Approved for Public Release;
Distribution Unlimited

MIL-STD-1574A (USAF)
15 August 1979
Superseding
MIL-STD-1574 (USAF)
15 March 1977

MILITARY STANDARD

SYSTEM SAFETY PROGRAM FOR SPACE AND MISSILE SYSTEMS

FSC 1810

AMSC 32000

DEPARTMENT OF THE AIR FORCE
Washington, D.C. 20360

System Safety Program for Space and Missile Systems

MIL-STD-1574A (USAF)

1. This Military Standard is approved for use by the Department of the Air Force, and is available for use by all Departments and Agencies of the Department of Defense.

2. Beneficial comments (recommendations, additions, deletions) and any pertinent data which may be of use in improving this document should be addressed to: SAMSO/AQM, P.O. Box 92960, Worldway Postal Center, Los Angeles, CA. 90009, by using the self-addressed Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter.

FOREWORD

1. Accident prevention is of major concern throughout the life cycle of a system. Planning and implementation of an effective system safety program, commensurate with the requirements of each phase of the acquisition process, is of prime importance in minimizing risk of accidents and their associated cost impacts during the systems test and operational phases. System safety responsibilities shall be an inherent part of every program and the implementation of the complete system safety program requires extensive participation and support by many disciplines and functional areas.

2. This document defines the management and technical requirements of a system safety program beginning during the conceptual phase of a development program and continuing throughout a system's life cycle. The requirements are presented in a manner which facilitates tailoring to specific program needs. It is the intent of this document that such tailoring, implemented through contract negotiation, be interpreted as meeting the requirements of this standard.

3. MIL-STD-1574A is a tailored application of MIL-STD-882A for space, missile, and related systems.

CONTENTS

CONTENTS (Continued)

CONTENTS (Continued)

in this standard.

1. SCOPE

1.1 Purpose. A system safety program, as specified herein, establishes administrative and technical means by which accident prevention requirements and policies are planned, managed and implemented into the total program effort. The activities of the system safety program include: planning, management, design, analysis, research, operational functions, auditing and training. The purpose of the program is to identify significant accident risk and define methods to cope effectively with that risk within program cost, schedule, performance, and technical acceptability parameters. This standard defines the requirements for implementation of system safety programs covering the life cycle of the system. It includes the safety requirements for the following activities/periods: design, development, test, checkout, modification, production, servicing, refurbishing, maintenance, transportation, handling, training, disposal, deployment, and normal and contingency operations. This standard also defines the management and technical tasks and controls required to minimize accident risks caused by human error, environment, deficiency/inadequacy of design, and component malfunction or interactions. Risks of concern are those which could result in major injury or fatality to personnel including flight or ground crews, or damage to the system including support equipment and facilities.

1.2 Application. This standard is applicable to all systems involving the development and use of experiments, flight vehicles, weapon systems, ground equipment and facilities. A system typically includes the airborne and ground support equipment required to interface and operate with the flight hardware; the personnel and ground support equipment required to service, test, checkout, maintain, refurbish, transport and handle the flight hardware; the ground and flight software required to checkout and control the flight hardware; and the personnel required to service, test, maintain, and operate the system.

1.3 Tailoring. The Purchasing Office will evaluate and tailor each requirement of this standard to realize the maximum compliance commensurate with the program phase being considered. The requirements are presented in a manner which facilitates tailoring to specific program needs. Tailoring may take the form of addition, alteration or deletion of tasks. In all cases, however, the inclusion of requirements

of paragraph 3.11, Qualified System Safety Engineer; 4.1, Safety Program Management and 5.4, Safety Data, is mandatory.

1.4 Compliance. Compilance with all contractually imposed requirements of this standard is mandatory. Failure to include any contractually imposed requirement in the contractor prepared plan does not mean or imply that the requirement is not applicable unless specific approval is granted by the Contracting Officer. A deviation request must be submitted by the contractor in accordance with paragraph 5.1.4 and approved by the contracting officer.

2. REFERENCED DOCUMENTS: Not Applicable

3. DEFINITIONS

3.1 Accident. An unplanned event or series of events that results in death or major injury to personnel or damage to the launch vehicle, experiments, spacecraft, associated support equipment or facilities.

3.2 Accident risk. Measure of vulnerability to loss, damage or injury caused by a dangerous element, or factor.

3.3 Accident risk factor. A dangerous element of a system, event, process or activity including casual factors such as design or programming deficiency, component malfunction, human error or environment which can propagate a hazard into an accident if adequate controls are not effectively applied.

3.4 Credible condition. A condition that can occur and is reasonably likely to occur.

3.5 Critical function. As applied to nuclear systems, those functions which apply directly to, or control, or reverse the enable, prearm, arm, unlock, release, or targeting functions.

3.6 Damage. Breakage, mangling, mutilation or ruin of items transmitted across system or component interfaces by inadvertent internal or external action including component failure and human error which could cause obstruction of critical functions or require repair or replacement.

3.7 Deviation. An alternate method of compliance with the intent of specific requirements.

3.8 Hazard. An existing or potential condition that can result in an accident.

3.9 Major injury. Any injury which results in admission to a hospital such as bone fracture, second or third degree burns, severe lacerations, internal injury, severe radiation exposure, chemical or physical agent toxic exposure, or unconsciousness.

3.10 Program safety requirements. Program safety requirements include the contractually imposed design and operational requirements listed in compliance documents, or system specifications. Program safety requirements define system constraints and capabilities, establish acceptable and unacceptable risk conditions, or identify specific design and operational criteria and approaches.

3.11 Qualified System Safety engineer. A technically competent individual who is educated at least to the bachelor of science level in engineering or related applied science and is registered as a professional engineer in one of the states or territories of the United States or has equivalent experience approved by the Purchasing Office. This individual shall have been assigned as a system safety engineer on a full-time basis for a minimum of four years in at least three of the six functional areas listed below:

a. System Safety Management

b. System Safety Analysis

c. System Safety Design

d. System Safety Research

e. System Safety Operations

f. Accident Investigation

3.12 Safety concerns. Those identified safety critical aspects or risk factors which cannot be satisfactorily resolved or closed out by the contractor and must be elevated to the purchasing office for resolution.

3.13 Safety critical. Any condition, event, operation, process, equipment, or system, with a potential for major injury or damage.

3.14 Support equipment. Support equipment is all system equipment required to support the ground and flight phases of the mission. Support equipment includes aerospace ground equipment (AGE), maintenance ground equipment (MGE), transportation and handling (T&H) equipment, and equipment used to support system deployment (i.e., assembly tools and fixtures, test and checkout equipment, personnel support and protection equipment).

3.15 System loss. Damage to an extent that renders repair impractical. Requires salvage or system replacement.

4. GENERAL REQUIREMENTS

4.1 Safety program management.

4.1.1 Management system. The contractor shall establish a safety management system to implement provisions of this standard commensurate with the program contractual requirements. The contractor program manager shall be responsible for the establishment, control, incorporation, direction and implementation of the system safety program policies and shall assure that the accident risk is identified and controlled or eliminated within established program accident risk acceptability parameters.

4.1.2 System Safety Program Plan. The contractor shall prepare a System Safety Program Plan based on the requirements of this standard which are identified in the contract Statement of Work (Ref. Data Item Description DI-H-7047). The plans shall be implemented upon approval by the Contracting Officer (PCO) and describe the system safety activities required during the life of the contracted program. The plan shall be updated at the end of each program phase to describe tasks and responsibilities required for the subsequent phase. The approved plan shall, on an

item-by-item basis, account for all contractually required requirements, tasks, and responsibilities. In the event of any conflict between the contractors approved plan and the tailored application of this standard the requirements of the standard shall apply.

The plan shall include:

a. Details of the system safety organization and full particulars of the System Safety Manager to Program Manager relationship and accountability (para. 4.1.3), including the following:

(1) The organization(s) directly responsible for each subtask accomplishment. Company policies, procedures and/or controls governing conduct of each subtask.

(2) A composite listing of applicable Company policies, procedures and controls, by title, number, and release date. This section of the contractor's working system safety program plan(s) shall be maintained current and subject to procuring activity review. The plan need not be resubmitted to the procuring activity for minor changes and changes in release date(s).

(3) A chart showing the contractor's program organization and identifying the organizational element assigned responsibility and authority for implementing the system safety program. The plan shall further identify the system safety organization through all management and supervisory levels.

(4) The interfaces between the system safety organization and other organizations, (including cross-references to applicable sections of other program plans). Describe the purpose of each interface, such as what data or information is transferred at these interfaces.

b. Details of how resolution and action relative to system safety will be affected at the program management level possessing resolution authority.

response. IR = No IR responses.

c. Details of the method by which problems encountered in the implementation of the System Safety Program and requirements are brought to the attention of the Program Manager.

d. Description of procedures to be used to assure completion of action regarding identified unacceptable risks (paragraph 5.1.1.1.).

e. Description of methods to be used in implementation of each task identified by the tailored application of this standard, including a breakout of task implementation responsibilities by organizational component discipline, functional area or any planned sub-contractor activity (paragraph 4.1.3).

f. Description of internal controls for the proper and timely identification and implementation of safety requirements affecting system design, operational resources and personnel.

g. A schedule of the system safety activities and a milestone chart (paragraph 4.2) showing relationships of the system safety activities with other program tasks and events.

h. Level of effort required for successful completion of contractually required tasks.

4.1.3 System safety organization. The contractor shall establish a system safety organization which has centralized accident risk management authority delegated from the contractor program manager, to maintain a continuous overview of the technical and planning aspects of the total program. The system safety organization shall be headed by an experienced system safety manager who shall be directly accountable to the program manager for the conduct and effectiveness of all contracted safety effort for the entire program. The system safety manager shall meet the requirements established in 3.11. The system safety manager shall be responsible for the primary control, direction, supervision, and management of the technical safety aspects of the program. He shall undertake himself, or direct accomplishment by personnel directly under his supervision, the technical tasks of the system safety program and provide guidance, assistance and surveillance for the successful accomplishment of safety tasks to be undertaken by others not under his direct supervision. Personnel assigned to accomplish the technical safety tasks

shall have the necessary engineering qualifications and a basic understanding of the system safety processes, but do not have to meet the requirements established in 3.11. The system safety manager shall be responsible for the effective implementation of the following tasks for the program:

a. Provide a single point of contact for the purchasing office, all contractor internal program elements, and other program associate or sub-contractors for safety related matters.

b. Review, and provide input to all plans and contractual documents related to safety.

c. Maintain a log, for purchasing office review, of all program documentation reviewed and record all concurrences, nonconcurrences, reasons for nonconcurrence, and actions taken to resolve any nonconcurrence (see 5.4.4).

d. Maintain approval authority over safety critical program documentation, and all items related to safety contained in the contract data requirements list (CDRL).

e. Coordinate safety related matters with contractor program management and all program elements and disciplines.

f. Provide internal approval and technical coordination on deviations to the contractually imposed system safety requirements as defined in 5.1.4.

g. Conduct or arrange for internal audits of safety program activities as defined in 5.6. Support purchasing office safety audits and inspections as required.

h. Coordinate system safety, industrial safety, and product safety activities on the program to ensure total coverage (see paragraph 4.6).

i. Establish internal reporting systems and procedures for investigation and disposition of accidents and safety incidents, including potentially hazardous conditions not yet involved in an accident/ incident. Report such matters to the purchasing office as required by the contract.

j. Provide participation in all requirements reviews, preliminary design reviews, critical design reviews and scheduled safety reviews to assure that:

(1) All contractually imposed system safety requirements including those imposed by this standard are complied with.

(2) Safety program schedule and CDRL data deliveries are compatible.

(3) Hazard analysis methods and formats from all safety program participants permit integration in a cost effective manner.

(4) Technical data are provided to support the preparation of the accident risk assessment report.

k. Participate in all test, flight or operational readiness reviews and arrange for presentation of required safety data.

l. Provide for technical support to program engineering activities on a daily basis. Such technical support will include consultation on safety related problems, research on new product development and research/interpretation of safety requirements, specifications and standards.

m. Provide participation in configuration control board activities as necessary to enable review and concurrence with safety significant system configuration and changes thereto.

n. Review all trade studies and identify those that involve or effect safety. Provide participation in all safety related trade studies to assure that System Safety trade criteria is developed and the final decision is made with proper consideration of accident risk (see paragraph 4.14).

o. Provide participation in program level status meetings where safety should be a topic of discussion. Provide the program manager the status of the the system safety program and open action items.

p. Provide for safety certification (para 5.4.1) of safety-critical program documentation and all safety data items contained in the contract data requirements list (CDRL).

4.2 System safety program milestones. The contractor shall prepare a milestone chart for the system safety effort specified by the purchasing office which identifies representative tasks, applicable program milestones, input required and program element responsibility for each, the output to be provided, and the schedule related to program milestones (Para. 4.1.2g). Both program and safety milestones shall be controlled by the program master schedule (PMS) and internal operations directives. Program milestones shall be the major checkpoints at which data verifying system safety will be presented. The audit program (see paragraph 5.6) shall be used to ensure major safety milestones and checkpoints are met and proper data provided.

4.3 Integration function.

4.3.1 Integrating agency/contractor. The integrator for the safety functions of all associate contractors will be designated by the purchasing office. The purchasing office itself, another Government agency, or a contractor may be so designated. The system safety integrator designated to perform this function shall:

a. Prepare an integrated system safety plan which establishes the authority of the integrator and defines the effort required from each associate contractor for integration of system safety requirements for the total system. Associate contractor system safety plans shall be incorporated as annexes to the integrated system safety plan. In addition to the other contractually imposed requirements from this standard, the plan shall address and identify:

(1) Analyses to be conducted by each associate contractor and format to be utilized.

(2) Data each associate contractor is required to submit to the integrator and its scheduled delivery keyed to program milestones.

(3) Schedule and other information considered pertinent by the integrator.

(4) The method for the development of system level requirements to be allocated to each of the associate contractors as a part of the system specification, end-item specifications, and/or other interface requirement documentation.

b. Initiate action through the contract manager to ensure that each associate contractor is contractually required to be responsive to the system safety program. Recommend contractual modifications where the need exists.

c. Conduct safety analyses of the integrated system, operations, and interfaces between assembled end items. Analyses provided by associate contractors (see 4.3.2) shall be used in the conduct of this effort.

d. Provide an assessment of the accident risk presented by the operation of the integrated system for approval by the purchasing office.

e. Provide assistance and guidance to associate contractors in the implementation of interface safety requirements.

f. Resolve differences between associate contractors in areas related to safety, especially during tradeoff studies. Where problems cannot be resolved by the integrator, a statement of the problem and the recommended solution will be provided to the purchasing office for resolution and action.

g. Ensure that information required by an associate contractor from other associate contractors to accomplish safety analyses is provided in a mutually agreed-to format for compatibility with the integrating process.

h. Develop a system for normal interchange and feedback of information related to safety between the purchasing office, integrating contractor, and associate contractors.

i. Schedule and conduct technical meetings between all associate contractors to discuss, review, and integrate the safety effort.

j. Notify in writing any associate contractor of their failure to meet contract program or technical system safety requirements for which they are responsible. The integrator for the safety effort will send a copy of the notification letter to the purchasing office whenever such written notification has been given.

k. Participate as an active member of the Purchasing Office System Safety Group (SSG) and shall present the integrated program safety status, results of design, operations or safety reviews; summarize hazard analysis results, identify all problems and status of resolution; and accept and respond to action items assigned by the chairman of the SSG.

4.3.2 Associate contractors. Associate contractors shall provide sufficient level of effort commensurate with contractual responsibilities for conducting analyses of effects on end items, or inputs, normal or abnormal, from other subsystems until such time as the integrator determines that such support is no longer necessary and such action is approved by the purchasing office. The system safety manager for each associate contractor shall control his own subcontractor system safety activities as defined in 4.4.

4.4 Subcontractors. Major subcontractors shall be required to maintain suitable documentation of safety analyses they have performed in formats which will permit incorporation of their data into the overall analysis program. Major subcontractors shall be required to develop system safety program plans that shall be included as annexes to the prime contractor's system safety program plan. Lesser subcontractors and vendors shall be required to provide information on component and subassembly characteristics including failure modes, failure rates, and possible hazards, which will permit prime contractor personnel to evaluate the items for their impact on safety of the system. Applicable provisions of this standard shall be included in all contracts with major subcontractors.

4.5 System safety group (SSG), and Safety Review Team (SRT) support

4.5.1 The contractor shall provide support to the SSG as required by the SSG charter

4.5.2 The contractor shall provide assistance to the safety review team to the extent necessary to support the system safety certification process.

4.6 Industrial safety. The contractor shall conduct the System Safety Program so that it supplements existing industrial safety and toxicology activities. This coordinated effort shall assure that Government equipment or properties being used or developed under contract are protected from damage or accident risk. When contractor owned or leased equipment is being used in manufacturing, testing or handling of products developed or produced under contract, analysis and operational proof checks shall be performed to show that risk of damage to those products has been minimized through proper design, maintenance, and operation by qualified personnel using approved procedures. This standard does not cover those functions the contractor is required by law to perform under Federal or State Occupational Safety and Health, Department of Transportation or Environmental Protection Agency regulations.

4.7 Operational site safety. The contractor system safety program shall encompass operational site activities. These activities shall include all operations listed in the operational time lines, including system installation, checkout, modification, and operation. Particular attention shall be given to operations and interfaces with ground support equipment and to the needs of the operators relating to personnel subsystems such as: panel layouts, individual operator tasks, fatigue prevention, biomedical considerations, etc.

4.8 Facilities. The contractor shall include facilities in the system safety analyses activity (see 5.2). Facility safety design criteria shall be incorporated in the facility specifications. Consideration shall be given to the test operational and maintenance aspects of the program. Identified requirements will include consideration of the compatibility with standards equal to or better than those specified by Federal and Air Force Occupational Safety and Health Regulations. The test and operations safety procedures shall encompass all development, qualification,

acceptance tests and operations. The procedures will include inputs from the safety analyses and identify test and operations facility and support requirements. The procedures shall be upgraded and refined as required to correct deficiencies identified by the system safety analyses to incorporate additional safety requirements.

4.9 Range safety. Compliance with the design and operational criteria contained in the applicable range safety manuals regulations and standards shall be considered in the system safety analysis of 5.2 and the system safety criteria of 5.1.

4.9.1 Missile flight analysis. Flight analysis and flight termination system requirements are applicable to the system during all flight phases until payload impact or orbital insertion. The Accident Risk Assessment Report shall include all aspects of flight safety systems. (see 5.2.14.2)

4.9.2 Missile systems safety. Verification of system design and operational planning compliance with range or operating site safety requirements shall be documented in the Accident Risk Assessment Report. (see 5.2.14.2)

4.10 Test safety. The contractor shall establish internal procedures for identification and timely action on elimination or control of potential hazardous test conditions induced by design deficiencies, unsafe acts or procedural errors. Procedures shall be established to identify, review and supervise potentially hazardous, high risk tests including those tests performed specifically to obtain safety data. The contractor system safety organization shall:

a. Review and approve of test plans, procedures and safety surveillance procedures and changes to verify incorporation of safety requirements identified by the system analyses of 5.2 (See 5.2.10).

b. Assure that an assessment of accident risk is included in all pre-test readiness reviews.

4.11 Support equipment. Safety requirements for support equipment shall be identified in the system safety analyses (see 5.2). Support equipment safety design criteria shall be incorporated in the segment specifications. Safety requirements for ground handling shall be developed and included in the transportation and handling plans and procedures. Safety requirements for operations and servicing shall be included

in the operational procedures. The procedures shall be upgraded and refined as required to correct deficiencies that could damage equipment or injure personnel. Special attention shall be given to the planning, design and refurbishment of reusable support equipment including equipment carried on flight vehicles to assure that safety is not degraded by continued usage. Identified requirements for support equipment used at the operational site but not carried on flight vehicles shall include consideration to the compatibility with standards equal to or better than those specified by Federal and Air Force Occupational Safety and Health Regulations.

4.12 Nuclear weapon safety. The Department of Defense has established four safety standards that are the basis for nuclear weapon system design and the safety rules governing nuclear weapon system operation. These standards require that, as a minimum, the system design shall incorporate positive measure to:

a. Prevent any nuclear weapon involved in an accident or incident, or a jettisoned weapon, from producing a nuclear yield.

b. Prevent deliberate prearming, arming, launching, firing, or releasing of any nuclear weapon, except upon execution of emergency war orders or when directed by competent authority.

c. Prevent inadvertent prearming, arming, launching, firing, or releasing of any nuclear weapon.

d. Ensure the adequate security of each nuclear weapon.

The contractor system safety effort on a nuclear weapon system program shall directly support the objectives included in these standards.

4.12.1 Critical function control. The contractor shall provide assurance that the four nuclear safety standards of 4.12 are met by designing each nuclear weapon system to control critical functions in the sequence leading to detonation of the weapon. As a minimum, the functions listed below are designated as critical and require specific safety devices or means for their control.

a. Authorization to use the weapon (enable function).

b. Intent Command signaling (weapon prearm function).

c. Arm/Unlock and Ignition/Release Commands (Launch or release function).

d. Launch/Release Environmental Sensing (Final Arming function).

4.12.2 Special nuclear safety analyses. The normal hazard analyses and Accident Risk Assessment specified in para 5.2 of this standard apply to nuclear weapon systems. However, because of the dire political and military consequences of an unauthorized or accidental nuclear or high explosive detonation, additional analyses are specified to demonstrate positive control of nuclear weapons in all probable environments. The following analyses, in whole or in part, shall be performed by the contractor on nuclear weapons programs as specified by the purchasing office:

a. A quantitative analysis to assure that the probability of Inadvertent Nuclear Detonation (IND), Inadvertent Programmed Launch (IPL), Accidental Motor Ignition (AMI), Inadvertent Enabling or Inadvertent Prearm (IPA) meets the numerical requirements specificed in applicable nuclear safety criteria documents.

b. An Unauthorized Launch (UL) analysis to define the time, tools and equipment required to accomplish certain actions leading to unauthorized launch. The results of this analysis are used by the nuclear safety evaluation agency in determining which components require additional protection, either by design or procedural means.

c. A Nuclear Safety Crosscheck Analysis (NSCCA) of software and certain firmware which directly or indirectly controls or could be modified to control critical weapon functions. This analysis, by an independent contracting agency, must determine that the final version of software or firmware is free from programming which could contribute to unauthorized, accidental or inadvertent activation of critical system function.

d. A Safety Engineering Analysis (SEA) of all tasks in modification or test programs at operational sites. This analysis is specifically oriented towards

identifying hazards to personnel and equipment in the work area and is in addition to the analysis of the safety impact of the change to the weapon system."

4.13 Radiological safety.

4.13.1 Radioactive sources. The contractor shall conduct safety analyses for all applications of radioactive sources, nuclear power systems, and other systems having sources of ionizing radiation. This analysis shall include a complete assessment of the accident risk in the following areas:

a. Normal mission analysis:

(1) Transportation, handling, calibration, testing and processing during pre-launch operations at the launch site including use of nonflight sources.

(2) Flight safety (launch, flight to orbit or ballistic reentry, and random reentry).

(3) Recovery operations at mission termination site.

b. Contingency analysis:

(1) Operational site accident (fire, explosion, impact, rupture, dispersal, and release quantity).

(2) Flight accident.

(3) Abnormal re-entry, recovery, or disposition.

(4) Abort conditions.

(5) Accident mode and characteristics.

(6) Accident probability, normal mission, and worst case accident consequences.

(7) Chemical toxicity and external radiation.

(8) Conclusions.

4.14 Trade studies. System safety engineering personnel shall participate in all trade studies that have

been identified as being safety related (see 4.1.3 n). System Safety engineering shall ensure that safety impact items and accident risk assessments are significantly highlighted and given appropriate weight as decision drivers. Documentation shall show that the accident risk for the recommended solution is equal to or less than the other alternatives being traded or provide sufficient justification for recommending another alternative. Results of trade studies shall be reviewed to ensure that recommendations for management level decisions include the optimum safety provisions developed for each option.

4.15 Government furnished equipment and property. Where safety analysis or risk assessments are not provided with Government furnished equipment and property, the contractor shall identify this deficiency to the purchasing office as a safety concern. Upon purchasing office direction the contractor shall perform a system safety analysis in accordance with paragraph 5. An accident risk assessment, shall be provided in accordance with paragraph 5.2.14.2. Recommendations for action and resolution of identified problems shall be included in an Accident Risk Assessment Report and submitted to the procuring contracting office.

4.16 Government furnished data. Where adequate data required to complete contracted safety tasks is not provided, the contractor shall identify this deficiency to the purchasing office as a safety concern. Upon purchasing office direction the contractor shall initiate efforts to develop or obtain the required data.

5. DETAILED REQUIREMENTS

5.1 System safety criteria. Effective accident control involves many aspects of system engineering including considerations of severity and cost versus impact potential, basic design options reaction time and procedural controls, etc.

5.1.1 Hazard level categories. The contractor's accident risk assessment efforts and related hazards analyses shall reflect relative severity and probability of occurrence. These categories shall be be used for tracking risk reduction. Probability of occurrence and severity may be expressed qualitatively or quantitatively as dictated by specific program requirement. Whatever method is used,

conditions such as those in the following subparagraphs shall be taken into consideration.

5.1.1.1 Unacceptable conditions. The following examples of representative safety critical conditions are considered unacceptable. Positive action and implementation verification is required to reduce the risk to an acceptable level as negotiated by the contractor and the purchasing office.

a. Single component failures, human error, or design features which could cause an accident such as:

(1) Damage which inhibits launch, staging, primary or secondary means of separating the payload, deployment of solar panels, firing of spacecraft or retro-rocket motors, or otherwise prevents the successful deployment or positioning of the vehicle for orbital operations, retrieval, reentry, or landing operations.

(2) Inadvertent arming or ignition of ordnance devices; inadvertent actuation or deployment of solar panels, antennas, staging devices, spring actuated covers, shrouds or any other safety critical device; inadvertent activation of hazardous electrical power or initiation of a command sequence which could cause an accident; overpressurization of a propellant or high pressure gas system.

(3) Uncontrolled or unplanned venting, dumping, ejection, or leakage of propellants, corrosive materials or high pressure gases.

(4) Malfunction, accidental operation of any single component, or any human error which could result in the pre-arming, arming, launching, firing or releasing of a nuclear weapon.

b. Dual independent component failures, dual human errors, or a combination of a component failure and a human error involving safety critical command and control functions such as engine firing or stage separation that could result in system loss.

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

d. Hazard level categories that are specified as unacceptable in the contract.

e. Packaging or handling procedures and characteristics which could cause an accident for which no controls have been provided to protect personnel or sensitive equipment.

5.1.1.2 Acceptable conditions. The following approaches are considered acceptable for correcting unacceptable conditions such as those referenced in 5.1.1.1 and will require no further analysis once controlling actions are implemented. Specific verification of implementation and effectiveness of controlling actions shall be provided (see 5.2.12). Hazard analysis showing identification, correction, and close-outs shall be included in the accident risk assessment report.

a. A system design which requires two or more human errors or which requires two or more independent failures or a combination of independent failures and human error to result in an accident that does not involve safety critical command and control functions which could cause system loss. Even though the unlikely event of multiple failures may appear to offer adequate protection, related tests, monitoring and specific flight preparation operations should be specified to assure acceptable risk levels. When redundant components are utilized to mitigate accident risk, provisions shall be made to verify operation of both redundant components prior to entering into irreversible portions of safety critical functions.

b. System designs that require at least three independent failures, or three human errors, or a combination of three independant failures and human errors for safety critical command and control functions such as engine firing or stage separation before any inadvertent operation occurs that could result in system loss.

c. System designs which positively prevent errors in assembly, installation, or connection which could result in an accident.

d. System designs which positively prevent damage propagation from one component to another or prevent sufficient energy propagation to cause an accident.

e. System design limitations on operation, interaction, or sequencing which preclude occurrence of an accident.

f. System designs that provide an approved safety factor, or fixed design allowance which minimizes possibilities of structural failure or release of energy sufficient to cause an accident.

g. System designs that control energy buildup which could potentially cause an accident (fuses, relief valves, electrical explosion proofing, etc.).

h. System designs in which 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. The assumptions made to reach the conclusion of "temporarily tolerated failure" shall be documented.

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

j. System designs which minimize/control the use of flammable materials.

5.1.2 System safety precedence. Contractor program management acceptance of credible risk shall be based upon the magnitude of risk compared with the impact of compensating for it. Risks which are not totally controllable by design action because of impact on cost, performance or schedule, shall be dealt with at the highest feasible order of precedence. Corrective action to be taken shall be in the following order of precedence:

a. Design for minimum hazards. The contractor system safety organization shall ensure, to the maximum

extent practical, the inherent safety of the system through the use of appropriate design features and qualified components. These features shall be subjected to analyses to provide a thorough review of their compatibility with maintenance, test and mission operations, and other task requirements. In addition, the design features shall be reviewed to minimize the probability of safety degradation because of human error. Particular attention shall be paid to primary system design to assure gradual degradation of function to permit detection of impending hazardous conditions in sufficient time to complete automatic or manual control actions.

b. Safety devices. Risks which cannot be totally controlled through design selection, or which are discovered too late for basic system redesign, shall be reduced through the use of appropriate safety devices, such as mechanical internal barriers or inhibiting mechanisms, as part of the system, subsystem or equipment.

c. Protective systems. In instances where accident risk exists and cannot be totally eliminated, the contractor shall provide for employment of appropriate protection systems (i.e., fire suppression, radiation shielding, explosion or detonation blast shields, etc.).

d. Warning devices. Where it is not possible to totally preclude the existence or occurrence of a known condition with a significant accident risk, reliable devices with proper emergency plans and procedures shall be employed for timely detection of the condition and the generation of an adequate warning signal. Warning signals shall be standardized within like types of systems, to minimize the probability of improper personnel reaction to the signals. Personnel shall be properly trained regarding the purpose of the warning devices and what to do when signals are activated.

e. Special procedures. Where it is not possible to reduce the magnitude of the risk factors through system design or the use of safety or warning devices, the contractor shall develop appropriate emergency procedures to effectively limit initiation of hazardous sequences. Provisions shall be made to

train personnel regarding the use of these procedures. Demonstrations shall verify the effectiveness of such procedures. Control of hazardous conditions by procedure alone shall be carried as a safety concern and shall require approval by the System Safety Manager, contractor program manager and the purchasing office for risk acceptance.

5.1.3 Design criteria. The contractor shall establish safety design criteria derived from all applicable data sources including compliance documents, reference documents, and the preliminary hazard analysis. This criteria shall be the basis for developing system specification safety requirements. The contractor shall continue to expand the criteria and requirements for inclusion in development specifications during the subsequent program phases. Safety criteria, requirements and an assessment of compliance, will be presented at appropriate program milestones such as preliminary design review (PDR) and critical design review (CDR) and at scheduled safety reviews. The contractor shall implement a closed loop system for assuring corrective action initiation and close-out for all safety related open items resulting from design and safety reviews.

5.1.4 Deviations. Contractor compliance with all contractually imposed technical and policy safety requirements is mandatory unless the exceptions are approved by the contracting officer. Requests for deviation will be prepared by the responsible contractor program function and submitted through the system safety manager to the purchasing office. The request shall include:

a. Identification of document, paragraph number, and full statement of the requirement.

b. Statement of the exception being requested.

c. Detailed description of the proposed equivalent requirement, policy method, or process to be used.

d. When requesting deviation of any contractually imposed technical system safety requirement, complete detailed technical justification for the exception, including analysis to show that the accident risk of the proposed alternate requirement, method, or process is equal to or less than it would be with the specified requirement.

e. Statement of impact should the exception be disapproved.

After approval by the system safety manager, the request will be processed in accordance with provisions of the contract. Deviations approved by the contracting officer will be maintained as an appendix to the accident risk assessment report.

5.2 System safety analyses. The contractor shall subject the system to a continuous iterative process of systematic accident risk identification by qualitative analysis. System safety analyses and their interrelations are discussed in the following subparagraphs. Qualitative analyses shall include the techniques of independent systems safety engineering analysis, or other related analyses and utilization of system safety check lists. Each identified accident risk factor shall be resolved and verified in accordance with paragraph 5.2.12 before being considered closed. Any accident risk factor that can not be resolved and verified in accordance with paragraph 5.2.12 or any safety check list noncompliance item shall be considered as a safety concern and will require program management action. The contractor shall require documentation of contracting office decisions, if any, to accept risks associated with an identified safety concern. Such documentation shall be included in the accident risk assessment report. While the analyses are listed as separate tasks, they are to be performed as a continuous effort commensurate with the program phase.

5.2.1 Preliminary hazards analysis. The contractor shall perform a preliminary hazard analysis to provide an initial evaluation of safety critical aspects and accident risk factors. Listed below are representative safety critical subsystems and operations associated with a typical flight vehicle:

a. General.

(1) Handling operations: transportation, lifting, or rotation of vehicle elements or major assemblies; mating/demating of stages, spacecraft or payload with booster stage.

(2) Radioactive components and materials (see 4.12) and 4.13.

(3) Cryogenic fluid handling operations, propellant handling operations, system leak tests.

b. Specific System Considerations.

(1) Propellant loading systems, safe and arm provisions, ignition control, propellant conditioning such as specified mixing ratios of propellants and ambient environmental conditions, leak checks, system activation, and safing. Solid motor assembly and test.

(2) Pressurization system: proof or leak checks, loading and off-loading of pressurants, emergency detanking, venting decontamination and disposal, toxic limits, ecological impacts, propellant tank pressurization control, emergency depressurization, post-mission safing, and aborted mission safing.

(3) Attitude control system: leak checks, propellant and pressurant loading or offloading, system activation, and safing.

(4) Ordnance: handling, transporting, installing and removing, connecting and disconnecting, checkout, storage and safing for aborted missions in all phases of pre-mission and post mission activities.

(5) Electrical power: handling, installing, connecting and activating batteries, connecting and power-up or power-down of ground or flight vehicle power supplies, and emergency removal of power supplies.

(6) Guidance, navigation, and control: attitude and guidance control during separation operations.

(7) Communications: Transmission of safety critical systems data and reception of commands to control/override safety critical functions and range destruct command uplink.

(8) Computerized sequences: Control of safety critical functions by computer issued discretes to sequence the system.

(9) Instrumentation: Sensing and measurement of safety critical parameters, including those of caution and warning displays.

(10) Structural interfaces: Payload attachments and stage or spacecraft separation provisions.

(11) Lasers: all operations involving lasers.

The complete list of safety critical aspects, including associated accident risk factors developed as a result of the preliminary hazards analysis, shall be refined as designs and operational planning develop and shall provide the basis for all subsequent analysis activities.

5.2.2 System safety checklist. The contractor shall ensure that safety requirements have been satisfied by use of suitable checklists or other effective means and a closed loop system verification. The requirement source and verification of implementation by reference to the applicable specification, drawing, procedure etc., shall be provided for each checklist item. The close-out action shall be signed off by the safety manager and the applicable subsystem managers. Each noncompliance item shall be documented by a hazard report and satisfactorily resolved before being closed. A composite response will be presented at safety reviews as an assessment of compliance with requirements.

5.2.3 System hazard analysis. The contractor shall perform a subsystem and system level hazard analysis for each system element being developed to provide a comprehensive evaluation of the risk being assumed when each system element is put into operation. This analysis shall identify accident risk and establish design criteria and operational constraints to eliminate or control accident risk. The analysis shall consider all planned and contingency operations including production, deployment, maintenance, repair, handling, storage, transportation, testing, assembly and checkout, launch base operations, flight operations and disposal. Flight operations include launch or spacecraft separation and positioning in orbit for operation or reentry, and landing. The analysis shall cover those conditions which have accident potential and could result in personnel injury or damage to other system elements (launch vehicle, payload or reentry vehicle, stage vehicle, support equipment, facilities, ground crew, flight crew, etc.). Conditions which only result in performance degradation are considered to fall within the jurisdiction of the engineering and reliability functions.

5.2.4 Interface hazard analysis. The contractor shall analyze the interface and interactions between each system element being developed and all other system elements (launch vehicle, experiments, payload or reentry vehicle, stage vehicle, support equipment, facilities, ground crew, flight crew, etc.) to identify and control or eliminate all accident risk factors that could be transmitted across these interfaces within the parameters specified by paragraph 5.1 and applicable interface control documentation.

5.2.5 Integrated system hazard analysis. The contractor shall perform an integrated system level hazard analysis to provide a comprehensive evaluation of the risk being assumed when the assembled system is put into operation. This analysis shall identify accident risk, establish design criteria and operational constraints to eliminate or control accident risk, and provide the basis for final accident risk assessments. The analysis shall consider the complete system in all planned and contingency operations including production, deployment, maintenance, repair, handling, storage, transportation, testing, assembly and checkout, launch base operations, flight operations, and disposal. Flight operations include payload or spacecraft separation and positioning in orbit for operation or ballistic reentry and include those conditions which have accident potential and could result in damage to the launch vehicle, upperstage, experiments, spacecraft, or reentry vehicle. Conditions which only results in performance degradation are considered to fall within the jurisdiction of the engineering and reliability functions. The contractor shall assure that all interfaces within the system have been appropriately analyzed, and shall conduct such system level analyses as necessary to complete the integrated system hazard analysis.

5.2.6 Software safety analysis. The contractor shall analyze the software of a system element to identify and eliminate software errors, faults or deficiencies relating to safety critical commands and control functions. The analysis shall concentrate on potential errors in program requirements definition, design, logic, coding, input device, mathematics and maintenance and shall consider overlapping conditions to assure that a non-planned event does not occur because of two routines changing a set state. This task shall include review of computer program development specification, flows,

and forms "B". The analysis shall cover the human interface and the hardware/software interface and evaluate both the effect of the software on other system elements and the effect of other system elements on the software. The analysis shall assure safety critical functions are adequately protected by inhibits, interlocks or hardwire. The results of the software safety task shall be a primary input to the verification and validation software testing activity.

5.2.7 Integrated software safety analysis. The contractor shall perform an integrated system level software safety analysis to provide a comprehensive evaluation of the risk being assumed when the assembled system is subject to operation or use. This analysis shall identify and eliminate software errors, faults or deficiencies relating to safety critical commands and control functions. The analysis shall concentrate on potential errors in program requirements definition, design, logic, coding, input device, mathematics and maintenance and shall consider overlapping conditions to assure that a non-planned event does not occur at the interfaces of system elements because of two routines changing a set state. This task shall include review of computer program development specifications, flows, forms "B" and safety critical functions identified in paragraph 5.2.6 above for system elements. The analysis shall cover the human interface and the hardware/software interfaces across all system elements at the system level and evaluate both the effect of the software on all system elements and the effect of other system elements on the software. The analysis shall assure safety critical functions are adequately protected by inhibits, interlocks, or hardwire. The results of the software safety task shall be a primary input to the verification and validation software testing activity. The contractor shall assure that all interfaces within the system have been appropriately analyzed and shall conduct a system level software safety analysis as necessary to complete the integrated system analysis.

5.2.8 Operating hazard analysis. The contractor shall perform an operating hazard analysis for each system element being developed to ensure a systematic and complete evaluation of the functional aspects of the system. This analysis shall include developing safety sequence charts to identify tasks which require mandatory sequencing and whether or not concurrent tasks are permissible. The analysis shall be based on the system safety analysis and the test operations functional flow diagrams, and shall provide the basis for

inputs to detail test operation and maintenance plans and procedure review. Analysis or test shall verify design action to limit operation and interaction or sequencing of subsystems or components within the system element, as well as procedural control of accepted risks.

5.2.9 Integrated operating hazard analysis. The contractor shall perform an integrated system level operating hazard analysis to ensure a systematic and complete evaluation of the functional aspects of the system. This analysis shall include developing safety sequence charts to identify tasks which require mandatory sequencing and whether or not concurrent tasks are permissible. The analysis shall be based on the system safety analysis and the test operations functional flow diagrams, and shall provide the basis for inputs to detail test operation and maintenance plans and procedure review. Analysis or test shall verify design action to limit operation and interaction or sequencing of system elements as well as procedural control of accepted risks. The contractor shall assure that all interfaces within the system have been apppropriately analyzed and shall conduct such system level analyses as necessary to complete the integrated operating hazard analysis.

5.2.10 Test/operating/maintenance procedures. Each test, operating or maintenance procedure including computer controlled test sequences shall be reviewed by the system safety manager or his designated representative. The review shall be based on available data including the results of the system safety analysis and operating hazard analysis. Test, operating or maintenance procedures that involve or effect safety shall be designated as safety critical procedures. Each procedure shall be validated prior to the first operation. The system safety manager or his designated representative shall participate in the validation process. The system safety manager or his designated representative shall approve and sign each validated safety critical procedure when it meets all safety requirements and contains appropriate caution and warning notations. Deviations from approved safety critical procedures shall require reassessment of the procedure and approval of the system safety manager or his designated representative. The system safety manager or his designated representative will also review all changes to previously reviewed procedures to assure the changes do not impact or effect safety.

5.2.11 Related analyses. The hazard identification process shall not duplicate other program analyses but shall

utilize data produced by them. For example, the failure mode and effects analysis can be utilized to provide for identification of single or multiple failure points presenting accident potential. The analyses format and procedures shall include provisions for identification of safety critical failure modes. This does not mean, however, that these related analysis techniques can be substituted in total for the system safety analysis process.

5.2.12 Implementation and effectiveness verification. The contractor, as a part of the safety analyses, shall develop verification criteria for each identified accident risk factor. The verification criteria shall identify the method or combination of methods that will be used to assure that the proposed design or procedural solutions have been implemented and also assure that these solutions meet the program safety requirements. Verification methods include examination of specifications and drawing, review of procedures, independant analysis, inspection, demonstration, test, or combinations of these activities. Tests and demonstrations conducted shall conform to the requirements of 4.10. Verification of implementation and effectiveness shall be completed and documented on the hazard report (see 5.2.14.1) before any item will be considered closed. The system safety manager shall approve each item closed-out by signature on the hazard report.

5.2.13 Accident risk assessment. The contractor shall develop and implement a comprehensive accident risk assessment procedure comensurate with system safety and other program requirements to evaluate the overall accident risk and associated controls for the system element/s on contract. The accident risk assessment procedure shall be an integral part of the overall program risk management activity. The implementation of design and operation controls shall be balanced against cost, performance and schedule constraints. The accident risk assessment shall be a qualitative evaluation of the interrelationships between the applicable system elements including associated personnel, support equipment, software, and facilities. Accident risk assessment procedures shall apply to system development, trade-studies, operations planning and system modifications or changes. The accident risk assessment shall be measured against established accident risk acceptability parameters including those specified in para. 5.1. As a part of the accident risk assessment, the contractor shall review and evaluate the results of all system safety analyses and data, related engineering analyses and data, and applicable

test and operations analysis and data and shall conduct additional analysis, as required, to assure that safe operating limits and constraints have been established and that all accident risk factors have been identified and either satisfactorily eliminated or controlled within the specified accident risk acceptability parameters or designated as safety concerns. The accident risk assessment must clearly specify the additional accident risk involved with each safety concern. The additional accident risk must be accepted by the purchasing office before the safety concern is closed.

5.2.14 Analysis documentation. The contractor shall document and report the results of the analysis activities to provide required visability and tracibility for management decision and safety certification.

5.2.14.1 Hazard report. A hazard report for each accident risk factor including those conditions defined in 5.1.1.1 and non-compliance safety checklist items shall be prepared by the contractor system safety organization. Each hazard report shall include information on how the hazardous condition can propagate into an accident, the potential effects, and whether any established safety requirement has been violated. The hazard report will include recommended corrective action to be initiated. Schematic drawings with the critical paths or pertinent areas identified should be attached as necessary for illustration purposes. The hazard report shall be used to document the status of actions taken on each identified accident risk factor. The hazard report will be jointly resolved between the responsible engineering activity and the system safety organization. Close-out action shall provide traceability and shall be verified (see 5.2.12) and approved by the contractor system safety manager and program manager. The hazard reports shall be incorporated into a hazard log and included in the Accident Risk Assessment Report (see 5.2.14.2). Hazard report close-out action will be approved by the purchasing office in the course of accident risk assessment report approval as indicated on the contract CDRL.

5.2.14.2 Accident risk assessment report. The contractor shall prepare an accident risk assessment report for the system element/s on contract to verify that the system design and operational planning meet program requirements (Data Item Description DI-S-30565A). The report shall be based on the system safety analysis tasks that have been performed. The report shall provide a comprehensive

evaluation of the overall system accident risk, identify operating limits and constraints, and constitute the safety baseline for operational planning and system modifications.

5.3 Certification. The contractor shall prepare a certification of compliance with all established safety requirements to support the flight readiness certification for each test flight or flight from a test range. The certification of compliance and substantiating data shall be included in the accident risk assessment report. Prior to reuse of any flight hardware, or subsequent flights with the same type of system, the entire system shall be verified for: (1) Correction of any safety deficiency encountered on previous launches as directed by the Procuring Contracting Officer; (2) Safety impact of any changes; and (3) Detailed information on maintenance or refurbishment.

5.4 Safety data

5.4.1 Deliverable data. Deliverable safety data, as cited on the Contract Data Requirement List (CDRL), shall be presented in the format specified unless a modification has been approved by the contracting officer. Where no format is indicated, the contractor may use any format that presents the information in a comprehensible manner. Management approval and submittal of all safety data produced in compliance with this standard shall constitute certification that accuracy, completeness and validity of safety data has been attested to by a qualified system safety engineer (see paragraph 3.11) and that the system can be operated safely within the parameters specified by the accident risk assessment report (see 5.2.14.2).

5.4.2 Non-deliverable data. Information necessary for contractor's conduct of the system safety effort but not contractually required to be submitted shall be available for on-site review on request to persons authorized by the purchasing office.

5.4.3 Data acquisitions and dissemination. The contractor system safety manager shall:

a. Pursue an aggressive program of acquiring and maintaining current safety related information and data pertinent to the contract.

b. Establish a system of safety information feedback to their design and safety personnel and to those of their associate and subordinate contractors.

c. Maintain liaison with purchasing office data sources to obtain: (1) Safety data as a design aid to prevent repetitive design or procedural deficiencies; (2) Information on operational systems which are similar to the system under this contract and should be studied for past safety problems and their solutions; and (3) Authority for access of personnel to nonproprietary information on accident and failure causes and preventive measures in possession of Government agencies and contractors involved with those systems.

5.4.4 Data files. The contractor shall maintain safety related data generated on the program in the program safety data file. A log of all safety-significant documentation shall be maintained showing concurrence or non-concurrence, reasons for nonconcurrence and corrective action taken to resolve the problem. The log shall be available for review by the purchasing office. The system safety organization shall also organize and maintain frequently used reference data.

5.5 Training. Safety inputs to training programs shall be tailored to the personnel categories involved, and included in lesson plans and examinations. Safety training will include such subjects as: Hazard types, recognition, causes, effects, and preventive and control measures; procedures, checklists, and human error; safeguards, safety devices, and protective equipment; monitoring and warning devices; and contingency procedures. Safety training programs will be developed and provided for specific types and levels of personnel: i.e., managers, engineers and technicians involved in the design, product assurance, test, operations, production, and field support. Test, operations, and field support personnel will be certified as having completed a training course in safety principles and methods. Specific certification requirements will be established by a program certification board that includes the system safety manager as a member. Contractor safety training shall also include Government personnel who will be involved in contractor activities.

5.6 Audit program and program reviews. System safety audits shall be conducted by the system safety manager and on

a periodic basis by a contractor management team independent of the program. The audit shall measure the status of each safety task, interrelationship between safety and other program disciplines, identification and implementation of safety requirements/criteria, and documented evidence which reflects planned vs actual safety accomplishment. Each audit shall evaluate program milestones and safety program milestones, incompatibilities that require remedial corrective action, and safety outputs to program requirements. The contractor shall initiate postive corrective actions where deficiencies are revealed by the audits. The system safety manager shall also support Government system safety audits as may be directed by the purchasing office. Components, equipment, conditions, designs, or procedures which provide unusual safety problems, shall be audited. Audits shall include verification or corrective action on problems revealed by previous audits.

5.6.1 Subcontractor audits. Subcontractors shall be audited by the prime contractor to ensure that: (1) They are producing items whose design or quality will not degrade safety; (2) Safety analyses are conducted as required; and (3) Problems are being brought to the attention of their own program managers and prime contractor management.

5.6.2 Program reviews. The system safety manager shall participate in all scheduled program, safety and design reviews. Presentation of system safety program status and safety problems having program impact shall be included in each program review. Presentation of hazard analysis status, identification of unacceptable accident potentials, and hazard reduction status, shall be included in each formal system review.

6. NOTES

6.1 Data requirements of this standard shall not be delivered to the purchasing office unless specified by the Contract Data Requirements List (CDRL).

CUSTODIAN
AIR FORCE-19

PREPARING ACTIVITY
AIR FORCE-19
(PROJECT 1810-F019)

(BLANK PAGE)

APPENDIX

BIBLIOGRAPHY

The fundamental documents applicable to the safety program are listed below. They are included for reference purposes only and reflect the source of the requirements contained in this standard.

Military specifications

MIL-H-46855	Human Engineering Requirements for Military Systems, Equipment and Facilities

Military standards

MIL-STD-454	Standard General Requirements for Electronic Equipment (Requirement 1 - Safety)
MIL-STD-882	System Safety Program Requirements
MIL-STD-1385	Preclusion of Ordnance Hazards in Electromagnetic Fields, General Requirements for
MIL-STD-1247	Marking, Functions and Hazard Designations of Hose, Pipe and Tube Lines for Aircraft, Missile and Space Systems
MIL-STD-1472	Human Engineering Design Criteria for Military Systems, Equipment and Facilities
MIL-STD-1512	Electroexplosive Subsystems, Electrically Initiated, Design Requirements and Test Methods
MIL-STD-1522	Standard General Requirements for Safe Design and Operation of Pressurized Missile and Space Systems

single component or any human error which

Other military publications

DODI 5000.36	System Safety Engineering and Management
AFR 122-1	The Air Force Nuclear Safety Program
AFR 122-2	Nuclear Weapon System Safety Studies, Safety Rules, and Operations Reviews.
AFR 122-9	The Nuclear Safety Cross-Check Analysis and Certification Program for Weapon Systems Software
AFR 122-10	Nuclear Weapon System Safety Design and Evaluation Criteria
AFR 122-15	Nuclear Power System Safety Studies and Surveys
AFR 122-16	Nuclear Safety Review Procedures for Space Applications of Minor Radioactive Sources
AFETRM 127-1	Range Safety Manual, Volume 1
SAMTECM 127-1	Range Safety Manual, Volume 1
AFR 127-4	Investigating and Reporting US Air Force Mishaps
AFR 127-8	Responsibilities of USAF System Safety Engineering Programs
SAMSOP 127-5	SAMSO Standard Satellite System Safety Design Criteria
SAMSOR 127-8	System Safety Engineering
AFM-127-100	Explosive Safety Manual
AFM 127-200	Missile and Space Systems Accident/ Incident Investigations
AFM 127-201	Missile Accident Prevention
AFM 161-30	Chemical Rocket/Propellant Hazards

Non-Government publications

TOR-0076(6451-03)-2 Fracture Control Criteria for Space Shuttle Pressure Vessels and Pressurized Systems, Aerospace Corporation Report, dated 5 December 1975.

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

(See Instructions – Reverse Side)

1. DOCUMENT NUMBER	2. DOCUMENT TITLE

a. NAME OF SUBMITTING ORGANIZATION	4. TYPE OF ORGANIZATION *(Mark one)*
b. ADDRESS *(Street, City, State, ZIP Code)*	☐ VENDOR ☐ USER ☐ MANUFACTURER ☐ OTHER *(Specify)*: _____

5. PROBLEM AREAS

a. Paragraph Number and Wording:

b. Recommended Wording:

c. Reason/Rationale for Recommendation:

6. REMARKS

7a. NAME OF SUBMITTER *(Last, First, MI)* – Optional	7b. WORK TELEPHONE NUMBER *(Include Area Code)* – Optional
7c. MAILING ADDRESS *(Street, City, State, ZIP Code)* – Optional	8. DATE OF SUBMISSION *(YYMMDD)*

DD FORM 82 MAR 1426

PREVIOUS EDITION IS OBSOLETE.

INSTRUCTIONS: In a continuing effort to make our standardization documents better, the DoD provides this form for use in submitting comments and suggestions for improvements. All users of military standardization documents are invited to provide suggestions. This form may be detached, folded along the lines indicated, taped along the loose edge *(DO NOT STAPLE)*, and mailed. In block 5, be as specific as possible about particular problem areas such as wording which required interpretation, was too rigid, restrictive, loose, ambiguous, or was incompatible, and give proposed wording changes which would alleviate the problems. Enter in block 6 any remarks not related to a specific paragraph of the document. If block 7 is filled out, an acknowledgement will be mailed to you within 30 days to let you know that your comments were received and are being considered.

NOTE: This form may not be used to request copies of documents, nor to request waivers, deviations, or clarification of specification 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.

(Fold along this line)

(Fold along this line)

DEPARTMENT OF THE AIR FORCE

NO POSTAGE NECESSARY IF MAILED IN THE UNITED STATES

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE $300

BUSINESS REPLY MAIL
FIRST CLASS PERMIT NO. 73236 WASHINGTON D C.

POSTAGE WILL BE PAID BY THE DEPARTMENT OF THE AIR FORCE

SAMSO/AQM
P.O. BOX 92960
WORLDWAY POSTAL CENTER
LOS ANGELES, CA 90009