MIL-STD-882A
28 June 1977
SUPERSEDING
MIL-STD-882
15 July 1969

MILITARY STANDARD

SYSTEM SAFETY PROGRAM REQUIREMENTS

FSC MISC

DEPARTMENT OF DEFENSE
WASHINGTON, DC 20301

System Safety Program Requirements
MIL-STD-882A

1. This Military Standard is approved 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: HQ Air Force Systems Command (IGFS), Andrews AFB, Washington, DC 20334, by using the self-addressed Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter.

3. MIL-STD-882A is exempt from OMB approval action. It is considered technical information incident to the design, production, or operation of contract items and is not subject to review under provisions of paragraph 9b, attachment A, OMB Circular A-40, revised by OMB Transmittal Memorandum No. 1, February 10, 1976.

FOREWORD

The principal objective of a system safety program within the Department of Defense is to ensure that safety, consistent with mission requirements, is designed into systems, subsystems, equipment, and facilities, hereinafter referred to as systems.

DOD has approved this military standard for all DOD departments and agencies to use in developing system safety programs.

The degree of safety achieved in a system depends directly on management emphasis. Government and contractors will apply management emphasis to safety during the system acquisition process and throughout the life cycle of each system.

The success of the system safety effort depends on definitive statements for safety objectives and requirements by the managing activity and their translation into functional hardware. A formal safety program that stresses early hazard identification and elimination or control is the principal contribution of effective system safety. Selective application and the tailoring of this military standard shall be accomplished, as indicated herein, to specify the extent of contractual and DoD in-house compliance.

CONTENTS

CONTENTS (Continued)

THIS IS A

BLANK PAGE

1. SCOPE

1.1 Purpose. This standard provides uniform requirements for developing and implementing a system safety program of sufficient comprehensiveness to identify the hazards of a system and to ensure that adequate measures are taken to eliminate or control the hazards.

1.2 Application. This standard applies to DoD systems and facilities, including support, test, maintenance, and training equipment. It applies to all phases of the system life cycle; e.g., design, research and development, test and evaluation, production, operation and support, and modification and disposal. The requirements shall also be applied to DoD in-house programs.

1.3 Implementation.

1.3.1 System safety program. A system safety program shall be developed according to the requirements of this standard. The requirements for a system safety program shall be included in all applicable contracts negotiated by the DoD managing activities. These contracts include those negotiated (a) within each DoD agency, (b) by one DoD agency for another, and (c) by DoD for other government agencies. In addition, a system safety program will be developed for each DoD in-house program.

1.3.2 System safety program plan. System safety program planning shall be included in all phases of DoD system acquisition documentation. For major systems acquisition or planned acquisition, a system safety program plan shall be developed. For nonmajor programs, system safety program plans shall be developed based on criteria such as mishap risk or as specified by the managing activity. The managing activity will either develop the system safety program plan or the contractor shall develop the plan based on system safety program requirements established by the managing activity. System safety program plans shall describe in detail how the program will be organized and conducted to implement the requirements of sections 4 and 5 of this military standard.

1.3.3 Contractual requirements. Tailored system safety program requirements shall be specified in the contractual provisions to include input to the statement of work, contractor data requirements list (CDRL), general and special provision sections, annexes, and other contractual means. When a system safety program plan is required, the plan shall be submitted with the contractor's proposal and be subject to contract negotiation. Upon approval by the managing activity, the system safety program plan shall be an attachment to the contract, referenced in the statement of work, and become the basis for contractual requirements. Format and content requirements for a system safety program plan are included in the Appendix.

1.3.4 Applicability. Each provision of this standard shall be reviewed by the managing activity to determine extent of applicability. Tailoring may take the form of deletion, alteration, or addition to the statements in 3, 4, and 5 to adapt this standard to specific system characteristics, program management options, contractual structure or life cycle phases (see 4.2). In tailoring the tasks, the detail and depth of the effort shall be defined by the managing activity and incorporated in the appropriate contractual or other program documents.

1.3.5 Duplication of effort. The managing activity shall review the contract for duplication of effort between system safety program requirements and other elements of the program (e.g., reliability, maintainability, and human factors). This review may also be required of a contractor. System safety

program requirements and tasks shall be cross-referenced in the system safety program plan or other contract documentation to avoid duplication of effort by the managing activity and the contractor.

1.3.6 Conflicting requirements. The managing activity shall specify in the statement of work that when conflicting requirements or deficiencies are identified within system safety program requirements, the contractor shall submit notification, with supporting rationale and proposed alternatives, to the managing activity for resolution.

2. REFERENCED DOCUMENTS

Referenced documents are not included in this document. Referenced documents required to supplement this military standard shall be specified in system specifications and contractual documents.

3. DEFINITIONS

The following definitions apply to this standard.

3.1 Contractor. A private sector enterprise or the organizational element of DoD (as used in this standard) engaged to provide services or products within agreed limits specified by the managing activity.

3.2 Managing activity. The DoD organizational element of DoD that will plan, organize, direct, contract, and control tasks and associated functions appropriate to the life cycle phase of the system.

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

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

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

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

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

3.5 Safety. Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property.

3.6 System. A composite, at any level of complexity, of personnel, materials, tools, equipment, facilities, and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific production, support, or mission requirement.

3.6.1 Subsystem. An element of a system that, in itself, may constitute a system.

3.7 System safety. The optimum degree of safety within the constraints of operational effectiveness, time, and cost attained through specific application of system safety management and engineering principles whereby hazards are identified and risk minimized throughout all phases of the system life cycle.

3.8 System safety engineering. An element of system engineering requiring specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify, eliminate, or control system hazards.

3.9 System safety group. A formally chartered group of persons organized to assist the program manager in achieving the system safety objectives.

3.10 System safety management. An element of management that establishes the system safety program requirements and ensures the planning, implementation and accomplishment of tasks and activities to achieve system safety consistent with the overall program requirements.

3.11 System safety program. The combined tasks and activities of system safety management and system safety engineering that enhance operational effectiveness by satisfying the system safety requirements in a timely, cost-effective manner throughout all phases of the system life cycle.

3.12 System safety program plan (SSPP). A formal document that fully describes the planned safety tasks required to meet the system safety requirements, including organizational responsibilities, methods of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems.

4. GENERAL REQUIREMENTS

4.1 System safety program objectives. The system safety program shall define a systematic approach to ensure that:

a. Safety consistent with mission requirements is designed into the system in a timely, cost-effective manner.

b. Hazards associated with each system are identified and evaluated, and eliminated or controlled to an acceptable level throughout the entire life cycle of a system.

c. Historical safety data generated by other systems are considered and used, where appropriate.

d. Minimum risk is involved in accepting and using of new designs, materials, and production and testing techniques.

e. Retrofit actions required to improve safety are minimized through the timely inclusion of safety features during development and acquisition of a system.

f. Modifications do not degrade the inherent safety of the system.

g. Consideration is given to safety and ease of disposal and demilitarization of any hazardous materials associated with the system.

4.2 System safety program requirements related to life cycle phases. The system safety program requirements are related here to the life cycle of a major system to show how the requirements of this military standard will be met. When the system program is not designated as a major program, the phases will be related to the major system life cycle phases to determine the safety tasks required. The system safety program requirements relating to each life cycle phase shall be selectively applied and tailored depending on the intended use of the system. If the acquisition has been in process before establishing the requirement for a system safety program, system safety program requirements normally performed during earlier phases will be evaluated for applicability to ensure risk is minimized. In all cases, the system safety program should be developed to facilitate continuation of the system safety effort into subsequent phases of the life cycle sequence; i.e., program initiation, demonstration and validation, full-scale engineering development, and production and deployment (including operation, support, and disposal).

4.2.1 Milestone 0 - program initiation

4.2.1.1 Milestone 0. The system safety effort will support the definition of mission element needs by identifying safety deficiencies in existing or projected capability and by identifying opportunities for system safety to improve mission capability or reduce life cycle costs.

4.2.1.2 Program initiation phase. System safety tasks applicable to the program initiation phase are those required to evaluate the alternative system concepts under consideration for development and establish the system safety program consistent with the identified mission need and life cycle requirements. System safety tasks will include the following:

a. Evaluate all material, design features, procedures and operational concepts and environments under consideration which will affect safety throughout the life cycle.

b. Perform a preliminary hazard analysis (PHA) to identify hazards associated with each alternative concept.

c. Identify possible safety interface problems.

d. Highlight special areas of safety consideration, such as system limitations, risks, and man-rating requirements.

e. Review safe and successful designs of similar systems for consideration in alternative concepts.

f. Define the system safety requirements based on past experience with similar systems.

g. Identify safety requirements that may require waiver during the system life cycle.

h. Identify any safety design analysis, test, demonstration and validation requirements.

i. Document the system safety analyses, results, and recommendations for each promising alternative system concept.

j. Prepare a summary report of the results of the system safety tasks conducted during the program initiation phase to support the decision-making process.

k. Tailor the system safety program for the subsequent phases of the life cycle and include detailed requirements in the appropriate demonstration and validation phase contractual documents.

4.2.2 Demonstration and validation phase. System safety tasks during the demonstration and validation phase will be tailored to programs ranging from extensive study and analyses through hardware development to prototype testing, demonstration and validation. System safety tasks will include the following:

a. Prepare or update the SSPP to describe the proposed integrated system safety effort planned for the demonstration and validation phase.

b. Perform or update the PHA performed during the program initiation phase. Prepare a PHA report of the proposed system concept in its intended use and operational environment.

c. Identify those technology, design, production, and operational and support (O&S) risks having an impact on safety.

d. Establish system safety requirements and criteria for verifying that requirements have been met.

e. Participate in tradeoff studies to reflect the impact on system safety requirements and risk. Recommend system design changes based on these studies to ensure that the optimum degree of safety is achieved consistent with performance and system requirements.

f. Identify for inclusion in the appropriate specifications any qualitative and quantitative system safety requirements for the system. Include contractor-furnished equipment, government-furnished equipment, ground support equipment, and all interfacing and ancillary equipment.

g. Perform subsystem, system, and operating and support (O&S) hazards analyses.

h. Review all test plans to ensure safe conduct of the tests.

i. Ensure that hazards identified by analyses and tests are eliminated or controlled.

j. Review training plans and programs for adequate safety considerations.

k. Evaluate results of failure analyses and mishap investigations recorded during the demonstration and validation phase. Recommend redesign or other corrective action.

l. Ensure that system safety requirements are incorporated into the system specification based on updated system safety studies, analyses, and tests.

m. Prepare a summary report of the results of the system safety tasks conducted during the demonstration and validation phase to support the decision-making process.

n. Continue to tailor the system safety program. Prepare an SSPP for the full-scale engineering development phase and initial production phase.

4.2.3 Full-scale engineering development phase. To provide support to the system engineering program, the system safety tasks during the full-scale engineering development phase will include the following:

a. Ensure effective and timely implementation of the SSPP for the full-scale engineering development phase.

b. Review preliminary engineering designs to ensure that safety design requirements are incorporated and hazards identified during the demonstration and validation phase are eliminated or controlled.

c. Update system safety requirements in system specifications.

d. Perform or update subsystem, system, and O&S hazard analyses and safety studies concurrent with the design/test effort to identify design and operating and support hazards. Recommend any required design changes and control procedures.

e. Identify testing facilities, test requirements, specifications, and criteria to ensure that design safety is verified. Review the test plans and programs to ensure safe conduct of the tests.

f. Participate in technical design and program reviews and present results of subsystem, system, and O&S hazard analyses.

g. Identify and evaluate the effects of storage, shelf-life, packaging, transportation, handling, test, operation, and maintenance on the safety of the system and its components.

h. Evaluate results of failure analyses and mishap investigations recorded during full-scale engineering development. Recommend redesign or other corrective action.

i. Identify, evaluate, and provide safety considerations for tradeoff studies.

j. Review appropriate engineering documentation (drawings, specifications, etc.) to ensure safety considerations have been incorporated.

k. Review, and provide safety inputs to, preliminary system operation and maintenance publications.

l. Verify the adequacy of safety and warning devices, life support equipment, and personal protective equipment.

m. Provide safety inputs to training courses.

n. Review the preliminary production engineering effort including purchase specifications, process quality control, inspection and acceptance, and test procedures to ensure that safety in the process and end product is established and maintained during production.

o. Ensure requirements are developed for demilitarization and for safe disposal of hazardous materials and equipment.

p. Prepare a summary report of the results of the system safety tasks conducted during the full-scale engineering development phase to support the decision-making process.

q. Tailor system safety program requirements for the production and deployment phase.

4.2.4 Production and deployment phase. As part of the on-going system safety program, the system safety tasks during the production and deployment phase will include the following:

a. Prepare or update the SSPP to reflect the system safety program requirements for the production and deployment phase.

b. Identify critical parts and assemblies, production techniques, assembly procedures, facilities, testing, and inspection requirements which may affect safety and will ensure:

(1) Adequate safety provisions are included in the planning and layout of the production line to establish safety control of the system within the production process and operations.

(2) Adequate safety provisions are included in inspections, tests, procedures, and checklists for quality control of the equipment being manufactured so that safety achieved in design is maintained during production.

(3) Production technical manuals or manufacturing procedures contain required warnings, cautions, and special procedures.

c. Verify that testing and evaluation is performed on early production hardware to detect and correct safety deficiencies at the earliest opportunity.

d. Review test plans and programs to ensure safe conduct of the tests.

e. Review warnings, cautions, and special procedures required for safe operation and maintenance.

f. Review procedures for storage, packaging, handling, and transportation to ensure that safety is maintained.

g. Review procedures and monitor results of periodic field inspections or tests (including recall-for-tests) to ensure acceptable levels of safety are maintained. This includes identifying major or critical characteristics of safety significant items that deteriorate with age, environmental conditions, or other factors.

h. Update hazard analyses to identify any new hazards that may result from engineering changes. Ensure that the safety implications of the changes are considered in all configuration control actions.

i. Evaluate results of failure analyses and mishap investigations. Recommend corrective action.

j. Monitor the system throughout the life cycle to determine the adequacy of the design, and operating, maintenance, and emergency procedures.

k. Conduct a safety review of proposed new operating and maintenance procedures, or changes, to ensure that the procedures, warnings, and cautions are adequate and inherent safety is not degraded. These reviews shall be documented as updates to the O&S hazards analyses.

l. Analyze safety deficiency reports submitted by operating and support personnel.

m. Review capability and procedures for demilitarization and disposal of hazardous material and equipment.

n. Document hazardous conditions and system deficiencies for development of follow-on requirements for modified or new systems.

o. Update safety documentation, such as design handbooks, military standards and specifications, to reflect safety "lessons learned".

5. DETAILED REQUIREMENTS

5.1 Development of the system safety program. A total program shall be developed in which design analyses, studies, and testing will identify system performance limitations, failure modes, safety margins, and critical operator tasks. All known facets of safety optimization including design, engineering, education, management policy and supervisory control shall be considered in the identifying and eliminating or controlling hazards. System safety management and engineering shall be integrated with other management and engineering disciplines in the interest of an optimum system design. Procedures for development and integration of the system safety effort shall be applied across the managing activity/contractor interface to assure a system safety program consistent with overall system requirements.

5.1.1 Managing activity responsibilities. The managing activity shall:

a. Establish, plan, organize, and implement an effective system safety program that is integrated into all life cycle phases.

b. Establish definitive system safety program requirements for the procurement or development of a system. The requirements shall be set forth clearly in the appropriate system specifications and contractual documents and define:

(1) In the appropriate system specifications, the system safety performance and design requirements that are available and applicable.

(2) In the statement of work, the system safety requirements that cannot be defined in the system specifications. This would include general design guidelines in 5.4.1.

(3) In the statement of work and CDRL as applicable, the specified safety data; e.g., analyses, tests, or progress reports that will be required during the scope of the effort.

c. Ensure that an SSPP is prepared that reflects in detail how the total program is to be conducted.

d. Review and approve for implementation the SSPPs prepared by the contractor.

e. Supply historical safety data as available.

f. Monitor contractors' system safety activities and review and approve deliverable data, if applicable, to ensure adequate performance and compliance with system safety requirements.

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

h. Evaluate new design criteria for inclusion into military specifications and standards and submit recommendations to the respective responsible organization.

i. Establish system safety groups as appropriate to assist the program manager in developing and implementing a system safety program.

5.1.2 Contractor responsibilities. The contractor shall:

a. Develop and submit an SSPP describing the proposed integrated safety effort in response to the specific requirements at the managing activity.

b. Establish a system safety organization or function that shall manage and perform the overall system safety program.

c. Ensure effective and timely implementation of the SSPP, approved by the managing activity, and the system safety program in accordance with the contractual requirements.

d. Establish interfacing procedures to subcontractors to meet the requirements of the managing activity.

e. Support system safety group activities as required by the managing activity and according to the contractual requirements.

5.2 System safety organization. A system safety organization shall be provided for the conduct and management of the system safety program for both the managing activity and contractor. The responsibilities and functions of those directly associated with system safety policies and implementation of the program shall be clearly defined. The authority delegated to this organization and the relationship between line, staff, and interdepartmental, project, functional, and general management organization shall be identified. Personnel assigned to the system safety program shall be identified including their qualifications, specific experience, and formal education or training.

5.3 System safety program milestones and reviews. Each system safety program shall be planned to provide for periodic status reviews, presentations of hazard analyses and risk assessments, and evaluation of the overall effectiveness of the system safety effort. These reviews and assessments, conducted jointly by the managing activity and contractor, shall be performed concurrently with the appropriate program milestones. System safety shall be an agenda item of the appropriate scheduled program or design review held for the system to assess the status of compliance with the system safety requirements. These reviews shall identify any deficiencies of the system with respect to safety and provide guidance for further development. At the discretion of the managing activity, a system safety group may be established for selected systems or additional ad hoc safety reviews may be scheduled as required.

5.4 System safety requirements. System safety requirements establish design and operational safety criteria for hazard elimination or control and may establish a quantitative value designating the level of system safety.

5.4.1 General requirements. System designs and operational procedures should consider the following:

a. Review pertinent standards, specifications, regulations, design handbooks, and other sources of design guidance for applicability to the design of the system.

b. Eliminate or control hazards identified by analyses or related engineering efforts through design solution, material selection, or substitution. Potentially hazardous materials (e.g., propellants, explosives, hydraulic fluids, solvents, lubricants or fuels) shall be selected to provide optimum safety characteristics.

c. Isolate hazardous substances, components, and operations from other activities, areas, personnel, and imcompatible materials.

d. Locate equipment so that access during operations, maintenance, repair, or adjustment minimizes personnel exposure to hazards (e.g., hazardous chemicals, high voltage, electromagnetic radiation, cutting edges, or sharp points).

e. Minimize hazards resulting from excessive environmental conditions (e.g., temperature, pressure, noise, toxicity, acceleration and vibration).

f. Design to minimize human error in the operation and support of the system.

g. Consider alternate approaches to minimize hazards that cannot be eliminated. Such approaches include interlocks, redundancy, failsafe design, system protection, fire suppression, and protective clothing, equipment, and devices.

h. Protect the power sources, controls and critical components for redundant subsystems by physical separation or shielding.

i. Provide suitable warning and caution notes in assembly, operations, maintenance, and repair instructions, and distinctive markings on hazardous components, equipment, or facilities to ensure personnel and equipment protection. These shall be standardized in accordance with the requirements of the managing activity.

j. Minimize the severity of personnel injury or damage to equipment in the event of a mishap (e.g., by incorporating crashworthy design features in all man-rated systems).

k. Review design criteria for inadequate or overly restrictive requirements regarding safety. Recommendations should be made for new design criteria supported by study, analyses, or test data.

5.4.2 System safety precedence. The order of precedence for satisfying system safety requirements and resolving identified hazards shall be as specified:

a. Design for minimum hazard. From the first, design to eliminate hazards. If an identified hazard cannot be eliminated, control hazards through design selection.

b. Safety devices. Hazards that cannot be eliminated or controlled through design selection shall be controlled to an acceptable level through the use of fixed, automatic, or other protective safety design features or devices. Provisions shall be made for periodic functional checks of safety devices.

c. Warning devices. When neither design nor safety devices can effectively eliminate or control an identified hazard, devices shall be used to detect the condition and to generate an adequate warning signal to correct the hazard or provide for personnel evacuation. Warning signals and their application shall be designed to minimize the probability of incorrect personnel reaction to the signals and shall be standardized within like types of systems.

d. Procedures and training. Where it is impossible to eliminate or adequately control a hazard through design selection or use of safety and warning devices, procedures and training shall be used to control the hazard. Procedures may include the use of personal protective equipment. Precautionary notations shall be standardized as specified by the managing activity. Safety critical tasks and activities may require certification of personnel proficiency.

5.4.3 Risk assessment. A risk assessment procedure commensurate with the system safety requirements shall be developed to establish priorities for corrective action and resolution of identified hazards. Since the priority for system safety is eliminating hazards by design, a risk assessment procedure considering hazard severity only will generally suffice during the early design phase to minimize hazards. When hazards are not eliminated during early design, a risk assessment procedure based upon the hazard probability, as well as hazard severity, may be required to establish priorities for corrective action and resolution of identified hazards. An example of a risk assessment is a numeric rank ordering of a mathematical combination arrived at by assigning numerical values to severity category and probability level.

5.4.3.1 Hazard severity. Hazard severity categories are defined to provide a qualitative measure of the worst potential consequences resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, system, subsystem or component failure or malfunction as follows:

a. Category I - Catastrophic. May cause death or system loss.

b. Category II - Critical. May cause severe injury, severe occupational illness, or major system damage.

c. Category III - Marginal. May cause minor injury, minor occupational illness, or minor system damage.

d. Category IV - Negligible. Will not result in injury, occupational illness, or system damage.

These hazard severity categories provide guidance to a wide variety of programs. However, adaptation to a particular program may be required. This adaptation may include definite transition points between categories and further definition of the degree of injury or damage.

5.4.3.2 Hazard probability. The probability that a hazard will occur during the planned life expectancy of the system can be described in potential occurrences per unit of time, events, population, items, or activity. Assigning a quantitative hazard probability to a potential design or procedural hazard is generally not possible early in the design process. A qualitative hazard probability may be derived from research, analysis, and evaluation of

historical safety data from similar systems. Supporting rationale for assigning a hazard probability shall be documented in hazard analysis reports. An example of a qualitative hazard probability ranking is:

Descriptive Word	Level	Specific Individual Item	Fleet or Inventory
Frequent	A	Likely to occur frequently	Continuously experienced
Reasonably Probable	B	Will occur several times in life of an item	Will occur frequently
Occasional	C	Likely to occur sometime in life of an item	Will occur several times
Remote	D	So unlikely, it can be assumed that this hazard will not be experienced	Unlikely to occur but possible
Extremely Improbable	E	Probability of occurrence cannot be distinguished from zero	So unlikely, it can be assumed that this hazard will not be experienced
Impossible	F	Physically impossible to occur	Physically impossible to occur

5.4.4 Action on identified hazard. Action shall be taken to eliminate or minimize hazards revealed by analyses or related engineering efforts. Catastrophic and critical hazards shall be eliminated or controlled. If these hazards cannot be eliminated or controlled to an acceptable level, the alternative controls and recommendations will be immediately presented to the managing activity. Hazard analyses and reports shall provide closed-loop procedures to ensure timely resolution of all identified hazards.

5.5 Hazard analyses. Analyses are performed to identify hazardous conditions to effect their elimination or control during all life cycle phases. Analyses shall be made to systematically examine the system, subsystem, facility, components, software, personnel, and their interrelationship including logistics, training, maintenance, test, modification, and operational environments. The analyses shall be accomplished to do the following:

a. Identify hazards, determine any needed corrective actions, and establish corrective action priorities.

b. Determine and evaluate safety considerations in tradeoff studies.

c. Determine and evaluate appropriate safety design and procedural requirements.

d. Provide documented evidence of compliance with specified safety tasks, objectives, and design requirements.

e. Support life-cycle-cost and design-to-cost analyses.

The selection of specific methods and techniques for performing these analyses is based on the level of complexity of the system element under consideration and the extent of system development. The hazard analyses methods and techniques selected for the system safety program should provide for continuity throughout the system life cycle and interfacing of results from one analysis to another to ensure identified hazards are corrected.

5.5.1 Analysis type, format and technique. Hazards analyses used in system safety are (a) preliminary hazards analysis (PHA) which is an initial safety assessment of the system, (b) subsystem hazard analysis (SSHA) which provides for hazard identification associated with the functional relationship of components and equipments comprising each subsystem, (c) system hazard analysis (SHA) which provides for hazard identification associated with subsystem interfaces, and (d) operating and support (O&S) hazard analyses which provide for an evaluation of procedural safety. Analyses may be qualitative or quantitative. The managing activity may specify the format and technique to be used for hazard analyses requiring submittal or integration. The format may be a structured or unstructured narration, a matrix chart, or a logic model. Models and techniques should be compatible with those being applied by other disciplines on the same program so that results are comparable.

5.5.1.1 Preliminary hazard analysis. A preliminary hazard analysis (PHA) shall be performed to obtain an initial risk assessment of a concept or system. The purpose of a PHA is to identify safety critical areas, evaluate hazards, and identify the safety design criteria to be used. The PHA effort shall be initiated during the program initiation phase or earliest life cycle phases of the program so that safety considerations are included in tradeoff studies and design alternatives. Based on the best available data, hazardous conditions associated with the proposed design or function should be evaluated for hazard severity, hazard probability, risk, and operational constraint. Safety provisions and alternatives needed to eliminate or control hazardous conditions should be considered. The information shall be used in the developing system safety requirements and in preparing performance and design specifications. Also, the PHA is the basic hazard analysis which establishes the framework for other hazard analyses and safety engineering evaluation of the design. The PHA should consider the following for identification of hazards:

a. Hazardous components (e.g., energy sources, fuels, propellants, explosives, and pressure systems).

b. Safety related interface considerations among various elements of the system (e.g., material compatibilities, electromagnetic interference and other possibilities of inadvertent activation, fire/explosive initiation and propagation).

c. Environmental constraints including the normal operating environments (e.g., drop, shock, extreme temperatures, noise and health hazards, fire, electrostatic discharge, lightning, X-ray, electromagnetic radiation, and laser radiation).

d. Operating, test, maintenance and emergency procedures (e.g., human error analysis of operator functions, tasks, and requirements; effect of environmental factors such as equipment layout and lighting requirements on human performance; life support requirements and their safety implications in manned systems; crash safety; egress, rescue, survival, and salvage).

e. Facilities, support equipmert, and training, (e.g., provisions for storage, assembly, checkout, prooftesting of hazardous systems/assemblies which may include toxic, flammable, explosive, corrosive or cryogenic fluids; electrical power sources; training and certification pertaining to safe operation and maintenance).

f. Safety related equipment, safeguards, and possible alternate approaches (e.g., interlocks, system redundancy, failsafe design considerations, subsystem protection, fire suppression systems, and personal protective equipment).

5.5.1.2 Subsystem hazard analysis. An analysis applied to some element of the total system is called a subsystem hazard analysis (SSHA). SSHA shall be performed to identify hazards associated with component failure modes and functional relationships of components and equipments comprising each subsystem. Such analysis should identify all components and equipments whose performance, performance degradation, functional failure, or inadvertent functioning could result in a hazard. The analysis should include a determination of the modes of failure including all single point failures and the effects on safety when failures occur in subsystem components. SSHA should normally be performed during the demonstration and validation phase and should be started as soon as the actual design of the subsystem has been refined to the point where detailed design information is available. The format for this analysis must be carefully established to minimize problems in integrating subsystem hazard analyses into the system hazard analysis. Techniques that may be used to complete the SSHA include:

a. Fault hazard analysis - An inductive method of analysis which can be used exclusively as a qualitative analysis, or, if desired, expanded to a quantitative one. The fault hazard analysis requires a detailed investigation of the subsystem to determine component hazard modes, causes of those hazards, and resultant effects to the subsystem and its operation.

b. Fault tree analysis - A deductive analytical tool used to analyze all events, faults, and occurrences and all their combinations that could cause or contribute to the occurrence of a defined undesired event. A qualitative or quantitative analysis may be conducted.

c. Sneak circuit analysis - Conducted on hardware and software to identify latent (sneak) circuits and conditions that inhibit desired functions or cause undesired functions to occur, without a component having failed. The analysis employs recognition of topological patterns which are characteristic of all circuits and electrical/electronic systems.

5.5.1.3 System hazard analysis. System hazard analysis (SHA) shall be performed on subsystem interfaces to determine the safety problem areas of the total system. Techniques similar to those used for the SSHA should be used. Such analyses should include a review of subsystems interrelationships for:

a. Compliance with safety criteria.

b. Possible independent, dependent, and simultaneous failures that could present a hazardous condition including failures of safety devices.

c. Degradation in the safety of a subsystem or the tot[illegible]ystem from normal operation of another subsystem.

d. Changes that occur within subsystems so th[illegible] the system hazard analysis can be updated accordingly.

5.5.1.4 Operating and support hazard analyses. Operating and support (O&S) hazard analyses shall be performed to identify and control hazards and determine safety requirements for personnel, procedures, and equipment used in production, installation, maintenance, testing, modification, transportation, storage, operation, emergency escape, egress, rescue, training, and disposal during all phases of intended use as specified in the system requirements. The O&S hazard analyses begun in the demonstration and validation phase should be oriented to development and operational testing. As the life cycle proceeds to production and deployment, O&S problems should be included. The analyses will also address hazards to the system that may be induced by maintenance personnel. Engineering data, procedures, and instructions developed from the engineering design and initial test programs should be used in support of this effort. Results of these analyses should provide the basis for:

a. Identifying a hazardous time period and actions required to minimize risk during this time.

b. Design changes to eliminate and control hazards.

c. Identifying requirements for safety devices and equipment and required maintenance procedures to detect their functional failure.

d. Warnings, cautions, and special and emergency procedures for operating and maintenance.

e. Special procedures for handling, storage, transportation, maintenance, and modification.

5.6 System safety data

5.6.1 Acquisition and use of safety data. Safety data shall be used as an aid to prevent design deficiencies, particularly those of a repetitive nature. Safety data are accumulated from prior programs, similar systems, earlier work on an on-going program, and other historical sources. The data are used to evaluate the safety of a system, or verify compliance with the system safety requirements. These data shall include: (a) mishap reports, (b) mishap probabilities, (c) failure rates, (d) test results, (e) system safety analyses, (f) failure mode and effects analyses, and (g) human factors data. Liaison with other data sources shall be sought and maintained to identify hazards and evaluate safety design deficiencies.

5.6.2 Mishap reporting. The managing activity will specify requirements for reporting mishaps or malfunctions during the system safety program.

5.6.3 Deliverable data. The managing activity will specify the deliverable safety data requirements in the contractor data requirements list (DD Form 1423) attached to a request for proposal, invitation for bid, or the contract, as appropriate. The SSPP and other required system safety data and reports submitted by the contractor will be subject to review and approval by the managing activity as specified in the CDRL.

5.6.4 Nondeliverable data. Nondeliverable data shall be indexed, filed, and maintained by the contractor for the time specified by the managing activity. The data shall be made available at the contractor's facility for review and use by authorized representatives of the managing activity upon request.

5.7 Safety testing and demonstrations. Tests and demonstrations shall be defined to validate selected safety features of the system. Tests or demonstrations shall be performed on safety critical equipment and procedures to determine the hazard severity or to establish the margin of safety of the design. Induced or simulated failures will be considered to demonstrate the failure mode and acceptability of safety critical equipment. Where hazards are identified during the development effort and it cannot be analytically determined whether the action taken will adequately control the hazard, safety tests shall be conducted to evaluate the effectiveness of the controls. Subsequent SSPPs and test program plans shall be revised to include these tests. 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, when approved by the managing activity. Specific safety tests shall be integrated into appropriate system test and demonstration plans to the maximum extent possible. Test plans, procedures, and test results for all tests including design verification, operational evaluation, production acceptance, and shelf-life validation shall 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, environment, etc., are properly identified and controlled.

5.8 Training. Approved safety procedures shall be included in instruction lesson plans and student examinations for the training of engineering, technician, operating and maintenance personnel. Safety and warning devices, personal protective equipment, and emergency equipment shall be identified.

5.9 Audit program. Techniques and procedures shall be implemented to ensure that the objectives and requirements of the system safety program are being accomplished. Procedures shall also be included for ensuring adequate on-the-job safety surveillance during system installation, checkout, maintenance, and modification activities.

5.10 Other safety matters. Specific requirements for other specialized safety activities (e.g., nuclear, range, explosive, chemical, biological, electromagnetic radiation, and lasers) shall be included as necessary to satisfy the requirements of the managing activity.

Custodians:
Army - AV
Navy - AS

Reviewer activities:
Army - AV, AT, EL, MU, MI
Navy - AS, OS/SH, YD, SA, EC
Air Force - 11, 13, 16, 19

Preparing activity:
Air Force - 10

Project No. MISC-0B11

APPENDIX

SYSTEM SAFETY PROGRAM PLAN

Format and content requirements for a system safety program plan shall be as specified by the managing activity and in accordance with one of the following data requirements:

DD Form 1664 identification number

DI-R-3531 (USAF)
DI-H-1320A (Army)
UDI-H-2041 (Navy)

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

INSTRUCTIONS: This form is provided to solicit beneficial comments which may improve this document and enhance its use. DoD contractors, government activities, manufacturers, vendors, or other prospective users of the document are invited to submit comments to the government. Fold on lines on reverse side, staple in corner and send to preparing activity. Attach any pertinent data which may be of use in improving this document. If there are additional papers, attach to form and place both in an envelope addressed to preparing activity. A response will be provided to the submitter, when name and address is provided, within 30 days indicating that the 1426 was received and when any appropriate action on it will be completed.

NOTE: This form shall not be used to submit requests for 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.

DOCUMENT IDENTIFIER *(Number)* AND TITLE

NAME OF ORGANIZATION AND ADDRESS OF SUBMITTER

☐ VENDOR ☐ USER ☐ MANUFACTURER

1. ☐ HAS ANY PART OF THE DOCUMENT CREATED PROBLEMS OR REQUIRED INTERPRETATION IN PROCUREMENT USE? ☐ IS ANY PART OF IT TOO RIGID, RESTRICTIVE, LOOSE OR AMBIGUOUS? PLEASE EXPLAIN BELOW.

A. GIVE PARAGRAPH NUMBER AND WORDING

B. RECOMMENDED WORDING CHANGE

C. REASON FOR RECOMMENDED CHANGE(S)

2. REMARKS

SUBMITTED BY *(Printed or typed name and address — Optional)*

TELEPHONE NO.

DATE

DD FORM 1426 1 OCT 76 PREVIOUS EDITION WILL BE USED.