DEPARTMENT OF DEFENSE

STANDARD PRACTICE FOR
SYSTEM SAFETY

AMSC N/A   **AREA SAFT**

MIL-STD-882D

FOREWORD

1. This standard is approved for use by all Departments and Agencies within the Department of Defense (DoD).

2. The DoD is committed to protecting: private and public personnel from accidental death, injury, or occupational illness; weapon systems, equipment, material, and facilities from accidental destruction or damage; and public property while executing its mission of national defense. Within mission requirements, the DoD will also ensure that the quality of the environment is protected to the maximum extent practical. The DoD has implemented environmental, safety, and health efforts to meet these objectives. Integral to these efforts is the use of a system safety approach to manage the risk of mishaps associated with DoD operations. A key objective of the DoD system safety approach is to include mishap risk management consistent with mission requirements, in technology development by design for DoD systems, subsystems, equipment, facilities, and their interfaces and operation. The DoD goal is zero mishaps.

3. This standard practice addresses an approach (a standard practice normally identified as system safety) useful in the management of environmental, safety, and health mishap risks encountered in the development, test, production, use, and disposal of DoD systems, subsystems, equipment, and facilities. The approach described herein conforms to the acquisition procedures in DoD Regulation 5000.2-R and provides a consistent means of evaluating identified mishap risks. Mishap risk must be identified, evaluated, and mitigated to a level acceptable (as defined by the system user or customer) to the appropriate authority, and compliant with federal laws and regulations, Executive Orders, treaties, and agreements. Program trade studies associated with mitigating mishap risk must consider total life cycle cost in any decision. Residual mishap risk associated with an individual system must be reported to and accepted by the appropriate authority as defined in DoD Regulation 5000.2-R. When MIL-STD-882 is required in a solicitation or contract and no specific references are included, then only those requirements presented in section 4 are applicable.

4. This revision applies the tenets of acquisition reform to system safety in Government procurement. A joint Government/Industrial process team oversaw this revision. The Government Electronic and Information Technology Association (GEIA), G-48 committee on system safety represented industry on the process action team. System safety information (e.g., system safety tasks, commonly used approaches, etc.) associated with previous versions of this standard are in the *Defense Acquisition Deskbook* (see 6.8). This standard practice is no longer the source for any safety-related data item descriptions (DIDs).

5. Address beneficial comments (recommendations, additions, and deletions) and any pertinent information that may be of use in improving this document to: HQ Air Force Materiel Command (SES), 4375 Chidlaw Road, Wright-Patterson AFB, OH 45433-5006. Use the Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter or electronic mail.

MIL-STD-882D

CONTENTS

MIL-STD-882D

TABLES

iv

MIL-STD-882D

1. SCOPE

1.1 <u>Scope</u>. This document outlines a standard practice for conducting system safety.

The system safety practice as defined herein conforms to the acquisition procedures in DoD Regulation 5000.2-R and provides a consistent means of evaluating identified risks. Mishap risk must be identified, evaluated, and mitigated to a level acceptable (as defined by the system user or customer) to the appropriate authority and compliant with federal (and state where applicable) laws and regulations, Executive Orders, treaties, and agreements. Program trade studies associated with mitigating mishap risk must consider total life cycle cost in any decision. When requiring MIL-STD-882 in a solicitation or contract and no specific paragraphs of this standard are identified, then apply only those requirements presented in section 4.

2. APPLICABLE DOCUMENTS

Sections 3, 4, and 5 of this standard contain no applicable documents. This section does not include documents cited in other sections of this standard or recommended for additional information or as examples.

3. DEFINITIONS

3.1 <u>Acronyms used in this standard</u>. The acronyms used in this standard are defined as follows:

a.	AMSDL	Acquisition Management System & Data Requirement List
b.	ANSI	American National Standard Institute
c.	DID	Data Item Description
d.	DoD	Department of Defense
e.	ESH	Environmental, Safety, and Health
f.	GEIA	Government Electronic & Information Technology Association
g.	MAIS	Major Automated Information System
h.	MDAP	Major Defense Acquisition Program
i.	USAF	United States Air Force

3.2 <u>Definitions</u>. Within this document, the following definitions apply (see 6.4):

3.2.1 <u>Acquisition program</u>. A directed, funded effort designed to provide a new, improved, or continuing system in response to a validated operational need.

3.2.2 <u>Developer</u>. The individual or organization assigned responsibility for a development effort. Developers can be either internal to the government or contractors.

3.2.3 <u>Hazard</u>. Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment.

1

3.2.4 <u>Hazardous material</u>. Any substance that, due to its chemical, physical, or biological nature, causes safety, public health, or environmental concerns that would require an elevated level of effort to manage.

3.2.5 <u>Life cycle</u>. All phases of the system's life including design, research, development, test and evaluation, production, deployment (inventory), operations and support, and disposal.

3.2.6 <u>Mishap</u>. An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

3.2.7 <u>Mishap risk</u>. An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence.

3.2.8 <u>Program Manager (PM)</u>. A government official who is responsible for managing an acquisition program. Also, a general term of reference to those organizations directed by individual managers, exercising authority over the planning, direction, and control of tasks and associated functions essential for support of designated systems. This term will normally be used in lieu of any other titles, e.g.; system support manager, weapon program manager, system manager, and project manager.

3.2.9 <u>Residual mishap risk</u>. The remaining mishap risk that exists after all mitigation techniques have been implemented or exhausted, in accordance with the system safety design order of precedence (see 4.4).

3.2.10 <u>Safety</u>. Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

3.2.11 <u>Subsystem</u>. A grouping of items satisfying a logical group of functions within a particular system.

3.2.12 <u>System</u>. An integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective.

3.2.13 <u>System safety</u>. The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.

3.2.14 <u>System safety engineering</u>. An engineering discipline that employs specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated mishap risk.

MIL-STD-882D

4. GENERAL REQUIREMENTS

This section defines the system safety requirements to perform throughout the life cycle for any system, new development, upgrade, modification, resolution of deficiencies, or technology development. When properly applied, these requirements should ensure the identification and understanding of all known hazards and their associated risks; and mishap risk eliminated or reduced to acceptable levels. The objective of system safety is to achieve acceptable mishap risk through a systematic approach of hazard analysis, risk assessment, and risk management. This document delineates the minimum mandatory requirements for an acceptable system safety program for any DoD system. When MIL-STD-882 is required in a solicitation or contract, but no specific references are included, then only the requirements in this section are applicable. System safety requirements consist of the following:

4.1 <u>Documentation of the system safety approach</u>. Document the developer's and program manager's approved system safety engineering approach. This documentation shall:

a. Describe the program's implementation using the requirements herein. Include identification of each hazard analysis and mishap risk assessment process used.

b. Include information on system safety integration into the overall program structure.

c. Define how hazards and residual mishap risk are communicated to and accepted by the appropriate risk acceptance authority (see 4.7) and how hazards and residual mishap risk will be tracked (see 4.8).

4.2 <u>Identification of hazards</u>. Identify hazards through a systematic hazard analysis process encompassing detailed analysis of system hardware and software, the environment (in which the system will exist), and the intended use or application. Consider and use historical hazard and mishap data, including lessons learned from other systems. Identification of hazards is a responsibility of all program members. During hazard identification, consider hazards that could occur over the system life cycle.

4.3 <u>Assessment of mishap risk</u>. Assess the severity and probability of the mishap risk associated with each identified hazard, i.e., determine the potential negative impact of the hazard on personnel, facilities, equipment, operations, the public, and the environment, as well as on the system itself. The tables in Appendix A are to be used unless otherwise specified.

4.4 <u>Identification of mishap risk mitigation measures</u>. Identify potential mishap risk mitigation alternatives and the expected effectiveness of each alternative or method. Mishap risk mitigation is an iterative process that culminates when the residual mishap risk has been reduced to a level acceptable to the appropriate authority. The system safety design order of precedence for mitigating identified hazards is:

a. <u>Eliminate hazards through design selection.</u> If unable to eliminate an identified hazard, reduce the associated mishap risk to an acceptable level through design selection.

3

b. Incorporate safety devices. If unable to eliminate the hazard through design selection, reduce the mishap risk to an acceptable level using protective safety features or devices.

c. Provide warning devices. If safety devices do not adequately lower the mishap risk of the hazard, include a detection and warning system to alert personnel to the particular hazard.

d. Develop procedures and training. Where it is impractical to eliminate hazards through design selection or to reduce the associated risk to an acceptable level with safety and warning devices, incorporate special procedures and training. Procedures may include the use of personal protective equipment. For hazards assigned Catastrophic or Critical mishap severity categories, avoid using warning, caution, or other written advisory as the only risk reduction method.

4.5 Reduction of mishap risk to an acceptable level. Reduce the mishap risk through a mitigation approach mutually agreed to by both the developer and the program manager. Communicate residual mishap risk and hazards to the associated test effort for verification.

4.6 Verification of mishap risk reduction. Verify the mishap risk reduction and mitigation through appropriate analysis, testing, or inspection. Document the determined residual mishap risk. Report all new hazards identified during testing to the program manager and the developer.

4.7 Review of hazards and acceptance of residual mishap risk by the appropriate authority. Notify the program manager of identified hazards and residual mishap risk. Unless otherwise specified, the suggested tables A-I through A-III of the appendix will be used to rank residual risk. The program manager shall ensure that remaining hazards and residual mishap risk are reviewed and accepted by the appropriate risk acceptance authority (ref. table A-IV). The appropriate risk acceptance authority will include the system user in the mishap risk review. The appropriate risk acceptance authority shall formally acknowledge and document acceptance of hazards and residual mishap risk.

4.8 Tracking of hazards, their closures, and residual mishap risk. Track hazards, their closure actions, and the residual mishap risk. Maintain a tracking system that includes hazards, their closure actions, and residual mishap risk throughout the system life cycle. The program manager shall keep the system user advised of the hazards and residual mishap risk.

5. DETAILED REQUIREMENTS

Program managers shall identify in the solicitation and system specification any specific system safety engineering requirements including risk assessment and acceptance, unique classifications and certifications (see 6.6 and 6.7), or any mishap reduction needs unique to their program. Additional information in developing program specific requirements is located in Appendix A.

MIL-STD-882D

6. NOTES

(This section contains information of a general or explanatory nature that may be helpful, but is not mandatory.)

6.1 <u>Intended use</u>. This standard establishes a common basis for expectations of a properly executed system safety effort.

6.2 <u>Data requirements</u>. Hazard analysis data may be obtained from contracted sources by citing DI-MISC-80508, Technical Report - Study/Services. When it is necessary to obtain data, list the applicable Data Item Descriptions (DIDs) on the Contract Data Requirements List (DD Form 1423), except where the DoD Federal Acquisition Regulation Supplement exempts the requirement for a DD Form 1423. The developer and the program manager are encouraged to negotiate access to internal development data when hard copies are not necessary. They are also encouraged to request that any type of safety plan required to be provided by the contractor, be submitted with the proposal. It is further requested that any of the below listed data items be condensed into the statement of work and the resulting data delivered in one general type scientific report.

Current DIDs, that may be applicable to a system safety effort (check DoD 5010.12-L, Acquisition Management Systems and Data Requirements Control List (AMSDL) for the most current version before using), include:

DID Number	DID Title
DI-MISC-80043	Ammunition Data Card
DI-SAFT-80101	System Safety Hazard Analysis Report
DI-SAFT-80102	Safety Assessment Report
DI-SAFT-80103	Engineering Change Proposal System Safety Report
DI-SAFT-80104	Waiver or Deviation System Safety Report
DI-SAFT-80105	System Safety Program Progress Report
DI-SAFT-80106	Occupational Health Hazard Assessment
DI-SAFT-80184	Radiation Hazard Control Procedures
DI-MISC-80508	Technical Report - Study Services
DI SAFT-80931	Explosive Ordnance Disposal Data
DI-SAFT-81065	Safety Studies Report
DI-SAFT-81066	Safety Studies Plan
DI-ADMN-81250	Conference Minutes
DI-SAFT-81299	Explosive Hazard Classification Data
DI-SAFT-81300	Mishap Risk Assessment Report
DI-ILSS-81495	Failure Mode, Effects, Criticality Analysis Report

MIL-STD-882D

6.3 <u>Subject term (key word) listing</u>.

Environmental
Hazard
Mishap
Mishap probability levels
Mishap risk
Mishap severity categories
Occupational Health
Residual mishap risk
System safety engineering

6.4 <u>Definitions used in this standard</u>. The definitions at 3.2 may be different from those used in other specialty areas. One must carefully check the specific definition of a term in question for its area of origination before applying the approach described in this document.

6.5 <u>International standardization agreements</u>. Certain provisions of this standard are the subject of international standardization agreements (AIR STD 20/23B, *Safety Design Requirements for Airborne Dispenser Weapons*, and STANAG No. 3786, *Safety Design Requirements for Airborne Dispenser Weapons*). When proposing amendment, revision, or cancellation of this standard that might modify the international agreement concerned, the preparing activity will take appropriate action through international standardization channels, including departmental standardization offices, to change the agreement or make other appropriate accommodations.

6.6 <u>Explosive hazard classification and characteristic data</u>. Any new or modified item of munitions or of an explosive nature that will be transported to or stored at a DoD installation or facility must first obtain an interim or final explosive hazard classification. The system safety effort should provide the data necessary for the program manager to obtain the necessary classification(s). These data should include identification of safety hazards involved in handling, shipping, and storage related to production, use, and disposal of the item.

6.7 <u>Use of system safety data in certification and other specialized safety approvals</u>. Hazard analyses are often required for many related certifications and specialized reviews. Examples of activities requiring data generated during a system safety effort include:
  a. Federal Aviation Agency airworthiness certification of designs and modifications
  b. DoD airworthiness determination
  c. Nuclear and non-nuclear munitions certification
  d. Flight readiness reviews
  e. Flight test safety review board reviews
  f. Nuclear Regulatory Commission licensing
  g. Department of Energy certification
  Special safety-related approval authorities include USAF Radioisotope Committee, Weapon System Explosive Safety Review Board (Navy), Non-Nuclear Weapons and Explosives Safety Board (NNWESB), Army Fuze Safety Review Board, Triservice Laser Safety Review

6

Board, and the DoD Explosive Safety Board. Acquisition agencies should ensure that appropriate service safety agency approvals are obtained prior to use of new or modified weapons systems in an operational or test environment.

6.8 <u>DoD acquisition practices</u>. Information on DoD acquisition practices is presented in the *Defense Acquisition Deskbook* available from the Deskbook Joint Program Office, Wright-Patterson Air Force Base, Ohio. Nothing in the referenced information is considered additive to the requirements provided in this standard.

6.9 <u>Identification of changes</u>. Due to the extent of the changes, marginal notations are not used in this revision to identify changes with respect to the previous issue.

MIL-STD-882D
APPENDIX A

GUIDANCE FOR IMPLEMENTATION OF
A SYSTEM SAFETY EFFORT

A.1 SCOPE

A.1.1 Scope. This appendix provides rationale and guidance to fit the needs of most system safety efforts. It includes further explanation of the effort and activities available to meet the requirements described in section 4 of this standard. This appendix is not a mandatory part of this standard and is not to be included in solicitations by reference. However, program managers may extract portions of this appendix for inclusion in requirement documents and solicitations.

A.2 APPLICABLE DOCUMENTS

A.2.1 General. The documents listed in this section are referenced in sections A.3, A.4, and A.5. This section does not include documents cited in other sections of this appendix or recommended for additional information or as examples.

A.2.2 Government documents.

A.2.2.1 Specifications, standards, and handbooks. This section is not applicable to this appendix.

A.2.2.2 Other Government documents, drawings, and publications. The following other Government document forms a part of this document to the extent specified herein. Unless otherwise specified, the issue is that cited in the solicitation.

DoD 5000.2-R   Mandatory Procedures for Major Defense Acquisition
                                      Programs (MDAPs) and Major Automated Information
                                      System (MAIS) Acquisition Programs

(Copies of DoD 5000.2-R are available from the Washington Headquarters Services, Directives and Records Branch (Directives Section), Washington, DC or from the DoD Acquisition Deskbook).

A.2.3 Non-Government publications. This section is not applicable to this appendix.

A.2.4 Order of precedence. Since this appendix is not mandatory, in event of a conflict between the text of this appendix and the reference cited herein, the text of the reference takes precedence. Nothing in this appendix supersedes applicable laws and regulations unless a specific exemption has been obtained.

MIL-STD-882D
APPENDIX A

A.3 DEFINITIONS

A.3.1 <u>Acronyms used in this appendix</u>. No additional acronyms are used in this appendix.

A.3.2 <u>Definitions</u>. Additional definitions that apply to this appendix:

A.3.2.1 <u>Development agreement</u>. The formal documentation of the agreed-upon tasks that the developer will execute for the program manager. For a commercial developer, this agreement usually is in the form of a written contract.

A.3.2.2 <u>Fail-safe</u>. A design feature that ensures the system remains safe, or in the event of a failure, causes the system to revert to a state that will not cause a mishap.

A.3.2.3 <u>Health hazard assessment</u>. The application of biomedical knowledge and principles to identify and eliminate or control health hazards associated with systems in direct support of the life-cycle management of materiel items.

A.3.2.4 <u>Mishap probability</u>. The aggregate probability of occurrence of the individual events/hazards that might create a specific mishap.

A.3.2.5 <u>Mishap probability levels</u>. An arbitrary categorization that provides a qualitative measure of the most reasonable likelihood of occurrence of a mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction.

A.3.2.6 <u>Mishap risk assessment</u>. The process of characterizing hazards within risk areas and critical technical processes, analyzing them for their potential mishap severity and probabilities of occurrence, and prioritizing them for risk mitigation actions.

A.3.2.7 <u>Mishap risk categories</u>. An arbitrary categorization of mishap risk assessment values often used to generate specific action such as mandatory reporting of certain hazards to management for action, or formal acceptance of the associated mishap risk.

A.3.2.8 <u>Mishap severity</u>. An assessment of the consequences of the most reasonable credible mishap that could be caused by a specific hazard.

A.3.2.9 <u>Mishap severity category</u>. An arbitrary categorization that provides a qualitative measure of the most reasonable credible mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction.

A.3.2.10 <u>Safety critical</u>. A term applied to any condition, event, operation, process, or item whose proper recognition, control, performance, or tolerance is essential to safe system operation and support (e.g., safety critical function, safety critical path, or safety critical component).

9

MIL-STD-882D
APPENDIX A

A.3.2.11 <u>System safety management</u>. All plans and actions taken to identify, assess, mitigate, and continuously track, control, and document environmental, safety, and health mishap risks encountered in the development, test, acquisition, use, and disposal of DoD weapon systems, subsystems, equipment, and facilities.

A.4 GENERAL REQUIREMENTS

A.4.1 <u>General</u>. System safety applies engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness, time, and cost, throughout all phases of the system life cycle. It draws upon professional knowledge and specialized skills in the mathematical, physical, and scientific disciplines, together with the principles and methods of engineering design and analysis, to specify and evaluate the environmental, safety, and health mishap risk associated with a system. Experience indicates that the degree of safety achieved in a system is directly dependent upon the emphasis given. The program manager and the developer must apply this emphasis during all phases of the system's life cycle. A safe design is a prerequisite for safe operations, with the goal being to produce an inherently safe product that will have the minimum safety-imposed operational restrictions.

A.4.1.1 <u>System safety in environmental and health hazard management</u>. DoD 5000.2-R has directed the integration of environmental, safety, and health hazard management into the systems engineering process. While environmental and health hazard management are normally associated with the application of statutory direction and requirements, the management of mishap risk associated with actual environmental and health hazards is directly addressed by the system safety approach. Therefore, environmental and health hazards can be analyzed and managed with the same tools as any other hazard, whether they affect equipment, the environment, or personnel.

A.4.2 <u>Purpose (see 1.1)</u>. All DoD program managers shall establish and execute programs that manage the probability and severity of all hazards for their systems (DoD 5000.2-R). Provision for system safety requirements and effort as defined by this standard should be included in all applicable contracts negotiated by DoD. These contracts include those negotiated within each DoD agency, by one DoD agency for another, and by DoD for other Government agencies. In addition, each DoD in-house program will address system safety.

A.4.2.1 <u>Solicitations and contracts</u>. Apply the requirements of section 4 to acquisitions. Incorporate MIL-STD-882 in the list of contractual compliance documents, and include the potential of a developer to execute section 4 requirements as source selection evaluation criteria. Developers are encouraged to submit with their proposal a preliminary plan that describes the system safety effort required for the requested program. When directed by the program manager, attach this preliminary plan to the contract or reference it within the statement of work; so it becomes the basis for a contractual system safety program.

A.4.3 <u>System safety planning</u>. Before formally documenting the system safety approach, the program manager, in concert with systems engineering and associated system safety

professionals, must determine what system safety effort is necessary to meet program and regulatory requirements. This effort will be built around the requirements set forth in section 4 and includes developing a planned approach for safety task accomplishment, providing qualified people to accomplish the tasks, establishing the authority for implementing the safety tasks through all levels of management, and allocating appropriate resources to ensure that the safety tasks are completed.

A.4.3.1 <u>System safety planning subtasks</u>. System safety planning subtasks should:

a. Establish specific safety performance requirements (see A.4.3.2) based on overall program requirements and system user inputs.

b. Establish a system safety organization or function and the required lines of communication with associated organizations (government and contractor). Establish interfaces between system safety and other functional elements of the program, as well as with other safety and engineering disciplines (such as nuclear, range, explosive, chemical, and biological). Designate the organizational unit responsible for executing each safety task. Establish the authority for resolution of identified hazards.

c. Establish system safety milestones and relate these to major program milestones, program element responsibility, and required inputs and outputs.

d. Establish an incident alerting/notification, investigation, and reporting process, to include notification of the program manager.

e. Establish an acceptable level of mishap risk, mishap probability and severity thresholds, and documentation requirements (including but not limited to hazards and residual mishap risk).

f. Establish an approach and methodology for reporting to the program manager the following minimum information:

(1) Safety critical characteristics and features.

(2) Operating, maintenance, and overhaul safety requirements.

(3) Measures used to eliminate or mitigate hazards.

(4) Acquisition management of hazardous materials.

g. Establish the method for the formal acceptance and documenting of residual mishap risks and the associated hazards.

h. Establish the method for communicating hazards, the associated risks, and residual mishap risk to the system user.

MIL-STD-882D
APPENDIX A

i. Specify requirements for other specialized safety approvals (e.g., nuclear, range, explosive, chemical, biological, electromagnetic radiation, and lasers) as necessary (reference 6.6 and 6.7).

A.4.3.2 <u>Safety performance requirements</u>. These are the general safety requirements needed to meet the core program objectives. The more closely these requirements relate to a given program, the more easily the designers can incorporate them into the system. In the appropriate system specifications, incorporate the safety performance requirements that are applicable, and the specific risk levels considered acceptable for the system. Acceptable risk levels can be defined in terms of: a hazard category developed through a mishap risk assessment matrix; an overall system mishap rate; demonstration of controls required to preclude unacceptable conditions; satisfaction of specified standards and regulatory requirements; or other suitable mishap risk assessment procedures. Listed below are examples of safety performance statements.

a. <u>Quantitative requirements</u>. Quantitative requirements are usually expressed as a failure or mishap rate, such as "The catastrophic system mishap rate shall not exceed x.xx X 10^{-y} per operational hour."

b. <u>Mishap risk requirements</u>. Mishap risk requirements could be expressed as "No hazards assigned a Catastrophic mishap severity are acceptable." Mishap risk requirements could also be expressed as a level defined by a mishap risk assessment (see A.4.4.3.2.3), such as "No Category 3 or higher mishap risks are acceptable."

c. <u>Standardization requirements</u>. Standardization requirements are expressed relative to a known standard that is relevant to the system being developed. Examples include: "The system will comply with the laws of the State of XXXXX and be operable on the highways of the State of XXXXX" or "The system will be designed to meet ANSI Std XXX as a minimum."

A.4.3.3 <u>Safety design requirements</u>. The program manager, in concert with the chief engineer and utilizing systems engineering and associated system safety professionals, should establish specific safety design requirements for the overall system. The objective of safety design requirements is to achieve acceptable mishap risk through a systematic application of design guidance from standards, specifications, regulations, design handbooks, safety design checklists, and other sources. Review these for safety design parameters and acceptance criteria applicable to the system. Safety design requirements derived from the selected parameters, as well as any associated acceptance criteria, are included in the system specification. Expand these requirements and criteria for inclusion in the associated follow-on or lower level specifications. See general safety system design requirements below.

a. Hazardous material use is minimized, eliminated, or associated mishap risks are reduced through design, including material selection or substitution. When using potentially hazardous materials, select those materials that pose the least risk throughout the life cycle of the system.

12

b. Hazardous substances, components, and operations are isolated from other activities, areas, personnel, and incompatible materials.

c. Equipment is located so that access during operations, servicing, repair, or adjustment minimizes personnel exposure to hazards (e.g., hazardous substances, high voltage, electromagnetic radiation, and cutting and puncturing surfaces).

d. Protect power sources, controls, and critical components of redundant subsystems by physical separation or shielding, or by other acceptable methods.

f. Consider safety devices that will minimize mishap risk (e.g., interlocks, redundancy, fail safe design, system protection, fire suppression, and protective measures such as clothing, equipment, devices, and procedures) for hazards that cannot be eliminated. Make provisions for periodic functional checks of safety devices when applicable.

g. System disposal (including explosive ordnance disposal) and demilitarization are considered in the design.

h. Implement warning signals to minimize the probability of incorrect personnel reaction to those signals, and standardize within like types of systems.

i. Provide warning and cautionary notes in assembly, operation, and maintenance instructions; and provide distinctive markings on hazardous components, equipment, and facilities to ensure personnel and equipment protection when no alternate design approach can eliminate a hazard. Use standard warning and cautionary notations where multiple applications occur. Standardize notations in accordance with commonly accepted commercial practice or, if none exists, normal military procedures. Do not use warning, caution, or other written advisory as the <u>only</u> risk reduction method for hazards assigned to Catastrophic or Critical mishap severity categories.

j. Safety critical tasks may require personnel proficiency; if so, the developer should propose a proficiency certification process to be used.

k. Severity of injury or damage to equipment or the environment as a result of a mishap is minimized.

l. Inadequate or overly restrictive requirements regarding safety are not included in the system specification.

m. Acceptable risk is achieved in implementing new technology, materials, or designs in an item's production, test, and operation. Changes to design, configuration, production, or mission requirements (including any resulting system modifications and upgrades, retrofits, insertions of new technologies or materials, or use of new production or test techniques) are accomplished in a manner that maintains an acceptable level of mishap risk. Changes to the environment in which the system operates are analyzed to identify and mitigate any resulting hazards or changes in mishap risks.

13

MIL-STD-882D
APPENDIX A

A.4.3.3.1 Some program managers include the following conditions in their solicitation, system specification, or contract as requirements for the system design. These condition statements are used optionally as supplemental requirements based on specific program needs.

A.4.3.3.1.1 <u>Unacceptable conditions</u>. The following safety critical conditions are considered unacceptable for development efforts. Positive action and verified implementation is required to reduce the mishap risk associated with these situations to a level acceptable to the program manager.

a. Single component failure, common mode failure, human error, or a design feature that could cause a mishap of Catastrophic or Critical mishap severity catagories.

b. Dual independent component failures, dual independent human errors, or a combination of a component failure and a human error involving safety critical command and control functions, which could cause a mishap of Catastrophic or Critical mishap severity catagories.

c. Generation of hazardous radiation or energy, when no provisions have been made to protect personnel or sensitive subsystems from damage or adverse effects.

d. Packaging or handling procedures and characteristics that could cause a mishap for which no controls have been provided to protect personnel or sensitive equipment.

e. Hazard categories that are specified as unacceptable in the development agreement.

A.4.3.3.1.2 <u>Acceptable conditions</u>. The following approaches are considered acceptable for correcting unacceptable conditions and will require no further analysis once mitigating actions are implemented and verified.

a. For non-safety critical command and control functions: a system design that requires two or more independent human errors, or that requires two or more independent failures, or a combination of independent failure and human error.

b. For safety critical command and control functions: a system design that requires at least three independent failures, or three independent human errors, or a combination of three independent failures and human errors.

c. System designs that positively prevent errors in assembly, installation, or connections that could result in a mishap.

d. System designs that positively prevent damage propagation from one component to another or prevent sufficient energy propagation to cause a mishap.
e. System design limitations on operation, interaction, or sequencing that preclude occurrence of a mishap.

14

f. System designs that provide an approved safety factor, or a fixed design allowance that limits, to an acceptable level, possibilities of structural failure or release of energy sufficient to cause a mishap.

g. System designs that control energy build-up that could potentially cause a mishap (e.g., fuses, relief valves, or electrical explosion proofing).

h. System designs where component failure can be temporarily tolerated because of residual strength or alternate operating paths, so that operations can continue with a reduced but acceptable safety margin.

i. System designs that positively alert the controlling personnel to a hazardous situation where the capability for operator reaction has been provided.

j. System designs that limit or control the use of hazardous materials.

A.4.3.4 Elements of an effective system safety effort. Elements of an effective system safety effort include:

a. Management is always aware of the mishap risks associated with the system, and formally documents this awareness. Hazards associated with the system are identified, assessed, tracked, monitored, and the associated risks are either eliminated or controlled to an acceptable level throughout the life cycle. Identify and archive those actions taken to eliminate or reduce mishap risk for tracking and lessons learned purposes.

b. Historical hazard and mishap data, including lessons learned from other systems, are considered and used.

c. Environmental protection, safety, and occupational health, consistent with mission requirements, are designed into the system in a timely, cost-effective manner. Inclusion of the appropriate safety features is accomplished during the applicable phases of the system life cycle.

d. Mishap risk resulting from harmful environmental conditions (e.g., temperature, pressure, noise, toxicity, acceleration, and vibration) and human error in system operation and support is minimized.

e. System users are kept abreast of the safety of the system and included in the safety decision process.

A.4.4 System safety engineering effort. As stated in section 4, a system safety engineering effort consists of eight main requirements. The following paragraphs provide further descriptions on what efforts are typically expected due to each of the system safety requirements listed in section 4.

A.4.4.1 Documentation of the system safety approach. The documentation of the system safety approach should describe the planned tasks and activities of system safety management

and system engineering required to identify, evaluate, and eliminate or control hazards, or to reduce the residual mishap risk to a level acceptable throughout the system life cycle. The documentation should describe, as a minimum, the four elements of an effective system safety effort: a planned approach for task accomplishment, qualified people to accomplish tasks, the authority to implement tasks through all levels of management, and the appropriate commitment of resources (both manning and funding) to ensure that safety tasks are completed. Specifically, the documentation should:

a. Describe the scope of the overall system program and the related system safety effort. Define system safety program milestones. Relate these to major program milestones, program element responsibility, and required inputs and outputs.

b. Describe the safety tasks and activities of system safety management and engineering. Describe the interrelationships between system safety and other functional elements of the program. List the other program requirements and tasks applicable to system safety and reference where they are specified or described. Include the organizational relationships between other functional elements having responsibility for tasks with system safety impacts and the system safety management and engineering organization including the review and approval authority of those tasks.

c. Describe specific analysis techniques and formats to be used in qualitative or quantitative assessments of hazards, their causes, and effects.

d. Describe the process through which management decisions will be made (for example, timely notification of unacceptable risks, necessary action, incidents or malfunctions, waivers to safety requirements, and program deviations). Include a description on how residual mishap risk is formally accepted and this acceptance is documented.

e. Describe the mishap risk assessment procedures, including the mishap severity categories, mishap probability levels, and the system safety design order of precedence that should be followed to satisfy the safety requirements of the program. State any qualitative or quantitative measures of safety to be used for mishap risk assessment including a description of the acceptable and unacceptable risk levels (if applicable). Include system safety definitions that modify, deviate from, or are in addition to those in this standard or generally accepted by the system safety community (see *Defense Acquisition Deskbook* and System Safety Society's *System Safety Analysis Handbook)* (see A.6.1).

f. Describe how resolution and action relative to system safety will be implemented at the program management level possessing resolution authority.

g. Describe the verification (e.g., test, analysis, demonstration, or inspection) requirements for ensuring that safety is adequately attained. Identify any certification requirements for software, safety devices, or other special safety features (e.g., render safe and emergency disposal procedures).

h. Describe the mishap or incident notification, investigation, and reporting process for the program, including notification of the program manager.

i. Describe the approach for collecting and processing pertinent historical hazard, mishap, and safety lessons learned data. Include a description on how a system hazard log is developed and kept current (see A.4.4.8.1).

j. Describe how the user is kept abreast of residual mishap risk and the associated hazards.

A.4.4.2 <u>Identification of hazards</u>. Identify hazards through a systematic hazard analysis process encompassing detailed analysis of system hardware and software, the environment (in which the system will exist), and the intended usage or application. Historical hazard and mishap data, including lessons learned from other systems, are considered and used.

A.4.4.2.1 <u>Approaches for identifying hazards</u>. Numerous approaches have been developed and used to identify system hazards. A key aspect of many of these approaches is empowering the design engineer with the authority to design safe systems and the responsibility to identify to program management the hazards associated with the design. Hazard identification approaches often include using system users in the effort. Commonly used approaches for identifying hazards can be found in the *Defense Acquisition Deskbook* and System Safety Society's *System Safety Analysis Handbook* (see A.6.1)

A.4.4.3 <u>Assessment of mishap risk</u>. Assess the severity and probability of the mishap risk associated with each identified hazard, i.e., determine the potential impact of the hazard on personnel, facilities, equipment, operations, the public, or environment, as well as on the system itself. Other factors, such as numbers of persons exposed, may also be used to assess risk.

A.4.4.3.1 <u>Mishap risk assessment tools</u>. To determine what actions to take to eliminate or control identified hazards, a system of determining the level of mishap risk involved must be developed. A good mishap risk assessment tool will enable decision makers to properly understand the level of mishap risk involved, relative to what it will cost in schedule and dollars to reduce that mishap risk to an acceptable level.

A.4.4.3.2 <u>Tool development</u>. The key to developing most mishap risk assessment tools is the characterization of mishap risks by mishap severity and mishap probability. Since the highest system safety design order of precedence is to eliminate hazards by design, a mishap risk assessment procedure considering only mishap severity will generally suffice during the early design phase to minimize the system's mishap risks (for example, just don't use hazardous or toxic material in the design). When all hazards cannot be eliminated during the early design phase, a mishap risk assessment procedure based upon the mishap probability as well as the mishap severity provides a resultant mishap risk assessment. The assessment is used to establish priorities for corrective action, resolution of identified hazards, and notification to management of the mishap risks. The information provided here is a suggested tool and set of definitions that can be used. Program managers can develop tools and definitions appropriate to their individual programs.

MIL-STD-882D
APPENDIX A

A.4.4.3.2.1 <u>Mishap severity</u>. Mishap severity categories are defined to provide a qualitative measure of the most reasonable credible mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction. Suggested mishap severity categories are shown in Table A-I. The dollar values shown in this table should be established on a system by system basis depending on the size of the system being considered to reflect the level of concern.

TABLE A-I. **Suggested mishap severity categories**.

Description	Category	Environmental, Safety, and Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.

NOTE: These mishap severity categories provide guidance to a wide variety of programs. However, adaptation to a particular program is generally required to provide a mutual understanding between the program manager and the developer as to the meaning of the terms used in the category definitions. Other risk assessment techniques may be used provided that the user approves them.

A.4.4.3.2.2 <u>Mishap probability</u>. Mishap probability is the probability that a mishap will occur during the planned life expectancy of the system. It can be described in terms of potential occurrences per unit of time, events, population, items, or activity. Assigning a quantitative mishap probability to a potential design or procedural hazard is generally not possible early in the design process. At that stage, a qualitative mishap probability may be

18

derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning a mishap probability is documented in hazard analysis reports. Suggested qualitative mishap probability levels are shown in Table A-II.

TABLE A-II. **Suggested mishap probability levels**.

Description*	Level	Specific Individual Item	Fleet or Inventory**
Frequent	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in that life.	Continuously experienced.
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.	Will occur frequently.
Occasional	C	Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.	Will occur several times.
Remote	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life.	Unlikely, but can reasonably be expected to occur.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life.	Unlikely to occur, but possible.

  *Definitions of descriptive words may have to be modified based on quantity of items involved.
 **The expected size of the fleet or inventory should be defined prior to accomplishing an assessment of the system.

        A.4.4.3.2.3 Mishap risk assessment. Mishap risk classification by mishap severity and mishap probability can be performed by using a mishap risk assessment matrix. This assessment allows one to assign a mishap risk assessment value to a hazard based on its mishap severity and its mishap probability. This value is then often used to rank different hazards as to their associated mishap risks. An example of a mishap risk assessment matrix is shown at Table A-III.

MIL-STD-882D
APPENDIX A

TABLE A-III. **Example mishap risk assessment values**.

SEVERITY PROBABILITY	Catastrophic	Critical	Marginal	Negligible
Frequent	1	3	7	13
Probable	2	5	9	16
Occasional	4	6	11	18
Remote	8	10	14	19
Improbable	12	15	17	20

A.4.4.3.2.4 Mishap risk categories. Mishap risk assessment values are often used in grouping individual hazards into mishap risk categories. Mishap risk categories are then used to generate specific action such as mandatory reporting of certain hazards to management for action or formal acceptance of the associated mishap risk. Table A-IV includes an example listing of mishap risk categories and the associated assessment values. In the example, the system management has determined that mishap risk assessment values 1 through 5 constitute "High" risk while values 6 through 9 constitute "Serious" risk.

TABLE A-IV. **Example mishap risk categories and mishap risk acceptance levels.**

Mishap Risk Assessment Value	Mishap Risk Category	Mishap Risk Acceptance Level
1 – 5	High	Component Acquisition Executive
6 – 9	Serious	Program Executive Officer
10 – 17	Medium	Program Manager
18 – 20	Low	As directed

  *Representative mishap risk acceptance levels are shown in the above table. Mishap risk acceptance is discussed in paragraph A.4.4.7. The using organization must be consulted by the corresponding levels of program management prior to mishap risk acceptance.

A.4.4.3.2.5 Mishap risk impact. The mishap risk impact is assessed, as necessary, using other factors to discriminate between hazards having the same mishap risk value. One might discriminate between hazards with the same mishap risk assessment value in terms of mission capabilities, or social, economic, and political factors. Program management will closely consult with the using organization on the decisions used to prioritize resulting actions.

A.4.4.3.3 Mishap risk assessment approaches. Commonly used approaches for assessing mishap risk can be found in the *Defense Acquisition Deskbook* and System Safety Society's *System Safety Analysis Handbook* (see A.6.1)

20

A.4.4.4 <u>Identification of mishap risk mitigation measures</u>. Identify potential mishap risk mitigation alternatives and the expected effectiveness of each alternative or method. Mishap risk mitigation is an iterative process that culminates when the residual mishap risk has been reduced to a level acceptable to the appropriate authority.

A.4.4.4.1 <u>Prioritize hazards for corrective action</u>. Hazards should be prioritized so that corrective action efforts can be focused on the most serious hazards first. A categorization of hazards may be conducted according to the mishap risk potential they present.

A.4.4.4.2 <u>System safety design order of precedence (see 4.4)</u>. The ultimate goal of a system safety program is to design systems that contain no hazards. However, since the nature of most complex systems makes it impossible or impractical to design them completely hazard-free, a successful system safety program often provides a system design where there exist no hazards resulting in an unacceptable level of mishap risk. As hazard analyses are performed, hazards will be identified that will require resolution. The system safety design order of precedence defines the order to be followed for satisfying system safety requirements and reducing risks. The alternatives for eliminating the specific hazard or controlling its associated risk are evaluated so that an acceptable method for mishap risk reduction can be agreed to.

A.4.4.5 <u>Reduction of mishap risk to an acceptable level</u>. Reduce the system mishap risk through a mitigation approach mutually agreed to by the developer, program manager and the using organization.

A.4.4.5.1 <u>Communication with associated test efforts</u>. Residual mishap risk and associated hazards must be communicated to the system test efforts for verification.

A.4.4.6 <u>Verification of mishap risk reduction</u>. Verify the mishap risk reduction and mitigation through appropriate analysis, testing, or inspection. Document the determined residual mishap risk. The program manager must ensure that the selected mitigation approaches will result in the expected residual mishap risk. To provide this assurance, the system test effort should verify the performance of the mitigation actions. New hazards identified during testing must be reported to the program manager and the developer.

A.4.4.6.1 <u>Testing for a safe design</u>. Tests and demonstrations must be defined to validate selected safety features of the system. Test or demonstrate safety critical equipment and procedures to determine the mishap severity or to establish the margin of safety of the design. Consider induced or simulated failures to demonstrate the failure mode and acceptability of safety critical equipment. When it cannot be analytically determined whether the corrective action taken will adequately control a hazard, conduct safety tests to evaluate the effectiveness of the controls. Where costs for safety testing would be prohibitive, safety characteristics or procedures may be verified by engineering analyses, analogy, laboratory test, functional mockups, or subscale/model simulation. Integrate testing of safety systems into appropriate system test and demonstration plans to the maximum extent possible.

A.4.4.6.2 Conducting safe testing. The program manager must ensure that test teams are familiar with mishap risks of the system. Test plans, procedures, and test results for all tests including design verification, operational evaluation, production acceptance, and shelf-life validation should be reviewed to ensure that:

a. Safety is adequately demonstrated.

b. The testing will be conducted in a safe manner.

c. All additional hazards introduced by testing procedures, instrumentation, test hardware, and test environment are properly identified and controlled.

A.4.4.6.3 Communication of new hazards identified during testing. Testing organizations must ensure that hazards and safety discrepancies discovered during testing are communicated to the program manager and the developer.

A.4.4.7 Review and acceptance of residual mishap risk by the appropriate authority. Notify the program manager of identified hazards and residual mishap risk. For long duration programs, incremental or periodic reporting should be used.

A.4.4.7.1 Residual mishap risk. The mishap risk that remains after all planned mishap risk management measures have been implemented is considered residual mishap risk. Residual mishap risk is documented along with the reason(s) for incomplete mitigation.

A.4.4.7.2 Residual mishap risk management. The program manager must know what residual mishap risk exists in the system being acquired. For significant mishap risks, the program manager is required to elevate reporting of residual mishap risk to higher levels of appropriate authority (such as the Program Executive Officer or Component Acquisition Executive) for action or acceptance. The program manager is encouraged to apply additional resources or other remedies to help the developer satisfactorily resolve hazards providing significant mishap risk. Table A-IV includes an example of a mishap risk acceptance level matrix based on the mishap risk assessment value and mishap risk category.

A.4.4.7.3 Residual mishap risk acceptance. The program manager is responsible for formally documenting the acceptance of the residual mishap risk of the system by the appropriate authority. The program manager should update this residual mishap risk and the associated hazards to reflect changes/modifications in the system or its use. The program manager and using organization should jointly determine the updated residual mishap risk prior to acceptance of the risk and system hazards by the risk acceptance authority, and should document the agreement between the user and the risk acceptance authority.

A.4.4.8 Tracking hazards and residual mishap risk. Track hazards, their closures, and residual mishap risk. A tracking system for hazards, their closures, and residual mishap risk must be maintained throughout the system life cycle. The program manager must keep the system user apprised of system hazards and residual mishap risk.

MIL-STD-882D
APPENDIX A

A.4.4.8.1 Process for tracking of hazards and residual mishap risk. Each system must have a current log of identified hazards and residual mishap risk, including an assessment of the residual mishap risk (see A.4.4.7). As changes are integrated into the system, this log is updated to incorporate added or changed hazards and the associated residual mishap risk. The Government must formally acknowledge acceptance of system hazards and residual mishap risk. Users will be kept informed of hazards and residual mishap risk associated with their systems.

A.4.4.8.1.1 Developer responsibilities for communications, acceptance, and tracking of hazards and residual mishap risk. The developer (see 3.2.2) is responsible for communicating information to the program manager on system hazards and residual mishap risk, including any unusual consequences and costs associated with hazard mitigation. After attempting to eliminate or mitigate system hazards, the developer will formally document and notify the program manager of all hazards breaching thresholds set in the safety design criteria. At the same time, the developer will also communicate the system residual mishap risk.

A.4.4.8.1.2 Program manager responsibilities for communications, acceptance, and tracking of hazards and residual mishap risk. The program manager is responsible for maintaining a log of all identified hazards and residual mishap risk for the system. The program manager will communicate known hazards and associated risks of the system to all system developers and users. As changes are integrated into the system, the program manager shall update this log to incorporate added or changed hazards and the residual mishap risk identified by the developer. The program manager is also responsible for informing system developers about the program manager's expectations for handling of newly discovered hazards. The program manager will evaluate new hazards and the resulting residual mishap risk, and either recommend further action to mitigate the hazards, or formally document the acceptance of these hazards and residual mishap risk. The program manager will evaluate the hazards and associated residual mishap risk in close consultation and coordination with the ultimate end user, to assure that the context of the user requirements, potential mission capability, and the operational environment are adequately addressed. Copies of the documentation of the hazard and risk acceptance will be provided to both the developer and the system user. Hazards for which the program manager accepts responsibility for mitigation will also be included in the formal documentation. For example, if the program manager decides to execute a special training program to mitigate a potentially hazardous situation, this approach will be documented in the formal response to the developer. Residual mishap risk and hazards must be communicated to system test efforts for verification.

A.5 SPECIFIC REQUIREMENTS

A.5.1 Program manager responsibilities. The program manager must ensure that all types of hazards are identified, evaluated, and mitigated to a level compliant with acquisition management policy, federal (and state where applicable) laws and regulations, Executive Orders, treaties, and agreements. The program manager should:

A.5.1.1 Establish, plan, organize, implement, and maintain an effective system safety effort that is integrated into all life cycle phases.

A.5.1.2 Ensure that system safety planning is documented to provide all program participants with visibility into how the system safety effort is to be conducted.

A.5.1.3 Establish definitive safety requirements for the procurement, development, and sustainment of the system. The requirements should be set forth clearly in the appropriate system specifications and contractual documents.

A.5.1.4 Provide historical safety data to developers.

A.5.1.5 Monitor the developer's system safety activities and review and approve delivered data in a timely manner, if applicable, to ensure adequate performance and compliance with safety requirements.

A.5.1.6 Ensure that the appropriate system specifications are updated to reflect results of analyses, tests, and evaluations.

A.5.1.7 Evaluate new lessons learned for inclusion into appropriate databases and submit recommendations to the responsible organization.

A.5.1.8 Establish system safety teams to assist the program manager in developing and implementing a system safety effort.

A.5.1.9 Provide technical data on Government-furnished Equipment or Government-furnished Property to enable the developer to accomplish the defined tasks.

A.5.1.10 Document acceptance of residual mishap risk and associated hazards.

A.5.1.11 Keep the system users apprised of system hazards and residual mishap risk.

A.5.1.12 Ensure the program meets the intent of the latest MIL-STD 882.

A.5.1.13 Ensure adequate resources are available to support the program system safety effort.

A.5.1.14 Ensure system safety technical and managerial personnel are qualified and certified for the job.

A.6 NOTES

A.6.1 DoD acquisition practices and safety analysis techniques. Information on DoD acquisition practices and safety analysis techniques is available at the referenced Internet sites. Nothing in the referenced information is considered binding or additive to the requirements provided in this standard.

A.6.1.1 *Defense Acquisition Deskbook.* Wright-Patterson Air Force Base, Ohio: Deskbook Joint Program Office.

MIL-STD-882D
APPENDIX A

A.6.1.2 *System Safety Analysis Handbook.* Unionville, VA: System Safety Society.

MIL-STD-882D

CONCLUDING MATERIAL

Custodians:
  Army - AV
  Navy - AS
  Air Force – 40

Preparing activity:
  Air Force - 40

Project SAFT - 0038

Reviewing activities:
  Army - AR, AT, CR, MI
  Navy - EC, OS, SA, SH
  Air Force - 10, 11, 13, 19

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

INSTRUCTIONS

1. The preparing activity must complete blocks 1, 2, 3, and 8. In block 1, both the document number and revision letter should be given.

2. The submitter of this form must complete blocks 4, 5, 6, and 7, and send to preparing activity.

3   The preparing activity must provide a reply within 30 days from receipt of the form.

NOTE: This form may not be used to request copies of documents, nor to request waivers, or clarification of requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements.

I RECOMMEND A CHANGE:	1. DOCUMENT NUMBER **MIL-STD-882**	2. DOCUMENT DATE *(YYYYMMDD)* **20000210**

3. DOCUMENT TITLE

System Safety

4. NATURE OF CHANGE *(Identify paragraph number and include proposed rewrite, if possible. Attach extra sheets as needed.)*

5. REASON FOR RECOMMENDATION

6. SUBMITTER

a. NAME *(Last, First, Middle Initial)*	b. ORGANIZATION	

c. ADDRESS *(Include zip code)*	d. TELEPHONE *(Include Area Code)*
	(1) Commercial
	(2) DSN
	  (if applicable)
		7. DATE SUBMITTED
		  (YYYYMMDD)

8. PREPARING ACTIVITY

a. NAME
  Headquarters, Air Force Materiel Command
  System Safety Division
	b. TELEPHONE *(Include Area Code)*
	(1) Commercial (937) 257-6007
	(2) DSN 787-6007

b. ADDRESS *(Include Zip Code)*
  HQ AFMC/SES
  4375 Chidlaw Road
  Wright Patterson AFB, Ohio 45433-5006
	IF YOU DO NOT RECEIVE A REPLY WITHIN 45 DAYS, CONTACT:
	  Defense Standardization Program Office (DLSC-LM)
	  8725 John J. Kingman Road, Suite 2533
	  Fort Belvoir, Virginia 22060-6621
	  Telephone 703 767-6888 DSN 427-6888

DD Form 1426, FEB 1999 (EG)   PREVIOUS EDITION IS OBSOLETE.   WHS/DIOR, Feb 99