall be evaluated in phase with program reviews. The contractor's system safety organization will insure effective and timely implementation of the approved SSPP. It is during the early phases of engineering design that the system safety program can be most effective with the least impact on schedules, and provide the greatest potential on cost saving. To provide support to the system engineering program, the system safety engineering activities shall include, but not be limited to the following:

(a) Furnishing safety design criteria; establishing safety objectives; and, reviewing preliminary engineering designs to identify hazards, methods of detection, and any required safety changes.

(b) Performing hazard analyses and safety studies to evaluate the system design.

(c) Establishing test requirements and insure that safety verification of design and data are included in the engineering test program.

(d) Participating in technical design and program reviews.

(e) Reviewing and providing inputs to preliminary system operator and maintenance publications, emergency procedures, etc.

(f) Evaluating results of failure analyses and accident investigations; recommending corrective action.

(g) Determining, evaluating, and providing safety considerations in tradeoff studies.

(h) Reviewing engineering documentation (drawings and specifications) to insure safety coverage.

(i) Identifying required safety and protective equipment and devices.

(j) Providing safety inputs to training courses.

4.2.4 Production Phase. The contractor shall identify critical production techniques, assembly procedures, facilities, testing and inspection requirements which affect system safety. Adequate procedures shall be invoked through the planned, controlled, and scheduled system quality control and monitoring specified contractually to insure that safety achieved in design is maintained during production. Corrective action shall be taken to eliminate, reduce or control hazards so identified. These corrections shall include necessary changes to engineering documentation. An audit shall be performed to identify any new system safety hazards which may result from the introduction of engineering changes. The impact of such changes on safety shall be evaluated to determine whether the previously established safety level of the system has been maintained; if not, redesign or change procedures shall be initiated to obtain the contracted level of safety.

4.2.5 Operational Phase (including disposal). The system safety program during the Operational Phase, and subsequent disposal, will include, but not be limited to the following functions:

(a) Operational safety review of system to determine if design, operating and maintenance procedures, and emergency procedures are adequate, based on user experience.

(b) Evaluation of design changes and modifications to operational equipment to insure inherent safety is not degraded.

(c) Continual review of operator and maintenance publication changes to insure that safety requirements, procedures, and cautions are adequate.

(d) Analyze system accidents/incidents or failures which caused, or could cause, an unsafe condition, and initiate corrective action.

(e) Data collection and analysis from system deficiency reports submitted by operating (user) personnel.

(f) Approval and application of procedures for disposal of hazardous material and equipment.

4.3 System safety organization. The contractor's organization shall be responsible for managing and performing the overall system safety program. The responsibilities and functions of those directly associated with system safety policies and implementation of the program shall be clearly defined. The authority delegated to this organization and the relationship between line, staff, and inter-departmental, project, functional, and general management organizations shall be identified. It is not the intent of this standard to prescribe or imply organizational structure, management methodology, implementation procedures, or internal documentation.

4.4 System safety program milestones. The system safety program shall be planned and scheduled to permit the contractor and the procuring activity to review its status, including the results achieved, at critical safety program checkpoints. These formal reviews and assessments of the system safety effort shall be performed concurrently with overall program milestones, such as requirements reviews, design reviews, and inspections. Safety milestones will be identified in a manner permitting evaluation of the effectiveness of the system safety effort. These milestones shall be presented in the SSPP and implemented as approved by the procuring activity.

5. DETAILED REQUIREMENTS

5.1 General. A system safety program is a formal approach to eliminate hazards through engineering, design, education, management policy, and supervisory control of conditions and practices. It insures the accomplishment of the system safety management and engineering tasks.

5.2 System Safety Program Plan (SSPP). The SSPP will be prepared in accordance with this standard and implemented as directed by the procuring activity. The SSPP, as approved by the procuring activity and incorporated into the contract, becomes the basis for contractual compliance. A sample SSPP outline is provided in Appendix A. When an integrating contractor is designated he will be responsible for the overall preparation, integration, and implementation of the SSPP. The plan shall describe an integrated effort within the total project, and shall include but not be limited to:

(a) Identification of system activities (i.e. design analyses, tests, demonstrations) specified elsewhere by the procuring activity and show how they will be used to preclude duplication.

(b) Providing specific information showing how the contractor will meet the safety requirements during development and manufacture including the design concepts to be utilized.

(c) The manner of demonstrating quantitative system safety requirements (if specified).

(d) A detailed listing of specific tasks.

(e) A current description of each task to be performed.

(f) Identification of the organization unit with the authority and responsibility for executing each task.

(g) The method of control to insure execution of each task.

(h) The scheduled start and completion dates of each task.

(i) Procedures for problem identification and solution.

(j) Procedures for recording and reporting status of actions to resolve problems.

(k) Method of assimilation and dissemination of system safety requirements to designers and associated personnel to expedite correction of known deficiencies.

(l) Designation of milestones, definitions or interrelationships, and estimation of personnel and man-hours required for system safety program activities and tasks.

(m) Periodic recording and reporting of predicted and achieved system and equipment safety.

(n) Delineate the safety data and analyses (including GFE) required of and to the integrating and associate contractors.

(o) Identification of special safety studies, research and test data.

(p) Safety data coordination flow.

(q) Range, flight, and operational test safety programs.

(r) The mathematical methods to be used; e.g. describe the appropriate models and analytical techniques to be employed.

5.3 Reviews.

5.3.1 Program and Design reviews. Safety shall be an integral part of all program and design reviews held for the system, subsystem, or equipment. System safety program reviews shall be conducted as part of the scheduled overall design and/or program reviews to assess the status of compliance with the overall safety program objectives. This review shall identify any deficiencies of the system with respect to safety and provide guidance for further development which may be required. The procuring activity shall be notified prior to each system safety program review, to permit participation by the safety organization of the procuring activity. Additional ad hoc safety reviews may be scheduled or required at the discretion of the contractor or the procuring

activity. Minutes of these system safety program reviews shall be recorded, and made available to the procuring activity.

5.4 System safety criteria and considerations.

5.4.1 General. System designs and operational procedures developed by each contractor should consider, but not be limited to, the following:

(a) Avoiding, eliminating or reducing significant hazards identified by analysis, design selection, material selection, or substitution. Composition of a propellant, explosive, hydraulic fluid, solvent, lubricant, or other hazardous material shall provide optimum safety characteristics.

(b) Controlling and minimizing hazards to personnel, equipment, and material which cannot be avoided or eliminated.

(c) Isolating hazardous substances, components, and operations from other activities, areas, personnel, and incompatible materials.

(d) Incorporating "fail-safe" principles where failures would disable the system or cause a catastrophe through injury to personnel, damage to equipment, or inadvertent operation of critical equipment.

(e) Locating equipment components so that access to them by personnel during operation, maintenance, repair, or adjustment shall not require exposure to hazards such as chemical burns, electrical shock, electromagnetic radiation, cutting edges, sharp points, or toxic atmospheres.

(f) Avoiding undue exposure of personnel to physiological and psychological stresses which might cause errors leading to mishaps.

(g) Providing suitable warning and caution notes in operations, assembly, maintenance, and repair instructions; and distinctive markings on hazardous components, equipment, or facilities for personnel protection. These shall be standardized in accordance with the requirements of the procuring activity.

(h) Designing to minimize damage by enemy action.

(i) Minimizing severe damage or injury to personnel and equipment in the event of an accident.

5.5 Hazard levels. The hazard levels, Category I (Negligible); Category II (Marginal); Category III (Critical); and Category IV (Catastrophic) as defined in section 3, shall be used as a qualitative measure of a system's hazards. These categories may be further defined by the procuring activity or by the contractor in the SSPP.

5.6 System safety precedence. Actions for satisfying safety requirements in order of precedence are specified below:

(a) Design for minimum hazard. The major effort throughout the design phases shall be to select appropriate safety design features; e.g. fail safe, redundancy.

(b) Safety devices. Known hazards which cannot be eliminated through design selection shall be reduced to an acceptable level through the use of appropriate safety devices.

(c) Warning devices. Where it is not possible to preclude the existence or occurrence of an identified hazard, devices shall be employed for the timely detection of the condition and the generation of an adequate warning signal. Warning signals and their application shall be designed to minimize the probability of incorrect personnel reaction to the signals, and shall be standardized within like types of systems, in accordance with the directives of the procuring activity.

(d) Special procedures. Where it is not possible to reduce the magnitude of an existing or potential hazard through design, or the use of safety and warning devices, the contractor shall develop special procedures. Precautionary notations shall be standardized in accordance with the directives of the procuring activity.

5.7 Design criteria/specifications. When design criteria specified by the procuring activity is proved inadequate in regards to safety, the contractor shall report the deficiency and recommend corrective actions with supporting evidence to the procuring activity.

5.8 Analyses. Analyses are performed to identify hazardous conditions for the purpose of their elimination or control. Analyses shall be made to examine the system, subsystems, components and their interrelationship to include logistic support, training, maintenance, and operational environments. The analyses shall be accomplished to do the following:

(a) Identify hazards and determine any needed corrective actions.

(b) Determine and evaluate safety considerations in tradeoff studies.

(c) Determine and evaluate appropriate safety design requirements.

(d) Determine and evaluate operational, test, and logistic safety requirements.

(e) Determine whether the qualitative objectives or quantitative numeric requirement established by the procuring activity have been achieved.

5.8.1 Qualitative or quantitative analysis. Qualitative and/or quantitative analyses will be performed as specified by the procuring activity. These analyses shall be revised when changes are made in components, subsystems, or total systems. The various types of hazard analyses are described below.

5.8.1.1 A qualitative analysis provides a technical assessment of the relative safety of a system design.

5.8.1.2 A quantitative analysis provides a numerical assessment of the relative safety of a system design. A quantitative analysis will determine:

(a) The probability of occurrence of critical or catastrophic hazards.
(b) The calculated system, subsystem, or equipment numeric requirement risk level.

5.8.2 System hazard analyses.

5.8.2.1 Preliminary hazard analysis. A preliminary hazard analysis shall be performed as the initial analysis task during the acquisition of a system. This analysis shall be a comprehensive, qualitative study. Such information shall be used in the development of safety criteria to be imposed in performance or design specifications. Areas to be considered shall include, but are not limited to the following:

(a) Isolation of energy sources.
(b) Fuels and propellants: their characteristics, hazard levels and quantity-distance constraints, handling, storage, transportation safety features, and compatibility factors.
(c) System environmental constraints.
(d) Use of explosive devices and their hazard constraints.
(e) Compatibility of materials.
(f) Effect of transient current, electrostatic discharges, electromagnetic radiation, and ionizing radiation to or by the system. Design of critical controls to prevent inadvertent activation and employment of electrical interlocks.
(g) Use of pressure vessels and associated plumbing, fittings, mountings, and hold-down devices.
(h) Crash safety.
(i) Safe operation and maintenance of the system.
(j) Training and certification pertaining to safe operation and maintenance of the system.
(k) Egress, rescue, survival, and salvage.
(l) Life support requirements and their safety implications in manned systems.
(m) Fire ignition and propagation sources and protection.
(n) Resistance to shock damage.
(o) Environmental factors such as equipment layout and lighting requirements and their safety implications in manual systems.
(p) Fail safe design considerations.
(q) Safety from a vulnerability and survivability standpoint; e.g., application of various types of personnel armor (metals, ceramics and glass), fire suppression systems, subsystems protection, and system redundancy.
(r) Protective clothing, equipment or devices.

(s) Lightning and electrostatic protection.
(t) Human error analysis of operator functions, tasks, and requirements.

5.8.2.2 Subsystem hazard analysis. This is an expansion of the preliminary hazard analysis. It shall be performed to determine, from a safety consideration, the functional relationships of components and equipments comprising each subsystem. Such analysis shall identify all components and equipments whose performance degradation or functional failure could result in hazardous conditions. The analysis should include a determination of the modes of failure and the effects on safety when failures occur in subsystem components.

5.8.2.3 System hazard analysis. The prime or integrating contractor shall conduct reviews or studies which define the safety integration and interface requirements of the total system. Analyses shall be performed of subsystem interfaces to determine the safety problem areas of the total system. Such analyses shall include, but not be limited to, review of subsystems interrelations for:

(a) Compliance with safety criteria.
(b) Possible independent, dependent, and simultaneous failures that could present a hazardous condition.
(c) Insuring that the normal operation of a subsystem cannot degrade the safety of another subsystem or the total system. When changes occur within subsystems, the system safety hazard analysis shall be changed accordingly. In the manned systems, consideration shall be given to crash safety, escape, egress, rescue, and survival.

5.8.2.4 Operating hazard analyses. Analyses shall be performed to determine safety requirements for personnel, procedures, and equipment used in installation, maintenance, support, testing, transportation, storage, operations, emergency escape, egress, rescue, and training during all phases of intended use as specified in the system requirements. Engineering data, procedures, and instructions developed from the engineering design and initial test programs shall be used in support of this effort. Results of these analyses shall provide the basis for:

(a) Design changes where feasible to eliminate hazards or provide safety devices, and safeguards.
(b) The warning, caution, special inspections and emergency procedures for operating and maintenance instructions including emergency action to minimize personnel injury.
(c) Identification of a hazardous period time span and actions required to preclude such hazards from occurring; and
(d) Special procedures for servicing, handling, storage and transportation.

5.9 Action on identified hazards. Action shall be taken to eliminate or minimize hazards revealed by analyses or related engineering efforts. Catastrophic and critical hazards shall be eliminated or controlled. If these hazards cannot be eliminated, or controlled to a specified probability of occurrence, the alternative controls will be immediately presented to the responsible procuring activity for resolution. Reporting shall be in accordance with the provisions of the System Safety Program Plan.

5.10 Supplier and subcontractor system safety program. Procedures shall be established to assure that the supplier and subcontractor system safety programs are consistent with overall system requirements. The contractor shall perform surveillance of the supplier and subcontractor system safety activities and insure adequate performance. Where the contractor and subcontractor determine that it is needed for satisfactory analyses, the contractor shall furnish in a timely manner sufficient system technical information to the subcontractor to enable the latter to consider system effects in a subsystem safety analysis.

6. DATA

6.1 Data requirements. The selected data requirements in support of this standard will be reflected in the Contractor Data Requirements List (DD Form 1423), attached to the request for proposal, invitation for bid, or the contract, as appropriate.

6.2 Data acceptance. Contractor-prepared data delivered in accordance with 6.1 to the procuring activity, shall be subject to review and approval by the procuring activity. In the absence of notification to the contrary within the time period specified in the contract, the data will be considered accepted. Non-delivered data shall be filed and maintained by the contractor for the duration of the contract period, but shall be made available for review and use by authorized representatives of the procuring activity upon request.

6.3 Acquisition and use of safety data. Safety data provided by the procuring activity should be used as a design aid to prevent repetitive design deficiencies. The contractor shall maintain liaison with other data sources to enable identification and evaluation of hazard and safety design deficiencies.

7. SAFETY TESTING

Tests shall be proposed in the SSPP to validate the safety of the product, including those tests already specified by the procuring activity. Safety tests shall be integrated into appropriate test plans. Where complete safety testing costs would be prohibitive, partial design verification of safety characteristics or procedures may be demonstrated by laboratory test, functional mock-ups or model simulation, when approved by the procuring activity.

Safety tests shall be performed on critical devices or components to determine the degree of hazard or margin of safety of design. Induced or simulated failures will be considered for demonstrating the failure mode of critical components. The detailed test plans for all tests shall be reviewed to insure that:

(a) Safety is adequately demonstrated.
(b) The testing will be carried out in a safe manner.
(c) All additional hazards introduced by testing procedures, instrumentation, test hardware, etc., are properly identified and minimized.

8. TRAINING

8.1 Safety Training for Operator and Maintenance Personnel. Safety information on approved methods and procedures will be included in instruction lesson plans and student examinations for the training of system (operator and maintenance) personnel. Protective devices and emergency equipment will be identified and included in training. Safety training aids, exhibits and displays may be used.

9. EFFECTS OF STORAGE, SHELF-LIFE, PACKAGING, TRANSPORTATION, HANDLING AND MAINTENANCE

The program shall consider, analyze, identify the effects of storage, shelf-life, packaging, transportation, handling and maintenance on the safety of the product. This shall include items such as:

(a) Identification of major or critical characteristics of safety significant items which deteriorate with age, environmental conditions, and other factors.
(b) Procedures for periodic field inspection or tests (including recall for test) of items to establish continuing acceptable levels of performance for parameters under test.
(c) Special safety procedures for maintenance or restoration.

10. INTEGRATION OF ASSOCIATED DISCIPLINES

10.1 Relationship to system engineering. Where the system engineering process is used as the mainstream engineering analysis effort, system safety requirements shall interface with the other engineering disciplines and tradeoff studies made in the interest of an optimum total system design.

Custodians:
Army - AV
Navy - AS

Preparing activity:
Air Force - 10

Reviewer activities:
Army - AV, AT, EL, WE, MU, MI
Air Force - 10
Navy - AS

Project No. MISC-0484

APPENDIX A

SYSTEM SAFETY PROGRAM PLAN OUTLINE

1. General
   - 1.1 Introduction
   - 1.2 Scope and purpose
   - 1.3 Application and implementation
   - 1.4 *Applicable documents*

2. Safety organization, responsibilities, and authority
   - 2.1 Integrating contractor organization and responsibilities
   - 2.2 Associate contractor organization and responsibilities
   - 2.3 Subcontractors responsibilities
   - 2.4 System safety working groups

3. System safety program milestones

4. System safety criteria
   - 4.1 Definitions
   - 4.2 *Hazard level categories*
   - 4.3 System safety precedence
   - 4.4 Special contractual requirements
   - 4.5 Identification and dissemination

5. System safety analyses
   - 5.1 Identification of analysis techniques
   - 5.2 *Qualitative and quantitative analyses*
   - 5.3 Preliminary hazard analysis
   - 5.4 Subsystem hazard analysis
   - 5.5 System hazard analysis
   - 5.6 Operating hazard analyses

6. Safety activities
   - 6.1 *Safety data*
     - 6.1.1 Identification of data requirements - deliverable and non-deliverable data
     - 6.1.2 Acquisition and use of safety data
       - 6.1.2.1 Hazard data collection
       - 6.1.2.2 Document tree and data flow
       - 6.1.2.3 Documentation and files
       - 6.1.2.4 Format for reports and data submittal
       - 6.1.2.5 Accident prevention, investigation, and reporting
       - 6.1.2.6 Safety reports
   - 6.2 Training
     - 6.2.1 *Crew qualification, training and certification*
     - 6.2.2 Maintenance personnel training and qualification

*U.S. GOVERNMENT PRINTING OFFICE: 1969-393-088/5191

7. Audit program
8. Ground handling, storage, servicing and transportation
9. Facilities and support requirements
10. Other system safety matters (not otherwise covered)