S-08-01

MIL-STD-882B
30 March 1984
SUPERSEDING
MIL-STD-882A
28 June 1977

MILITARY STANDARD

SYSTEM SAFETY PROGRAM REQUIREMENTS

AMSC Number F3329

FSC SAFT

THIS DOCUMENT CONTAINS 98 PAGES.

114-00-1427

MIL-STD-882B
30 March 1984

DEPARTMENT OF DEFENSE
WASHINGTON, DC 20301

System Safety Program Requirements
MIL-STD-882B

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 (ALX ComSO), 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-882B 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 (DoD) is to make sure safety, consistent with mission requirements, is designed into systems, subsystems, equipment, and facilities, and their interfaces.

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, making sure mishap risk is understood and risk reduction is always considered in the management review process.

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

CONTENTS

APPENDIX A

GUIDANCE FOR IMPLEMENTATION OF SYSTEM SAFETY PROGRAM REQUIREMENTS

APPENDIX B

SYSTEM SAFETY PROGRAM REQUIREMENTS RELATED TO LIFE CYCLE PHASES

APPENDIX C

DATA REQUIREMENTS FOR MIL-STD-882B

TABLES

FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

SYSTEM SAFETY PROGRAM REQUIREMENTS

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 impose design requirements and management controls to prevent mishaps by eliminating hazards or reducing the associated risk to a level acceptable to the managing activity (MA). The term "managing activity" usually refers to the Government procuring activity, but may include prime or associate contractors or subcontractors who wish to impose system safety tasks on their suppliers.

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

1.3 Application.

1.3.1 Applying Tasks. Tasks described in this standard are to be selectively applied in DoD contract-definitized procurements, requests for proposal (RFP), statements of work (SOW), and Government in-house developments requiring system safety programs for the development, production, and initial deployment of systems, facilities, and equipment. The word "contractor" herein also includes Government activities developing military systems and equipment.

1.3.2 Tailoring of Task Descriptions. Task descriptions contained in Section 5 are to be tailored by the MA as required by governing regulations and as appropriate to particular systems or equipment program type, magnitude, and funding. In tailoring the tasks, the detail and depth of the effort is defined by the MA and incorporated in the appropriate contractual documents. When preparing proposals the contractor may include additional tasks or task modifications with supporting rationale for each addition or modification.

1.3.2.1 Details to be Specified. The "Details to be Specified" paragraph under each task description in Section 5 is intended for listing the specific details, additions, modifications, deletions, or options to the requirements of the task that should be considered by the MA when tailoring the task description to fit program needs. "Details to be Specified" annotated by an "(R)" are required and must be provided to the contractor for proper implementation of the task, if the task is to be contractually implemented.

1.3.2.2 Application Guidance. Application guidance and rationale for selecting tasks to fit the needs of a particular system safety program are included in appendices A and B. These appendices are generally not contractually binding; however, the MA may choose to impose portions of Appendix B as part of Task 100.

1.3.2.3 Method of Reference. When specifying the tasks of this standard as contractual requirements, both this standard and each specific task number are to be cited. Applicable "Details To Be Specified" will be included in the SOW.

1.3.3 Conflicting Requirements. When conflicting requirements or deficiencies are identified within system safety program requirements, the contractor shall submit notification, with proposed alternatives and supporting rationale, to the MA for resolution.

2. REFERENCED DOCUMENTS. Referenced documents are not included in this document. Referenced documents required to supplement this military standard must be specified in system specifications and other contractual documents.

3. DEFINITIONS AND ABBREVIATIONS.

3.1 Definitions. The following definitions apply:

3.1.1 Contractor. A private sector enterprise or the organizational element of DoD or any other Government agency engaged to provide services or products within agreed limits specified by the MA.

3.1.2 Damage. The partial or total loss of hardware caused by component failure; exposure of hardware to heat, fire, or other environments; human errors; or other inadvertent events or conditions.

3.1.3 Hazard. A condition that is prerequisite to a mishap.

3.1.4 Hazardous Event. An occurrence that creates a hazard.

3.1.5 Hazardous Event Probability. The likelihood, expressed in quantitative or qualitative terms, that a hazardous event will occur.

3.1.6 Hazard Probability. The aggregate probability of occurrence of the individual hazardous events that create a specific hazard.

3.1.7 Hazard Severity. An assessment of the worst credible mishap that could be caused by a specific hazard.

3.1.8 Managing Activity. The organizational element of DoD assigned acquisition management responsibility for the system, or prime or associate contractors or subcontractors who wish to impose system safety tasks on their suppliers.

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

3.1.10 Off-the-Shelf Item. An item determined by a material acquisition decision process review (DoD, Military Component, or subordinate organization as appropriate) to be available for acquisition to satisfy an approved

materiel requirement with no expenditure of funds for development, modification, or improvement (e.g., commercial products, materiel developed by other Government agencies, or materiel developed by other countries). This item may be procured by the contractor or furnished to the contractor as Government-furnished equipment (GFE) or Government-furnished property (GFP).

3.1.11 Risk. An expression of the possibility of a mishap in terms of hazard severity and hazard probability.

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

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

3.1.14 System. A composite, at any level of complexity, of personnel, procedures, 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.

3.1.15 System Safety. The application of engineering and management principles, criteria, and techniques to optimize safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.

3.1.16 System Safety Engineer. An engineer who is qualified by training and/or experience to perform system safety engineering tasks.

3.1.17 System Safety Engineering. An engineering discipline requiring specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, or reduce the risk associated with hazards.

3.1.18 System Safety Group/Working Group. A formally chartered group of persons, representing organizations associated with the system acquisition program, organized to assist the MA system program manager in achieving the system safety objectives. Regulations of the Military Components define requirements, responsibilities, and memberships.

3.1.19 System Safety Management. An element of management that defines the system safety program requirements and ensures the planning, implementation and accomplishment of system safety tasks and activities consistent with the overall program requirements.

3.1.20 System Safety Manager. A person responsible to program management for setting up and managing the system safety program.

3.1.21 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.

3.1.22 System Safety Program Plan. A description of the planned methods to be used by the contractor to implement the tailored requirements of this standard, including organizational responsibilities, resources, methods of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems.

3.2 Abbreviations. Abbreviations used in this document are defined as follows:

AE	Architect and Engineering Firm
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CPCI	Computer Program Configuration Item
DID	Data Item Description
DoD	Department of Defense
DOT	Department of Transportation
ECP	Engineering Change Proposal
EPA	Environmental Protection Agency
MA	Managing Activity
O&SHA	Operating & Support Hazard Analysis
OSHA	Occupational Safety and Health Administration
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
RFP	Request for Proposal
SHA	System Hazard Analysis
SOW	Statement of Work
SSG	System Safety Group
SSHA	Subsystem Hazard Analysis
SSPP	System Safety Program Plan
SSWG	System Safety Working Group

4. SYSTEM SAFETY REQUIREMENTS.

4.1 System Safety Program. The contractor shall establish and maintain a system safety program to support efficient and effective achievement of overall objectives.

4.2 System Safety Program Objectives. The system safety program shall define a systematic approach to make sure:

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, evaluated, and eliminated, or the associated risk reduced to a level acceptable to the MA throughout the entire life cycle of a system. Risk shall be described in risk assessment terms (see paragraph 4.5 below).

c. Historical safety data, including lessons learned from other systems, are considered and used.

d. Minimum risk is sought in accepting and using new designs, materials, and production and test techniques.

e. Actions taken to eliminate hazards or reduce risk to a level acceptable to the MA are documented.

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

g. Changes in design, configuration, or mission requirements are accomplished in a manner that maintains a risk level acceptable to the MA.

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

i. Significant safety data are documented as "lessons learned" and are submitted to data banks or as proposed changes to applicable design handbooks and specifications.

4.3 System Safety Design Requirements. System safety design requirements will be specified after review of pertinent standards, specifications, regulations, design handbooks and other sources of design guidance for applicability to the design of the system. Some general system safety design requirements are:

a. Eliminate identified hazards or reduce associated risk through design, including material selection or substitution. When potentially hazardous materials must be used, select those with least risk throughout the life cycle of the system.

b. Isolate hazardous substances, components, and operations from other activities, areas, personnel, and incompatible materials.

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

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

e. Design to minimize risk created by human error in the operation and support of the system.

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

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

h. When alternate design approaches cannot eliminate the hazard, provide warning and caution notes in assembly, operations, maintenance, and repair instructions, and distinctive markings on hazardous components and materials, equipment, and facilities to ensure personnel and equipment protection. These shall be standardized in accordance with MA requirements.

i. Minimize the severity of personnel injury or damage to equipment in the event of a mishap.

j. Design software controlled or monitored functions to minimize initiation of hazardous events or mishaps.

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

4.4 System Safety Precedence. The order of precedence for satisfying system safety requirements and resolving identified hazards shall be as follows:

a. Design for Minimum Risk. From the first, design to eliminate hazards. If an identified hazard cannot be eliminated, reduce the associated risk to an acceptable level, as defined by the MA, through design selection.

b. Incorporate Safety Devices. If identified hazards cannot be eliminated or their associated risk adequately reduced through design selection, that risk shall be reduced to a level acceptable to the MA 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 when applicable.

c. Provide Warning Devices. When neither design nor safety devices can effectively eliminate identified hazards or adequately reduce associated risk, devices shall be used to detect the condition and to produce an adequate warning signal to alert personnel of the hazard. 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. Develop Procedures and Training. Where it is impractical to eliminate hazards through design selection or adequately reduce the associated risk with safety and warning devices, procedures and training shall be used. However, without a specific waiver, no warning, caution, or other form of written advisory shall be used as the only risk reduction method for Category I or II hazards (as defined in paragraph 4.5.1 below). Procedures may include the use of personal protective equipment. Precautionary notations shall be standardized as specified by the MA. Tasks and activities judged critical by the MA may require certification of personnel proficiency.

4.5 Risk Assessment. Decisions regarding resolution of identified hazards shall be based on assessment of the risk involved. To aid the achievement of the objectives of system safety, hazards shall be characterized as to hazard severity categories and hazard probability levels, when possible. Since the priority for system safety is eliminating hazards by design, a risk assessment procedure considering only hazard severity will generally suffice during the early design phase to minimize risk. When hazards are not eliminated during the early design phase, a risk assessment procedure based upon the hazard probability, as well as hazard severity, shall be used to establish priorities for corrective action and resolution of identified hazards.

4.5.1 Hazard Severity. Hazard severity categories are defined to provide a qualitative measure of the worst credible mishap resulting from personnel

error; environmental conditions; design inadequacies; procedural deficiencies; or system, subsystem or component failure or malfunction as follows:

Description	Category	Mishap Definition
CATASTROPHIC	I	Death or system loss.
CRITICAL	II	Severe injury, severe occupational illness, or major system damage.
MARGINAL	III	Minor injury, minor occupational illness, or minor system damage.
NEGLIGIBLE	IV	Less than minor injury, occupational illness, or system damage.

These hazard severity categories provide guidance to a wide variety of programs. However, adaptation to a particular program is generally required to provide a mutual understanding between the MA and the contractors as to the meaning of the terms used in the category definitions. The adaptation must define what constitutes system loss, major or minor system damage, and severe and minor injury and occupational illness.

4.5.2 Hazard Probability. The probability that a hazard will be created 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:

Description*	Level	Specific Individual Item	Fleet or Inventory**
FREQUENT	A	Likely to occur frequently.	Continuously experienced
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	Unlikely but possible to occur in life of an item	Unlikely but can reasonably be expected to occur
IMPROBABLE	E	So unlikely, it can be assumed occurence may not be experienced	Unlikely to occur, but possible

*Definitions of descriptive words may have to be modified based on quantity involved.
**The size of the fleet or inventory should be defined.

4.6 Action on Identified Hazards. Action shall be taken to eliminate identified hazards or reduce the associated risk. CATASTROPHIC and CRITICAL hazards shall be eliminated or their associated risk reduced to a level acceptable to the MA. If this is impossible or impractical, alternatives shall be recommended to the MA.

5. TASK DESCRIPTIONS. The task descriptions are divided into two general sections: Section 100, Program Management and Control and Section 200, Design and Evaluation.

Custodians:
Army - AV
Navy - AS

Reviewing Activities:
Army - AV, AT, SC, AR, MI
Navy - AS, OS, SH, YD, SA, EC
Air Force - 11, 13, 19, 26

Preparing Activity
Air Force - 10

Project No. - SAFT-0002

TASK SECTION 100

PROGRAM MANAGEMENT AND CONTROL

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 100

SYSTEM SAFETY PROGRAM

100.1 Purpose. The purpose of Task 100 is to conduct a basic system safety program. The total system safety program is this task plus all other tasks in Sections 100 and 200 designated by the MA.

100.2 Task Description. Set up a system safety program which meets the requirements of Section 4., SYSTEM SAFETY REQUIREMENTS, and all other designated tasks in Sections 100 and 200.

100.3 Details to be Specified by the MA (Reference 1.3.2.1).

100.3.1 Details to be specified in the SOW shall include the following as applicable:

(R) a. Imposition of Task 100.

(R) b. Tailoring of Section 4 to meet specific program requirements.

(R) c. Acceptable level of risk.

d. Addition of other specific system safety program requirements.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 101

SYSTEM SAFETY PROGRAM PLAN

101.1 Purpose. The purpose of the Task 101 is to develop a system safety program plan (SSPP). It shall describe in detail tasks and activities of system safety management and system safety engineering required to identify, evaluate, and eliminate hazards, or reduce the associated risk to a level acceptable to the MA throughout the system life cycle.

101.2 Task Description. The contractor shall develop a SSPP to provide a basis of understanding between the contractor and the MA as to how the system safety program will be accomplished to meet contractual safety requirements included in the general and special provisions of the contract. The SSPP shall include the following:

101.2.1 Program Scope and Objectives. Each SSPP shall describe, as a minimum, the four elements of an effective system safety program: a planned approach for task accomplishment, qualified people to accomplish tasks, authority to implement tasks through all levels of management, and appropriate resources both manning and funding to assure tasks are completed. The SSPP shall define a program to satisfy the system safety requirements imposed by the contract. This section shall:

a. Describe the scope of the overall program and the related system safety program.

b. List the tasks and activities of system safety management and engineering. Describe the interrelationships between system safety and other functional elements of the program. Other program requirements and tasks applicable to system safety shall be listed including the identification of where they are specified or described.

101.2.2 System Safety Organization. The SSPP shall describe:

a. The system safety organization or function within the organization of the total program using charts to show the organizational and functional relationships, and lines of communication.

b. The responsibility and authority of system safety personnel, other contractor organizational elements involved in the system safety effort, subcontractors, and system safety groups. Identify the organizational unit responsible for executing each task. Identify the authority in regard to resolution of all identified hazards. Include the name, address and telephone number of the system safety program manager.

c. The staffing of the system safety organization for the duration of the contract to include manpower loading, control of resources and the

qualifications of key system safety personnel assigned, including those who possess coordination/approval authority for contractor prepared documentation.

d. The procedures by which the contractor will integrate and coordinate the system safety efforts including assignment of the system safety requirements to action organizations and subcontractors, coordination of subcontractor system safety programs, integration of hazard analyses, program and design reviews, program status reporting, and system safety groups.

e. The process through which contractor management decisions will be made including timely notification of unacceptable risks, necessary action, mishaps or malfunctions, waivers to safety requirements, program deviations, etc.

101.2.3 System Safety Program Milestones. The SSPP shall:

a. Define system safety program milestones.

b. Provide a program schedule of safety tasks including start and completion dates, reports, reviews, and estimated manpower loading.

c. Identify integrated system activities (i.e., design analyses, tests, and demonstrations) applicable to the system safety program but specified in other engineering studies to preclude duplication. Included as a part of this section shall be the estimated manpower loading required to do these tasks.

101.2.4 General System Safety Requirements and Criteria. The SSPP shall:

a. Describe general engineering requirements and design criteria for safety. Describe safety requirements for support equipment and operational safety requirements for all appropriate phases of the life cycle up to, and including, disposal. List the safety standards and system specifications containing safety requirements that shall be complied with by the contractor. Include titles, dates, and where applicable, paragraph numbers.

b. Describe the risk assessment procedures. The hazard severity categories, hazard probability levels, and the system safety precedence that shall be followed to satisfy the safety requirements of this standard. State any qualitative or quantitative measures of safety to be used for risk assessment including a description of the acceptable risk level. Include system safety definitions which deviate from or are in addition to those in this standard.

c. Describe closed-loop procedures for taking action to resolve identified hazards including those involving GFE and off-the-shelf equipment.

101.2.5 Hazard Analyses. The SSPP shall describe:

a. The analysis techniques and formats to be used in qualitative or quantitative analysis to identify hazards, their causes and effects, hazard elimination, or risk reduction requirements and how those requirements are met.

b. The depth within the system to which each technique is used including hazard identification associated with the system, subsystem, components, personnel, ground support equipment, GFE, facilities, and their interrelationship in the logistic support, training, maintenance, and operational environments.

c. The integration of subcontractor hazard analyses with overall system hazard analyses.

101.2.6 System Safety Data. The SSPP shall:

a. Describe the approach for researching, distributing, and analyzing pertinent historical hazard or mishap data.

b. Identify deliverable data by title and number.

c. Identify non-deliverable system safety data and describe the procedures for accessibility by the MA and retention of data of historical value.

101.2.7 Safety Verification. The SSPP shall describe:

a. The verification (test, analysis, inspection, etc.) requirements for making sure that safety is adequately demonstrated. Identify any certification requirements for safety devices or other special safety features.

b. Procedures for making sure test information is transmitted to the MA for review and analysis.

c. Procedure for ensuring the safe conduct of all tests.

101.2.8 Audit Program. The SSPP shall describe the techniques and procedures to be employed by the contractor to make sure the objectives and requirements of the system safety program are being accomplished.

101.2.9 Training. The SSPP shall describe the safety training for engineering, technician, operating, and maintenance personnel.

101.2.10 Mishap and Hazardous Malfunction Analysis and Reporting. The contractor shall describe in the SSPP the mishap and hazardous malfunction analysis process including alerting the MA.

101.2.11 System Safety Interfaces. The SSPP shall identify, in detail:

a. The interface between system safety and all other applicable safety disciplines such as: nuclear safety, range safety, explosive and ordinance safety, chemical and biological safety, laser safety and any others.

b. The interface between system safety and all other support disciplines such as: maintenance, quality control, reliability, human factors engineering, medical support (health hazard assessments), and any others.

101.3 Details to be Specified by the MA (Reference 1.3.2.1).

101.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100 and 101.

(R) b. Identification of contractual status of the SSPP.

c. Identification of additional tasks to be performed or additional information to be provided.

d. Format, content, and delivery schedule including updates of any data required.

e. Requirements for reporting mishaps and hazardous malfunctions.

TASK 102

INTEGRATION/MANAGEMENT OF ASSOCIATE CONTRACTORS, SUBCONTRACTORS, AND ARCHITECT AND ENGINEERING FIRMS

102.1 Purpose. The purpose of Task 102 is to provide the system integrating contractor and MA with appropriate management surveillance of other contractors' system safety programs, and the capability to establish and maintain uniform integrated system safety program requirements. This task will also describe architect and engineering firms' (AE) system safety programs.

102.2 Task Description.

102.2.1 Integrating Contractor. The contractor designated as integrator for the safety functions of all associated contractors shall:

a. Prepare an integrated system safety program plan (ISSPP) as the SSPP required by Task 101 defining the role of the integrator and the effort required from each associate contractor to help integrate system safety requirements for the total system. In addition to the other contractually imposed requirements from this standard, the plan shall address and identify:

(1) Analyses, risk assessment, and verification data to be developed by each associate contractor with format and method 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 of 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 other interface requirement documentation.

(5) Safety-related data pertaining to off-the-shelf items.

b. Initiate action through the MA to make sure each associate contractor is required to be responsive to the ISSPP. Recommend contractual modification where the need exists.

c. When conducting risk assessments, examine the integrated system design, operations, and specifically the interfaces between the products of each associate contractor. Data provided by associate contractors shall be used in the conduct of this effort.

d. When performing a safety assessment, summarize the mishap risk presented by the operation of the integrated system.

e. Provide assistance and guidance to associate contractors regarding safety matters.

f. Resolve differences between associate contractors in areas related to safety, especially during development of safety inputs to system and item specifications. Where problems cannot be resolved by the integrator, notify the MA for resolution and action.

g. Initiate action through the MA to make sure information required by an associate contractor (from the integrating contractor or other associate contractors) to accomplish safety tasks, is provided in an agreed-to format.

h. Develop a method of exchanging safety information between contractors. If necessary, schedule and conduct technical meetings between all associate contractors to discuss, review, and integrate the safety effort.

i. Implement an audit program to make sure the objectives and requirements of the system safety program are being accomplished.

102.2.2 Associate Contractor. Associate contractors shall provide safety data and support needed by other associate contractors and the integrator until the integrator decides that such support is no longer necessary and that decision is approved by the MA.

102.2.3 Subcontractors. Applicable provisions of this standard shall be included in all contracts with major subcontractors.

a. 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.

b. Major subcontractors shall be required to develop system safety program plans to be included as annexes to the prime contractor's SSPP.

c. 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.

102.2.4 Architect and Engineering Firms. The AE shall be responsible for conducting facility hazard analyses and other facility SSPP functions as specified in the SOW. The AE shall be responsible for securing the expertise necessary to perform the required work and will have the same responsibilities as a prime contractor in hazard identification, tracking, and resolution. The AE shall assure that design subcontrators or consultants maintain and provide suitable documentation of any safety analyses performed.

102.3 Details to be Specified by the MA (Reference 1.3.2.1).

102.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Designation of the system safety integrating contractor.

(R) b. Imposition of Tasks 100, 101 and 102 as tailored.

c. Format, content, and delivery schedule of any data required.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 103

SYSTEM SAFETY PROGRAM REVIEWS

103.1 Purpose. The purpose of Task 103 is to establish a requirement for the contractor to present system safety program reviews, to periodically report the status of the system safety program, and, when needed, to support special requirements such as certifications and first flight readiness reviews.

103.2 Task Description. The contractor shall provide system safety program reviews to periodically report to the MA the status of hazard analyses, safety assessments, and other parts of the system safety program. Also, when needed, the contractor shall support presentations to Government certifying activities such as munitions safety boards, nuclear safety boards, or flight safety review boards. These may also include special reviews such as first flight reviews or pre-construction briefings.

103.3 Details to be Specified by the MA (Reference 1.3.2.1).

103.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100 and 103.

b. Identification of reviews, their content, and probable location(s).

c. Method of documenting the results of system safety reviews.

d. Schedule for system safety reviews.

e. Delivery schedule for any data required prior to and after the reviews.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 104

SYSTEM SAFETY GROUP/SYSTEM SAFETY WORKING GROUP SUPPORT

104.1 Purpose. The purpose of Task 104 is to require contractors to support system safety groups (SSGs) and system safety working groups (SSWGs) which are established in accordance with service regulations or as otherwise defined by the MA.

104.2 Task Description. The contractor shall participate as an active member of MA SSG/SSWGs. Such participation shall include activities specified by the MA such as:

a. Presentation of the contractor safety program status, including results of design or operations risk assessments.

b. Summaries of hazard analyses including identification of problems and status of resolution.

c. Presentation of results of analyses of R&D mishaps and hazardous malfunctions including recommendations and action taken to prevent future recurrences.

d. Documentation and distribution of meeting agendas and minutes.

e. Responding to action items assigned by the chairman of the SSG/SSWG.

104.3 Details to be Specified by the MA (Reference 1.3.2.1).

104.3.1 Details to be specified in the SOW should include the following, as applicable:

(R) a. Imposition of Tasks 100 and 104.

(R) b. Contractor membership requirements and role assignments, e.g., recorder, member, alternate, or technical advisor.

(R) c. Frequency or total number of SSG/SSWG meetings and probable locations.

d. Specific SSG/SSWG support tasks.

e. Format, content, and delivery schedule of any data required.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 105

HAZARD TRACKING AND RISK RESOLUTION

105.1 Purpose. The purpose of Task 105 is to establish a single closed-loop hazard tracking system.

105.2 Task Description. The contractor shall develop a method or procedure to document and track hazards from identification until the hazard is eliminated or the associated risk is reduced to a level acceptable to the MA, thus providing an audit trail of hazard resolutions. A centralized file or document called a "hazard log" shall be maintained. The hazard log shall contain as a minimum:

a. Description of each hazard.

b. Status of each hazard.

c. Traceability of resolution action on each hazard from the time the hazard was identified to the time the risk associated with the hazard was reduced to a level acceptable to the MA.

105.3 Details to be Specified by the MA (Reference 1.3.2.1).

105.3.1 Details to be specified in the SOW shall include the following as applicable:

(R) a. Imposition of Tasks 100 and 105.

(R) b. Hazard threshold for inclusion in the hazard log.

c. Complete set of data required on the hazard log, including format.

d. Procedure by which hazards are entered into the log.

e. Procedure by which the contractor shall obtain close-out or risk acceptance by the MA of each hazard.

f. Format, content, and delivery schedule of any data required.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 106

TEST AND EVALUATION SAFETY

106.1 Purpose. The purpose of Task 106 is to make sure safety is considered in test and evaluation, to provide existing analysis reports and other safety data, and to respond to all safety requirements necessary for testing in-house, at other contractor facilities, and at Government ranges, centers, or laboratories.

106.2 Task Description. The contractor shall make sure the contractor test and evaluation safety activities recommend actions and evaluate actions taken to reduce or correct CATASTROPHIC and CRITICAL hazards in the test and evaluation environment. Specific test and evaluation safety activity tasks shall include the following:

106.2.1 Test and Evaluation Planning. Planning for test and evaluation safety from the beginning of the contract period to consider the following:

a. Test program milestones requiring completion of hazard analyses, risk assessments, or other safety studies.

b. Schedule for analysis, evaluation, and approval of test plans, procedures, and other documents to make sure safety is considered during all testing.

c. That test equipments, installation of test equipments, and instrumentation are considered in hazard analyses prior to test start.

d. Meeting specialized requirements designated by the MA and informing the MA of any identified hazards that are unique to the test environment.

106.2.2 Follow-up Actions. Initiating follow-up action to insure completion of the corrective efforts taken to reduce or correct test and evaluation hazards.

106.2.3 Reports. Maintaining a repository of test and evaluation hazard/action status reports.

106.3 Details to be Specified by the MA (Reference 1.3.2.1).

106.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100 and 106.

(R) b. Designation of applicable specialized system safety requirements for testing.

(R) c. Schedule for meeting requirements designated in 106.2 above.

d. Format, content, and delivery schedule of any data required.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 107

SYSTEM SAFETY PROGRESS SUMMARY

107.1 Purpose. The purpose of Task 107 is to provide a periodic progress report summarizing the pertinent system safety management and engineering activity that occurred during the reporting period.

107.2 Task Description. The contractor shall provide a periodic system safety progress report summarizing general progress made relative to the system safety program during the specified reporting period, and projected work for the next reporting period. The report shall contain the following information:

a. A brief summary of activities, progress, and status of the safety effort in relation to the scheduled program milestones. It shall highlight significant achievements and problems. It shall include progress toward completion of safety data prepared or in work.

b. Newly recognized significant hazards and significant changes in the degree of control of the risk of known hazards.

c. Status of all recommended corrective actions that have not been implemented.

d. Significant cost and schedule changes that impact the safety program.

e. Discussion of contractor documentation reviewed by safety during the reporting period. Indicate whether the documents were acceptable for safety content and whether or not inputs to improve the safety posture were made.

f. Proposed agenda items for the next system safety group/working group meeting, if such groups are formed.

107.3 Details to be Specified by the MA (Reference 1.3.2.1).

107.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100 and 107.

(R) b. Specification of progress reporting period.

c. Format, content, and delivery schedule of any data required.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 108

QUALIFICATIONS OF KEY CONTRACTOR SYSTEM SAFETY ENGINEERS/MANAGERS

108.1 Purpose. The purpose of Task 108 is to establish qualifications for key contractor system safety engineers and managers.

108.2 Task Description. The contractor shall assign and retain qualified individuals as key system safety engineers and managers. Key engineers and managers are those who possess coordination or approval authority for contractor documentation.

108.2.1 Principal System Safety Engineer/Manager. Qualifications of the principal system safety engineer or manager shall consist of one of each of the options in each of the following categories of education, training, and experience.

a. A minimum of a Bachelor of Science degree in engineering, applied or general science, or safety or business management.

b. Registration as a professional safety engineer in one of the states of the United States, or certification by the Board of Certified Safety Professionals in system safety.

c. Prior experience as a system safety engineer on a full-time basis on products or systems for a minimum of three (3) years during the preceding ten (10) years in at least one of the following functional areas:

1. System Safety Management
2. System Safety Analysis
3. System Safety Design
4. System Safety Research
5. System Safety Operations
6. System Safety Administration
7. System or Equipment Mishap Investigation
8. Human Factors Engineering
9. Task Analysis
10. Product Assurance Engineering
11. Reliability Engineering

108.2.2 Other Safety Engineers/Managers. Qualifications for other key safety engineers and managers shall be:

a. A minimum of a Bachelor of Science degree in engineering, applied or general science, safety or business management.

b. Prior degree related experience of two (2) years in a non-safety field or one (1) year in safety.

108.2.3 Waiver for Not Meeting Qualifications. The contractor shall submit a request for waiver if the principal system safety engineer does not meet the above qualifications.

108.3 Details to be Specified by the MA (Reference 1.3.2.1).

108.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100 and 108.

b. Specification of other minimum qualifications.

TASK SECTION 200

DESIGN AND ENGINEERING

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 201

PRELIMINARY HAZARD LIST

201.1 Purpose. The purpose of Task 201 is to compile a preliminary hazard list (PHL) very early in the system acquisition life cycle to enable the MA to choose any hazardous areas on which to put management emphasis.

201.2 Task Description. The contractor shall examine the system concept shortly after the concept definition effort begins and compile a PHL identifying possible hazards that may be inherent in the design. The contractor shall further investigate selected hazards or hazardous characteristics identified by the PHL as directed by the MA to determine their significance.

201.3 Details to be Specified by the MA (Reference 1.3.2.1).

201.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100 and 201.

b. Format, content, and delivery schedule of any data required.

c. Identification of special concerns.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 202

PRELIMINARY HAZARD ANALYSIS

202.1 Purpose. The purpose of Task 202 is to perform and document a preliminary hazard analysis (PHA) to identify safety critical areas, evaluate hazards, and identify the safety design criteria to be used.

202.2 Task Description. The contractor shall perform and document a preliminary hazard analysis to obtain an initial risk assessment of a concept or system. The PHA effort shall be started during the concept exploration 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, including mishap data from similar systems and other lessons learned, hazards associated with the proposed design or function shall be evaluated for hazard severity, hazard probability, and operational constraint. Safety provisions and alternatives needed to eliminate hazards or reduce their associated risk to a level acceptable to the MA shall be considered. The PHA shall consider the following for identification and evaluation of hazards as a minimum:

a. Hazardous components (e.g., fuels, propellants, lasers, explosives, toxic substances, hazardous construction materials, pressure systems, and other energy sources).

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

c. Environmental constraints including the operating environments (e.g., drop, shock, vibration, extreme temperatures, noise, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, electromagnetic environmental effects, ionizing and non-ionizing radiation including laser radiation).

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

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

f. Safety related equipment, safeguards, and possible alternate approaches (e.g., interlocks, system redundancy, hardware or software fail safe design considerations, subsystem protection, fire suppression systems, personal protective equipment, industrial ventilation, and noise or radiation barriers).

202.3 Details to be Specified by the MA (Reference 1.3.2.1).

202.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100 and 202.

b. Format, content, and delivery schedule of any data required, including minimum hazard probability and severity reporting thresholds.

c. Any selected hazards or hazardous areas to be specifically examined or excluded.

TASK 203

SUBSYSTEM HAZARD ANALYSIS

203.1 Purpose. The purpose of Task 203 is to perform and document a subsystem hazard analysis (SSHA) to identify hazards associated with design of subsystems including component failure modes, critical human error inputs, and hazards resulting from functional relationships between components and equipments comprising each subsystem.

203.2 Task Description. The contractor shall perform and document a subsystem hazard analysis to identify all components and equipments, including software, whose performance, performance degradation, functional failure, or inadvertent functioning could result in a hazard or whose design does not satisfy contractual safety requirements. The analysis shall include a determination of the modes of failure including reasonable human errors as well as single point failures and the effects on safety when failures occur in subsystem components. If no specific analysis techniques are directed, the contractor shall obtain MA approval of technique(s) to be used prior to performing the analysis. The contractor shall update the SSHA when needed as a result of any system design changes.

203.3 Details to be Specified by the MA (Reference 1.3.2.1).

203.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100 and 203.

(R) b. Format, content, and delivery schedule of any data required including minimum hazard severity and probability reporting thresholds.

c. The specific subsystems to be analyzed.

d. Specification of desired analysis technique(s) and/or format.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 204

SYSTEM HAZARD ANALYSIS

204.1 Purpose. The purpose of Task 204 is to perform and document a system hazard analysis (SHA) to determine the safety problem areas of the total system design including potential safety critical human errors.

204.2 Task Description. The contractor shall perform and document a system hazard analysis to identify hazards and assess the risk of the total system design, including software, and specifically of the subsystem interfaces. This analysis shall include a review of subsystems interrelationships for:

a. Compliance with specified safety criteria.

b. Possible independent, dependent, and simultaneous hazardous events including failures of safety devices and common cause that could create a hazard.

c. Degradation in the safety of a subsystem or the total system from normal operation of another subsystem.

d. Design changes that affect subsystems.

e. Effects of reasonable human errors.

If no specific analysis techniques are directed, the contractor shall obtain MA approval of technique(s) to be used prior to performing the analysis. The SHA may be performed using similar techniques to those used for the SSHA. The contractor shall update the SHA when needed as a result of any system design changes.

204.3 Details to be Specified by the MA (Reference 1.3.2.1).

204.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100 and 204.

b. Format, content, and delivery schedule of any data required including minimum hazard severity and probability reporting thresholds.

c. Specification of desired analysis technique(s) and/or format.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 205

OPERATING AND SUPPORT HAZARD ANALYSIS

205.1 Purpose. The purpose of Task 205 is to perform and document an operating and support hazard analysis (O&SHA) to identify hazards and recommend risk reduction alternatives during all phases of intended system use.

205.2 Task Description. The contractor shall perform and document an O&SHA to examine procedurally controlled activities. The O&SHA identifies and evaluates hazards resulting from the implementation of operations or tasks performed by persons, considering: the planned system configuration/state at each phase of activity; the facility interfaces; the planned environments (or ranges thereof); the supporting tools or other equipment specified for use; operational/task sequence, concurrent task effects and limitations; biotechnological factors, regulatory or contractually specified personnel safety and health requirements; and the potential for unplanned events including hazards introduced by human errors. The O&SHA must identify the safety requirements (or alternatives) needed to eliminate identified hazards, or to reduce the associated risk to a level which is acceptable under either regulatory or contractually specified criteria. The analysis shall identify:

a. Activities which occur under hazardous conditions, their time periods, and the actions required to minimize risk during these activities/time periods.

b. Changes needed in functional or design requirements for system hardware/software, facilities, tooling, or support/test equipment to eliminate hazards or reduce associated risks.

c. Requirements for safety devices and equipment, including personnel safety and life support equipment.

d. Warnings, cautions, and special emergency procedures (e.g., egress, rescue, escape, render-safe, back-out, etc.).

e. Requirements for handling, storage, transporation, maintenance, and disposal of hazardous materials.

f. Requirements for safety training and personnel certification.

The O&SHA documents system safety assessment of procedures involved in: system production, deployment, installation, assembly, test, operation, maintenance, servicing, transportation, storage, modification, demilitarization, and disposal. The contractor shall update the O&SHA when needed as a result of any system design or operational changes. If no specific analysis techniques are directed, the contractor shall obtain MA approval of technique(s) to be used prior to performing the analysis.

205.3 Details to be Specified by the MA (Reference 1.3.2.1).

205.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100 and 205.

(R) b. Format, content, and delivery schedule of any data required, including minimum hazard probability and severity reporting thresholds.

c. Specification of desired analysis technique(s) and/or format.

TASK 206

OCCUPATIONAL HEALTH HAZARD ASSESSMENT

206.1 Purpose: The purpose of Task 206 is to perform and document an occupational health hazard assessment (OHHA) to identify health hazards and propose protective measures to reduce the associated risk to a level acceptable to the MA.

206.2 Task Description

206.2.1 An OHHA shall be performed and documented to identify health hazards and to recommend engineering controls, equipment, and/or protective procedures, to reduce the associated risk to a level acceptable to the MA. Specific occupational health hazards and impacts that shall be considered include:

a. Toxic materials (e.g., carcinogens or suspected carcinogens, systemic poisons, asphyxiants, and respiratory irritants).

b. Physical agents (e.g., noise, heat or cold stress, ionizing and non-ionizing radiation).

c. System, facility and personnel protective equipment design requirements (e.g., ventilation, noise attenuation, radiation barriers, etc.) to allow safe operation and maintenance. When feasible engineering designs are not available to reduce hazards to acceptable levels, alternative protective measures must be specified (e.g., protective clothing, specific operation or maintenance practices to reduce risk to an acceptable level).

206.3 Details to be Specified by the MA (Reference 1.3.2.1).

206.3.1 Details to be specified in the SOW shall include the following as applicable:

(R) a. Imposition of Tasks 100 and 206.

b. Format, content, and delivery schedule of any data required.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 207

SAFETY VERIFICATION

207.1 Purpose. The purpose of Task 207 is to define and perform tests and demonstrations or use other verification methods on safety critical hardware, software, and procedures to verify compliance with safety requirements.

207.2 Task Description. The contractor shall define and perform tests, demonstrations, or otherwise verify the compliance with safety requirements on safety critical (defined by the MA) hardware, software, and procedures. Induced or simulated failures shall be considered to demonstrate the failure mode and acceptability of safety critical equipment and software. Where hazards are identified during the development effort and it cannot be determined by analysis or inspection whether the action taken will adequately reduce the risk, safety tests shall be conducted to evaluate the effectiveness of the actions taken. 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 MA. Specific safety tests shall be integrated into appropriate system test and demonstration plans to the maximum extent possible. Test plans, test procedures, and results of all tests including design verification, operational evaluation, technical data validation and verification, production acceptance, and shelf-life validation shall be reviewed to make sure:

a. Safety of the design is adequately demonstrated (including operating and maintenance procedures), including verification of safety devices, warning devices, etc. for all CATASTROPHIC hazards not eliminated by design.

b. Results of safety evaluations of the system are included in the test and evaluation reports.

207.3 Details to be Specified by the MA (Reference 1.3.2.1).

207.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100 and 207.

(R) b. Definition of safety critical or identification of safety critical equipment and procedures.

c. Development of or inputs to test plans, procedures and reports to verify safety requirements.

d. Format, content, and delivery schedule of any data required.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 208

TRAINING

208.1 Purpose. The purpose of Task 208 is to provide training for necessary certification of contractor and Government personnel who will be involved with contractor activities in such subjects as hazard types and their recognition, causes, effects, and preventive and control measures; procedures, checklists, and human error; safeguards, safety devices, protective equipment; monitoring and warning devices; and contingency procedures.

208.2 Task Description.

208.2.1 Training of Test, Operating, and Support Personnel. The contractor shall conduct a system safety training program for certification of test, operating and support personnel. Approved safety procedures shall be included in instruction lesson plans and student examination for the training of engineering, technician, operating, and maintenance personnel. Contractor test, operations, and field support personnel shall be certified as having completed a training course in safety principles and methods. Specific certification requirements shall be established by a program certification board that includes the system safety manager as a member.

208.2.2 Training of Personnel Involved in Design, Development, and Production. The contractor shall develop safety training programs using results of system and operating hazard analyses, and shall provide for specific types and levels of contractor personnel: i.e., managers, engineers, and technicians involved in design, product assurance, test, and production.

208.2.3 Training of Government Personnel. Contractor safety training shall also include Government personnel who will be involved in contractor activities.

208.3 Details to be Specified by the MA (Reference 1.3.2.1).

208.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100 and 208.

b. Format, content, and delivery schedule of any data required.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 209

SAFETY ASSESSMENT

209.1 Purpose. The purpose of Task 209 is to perform and document a comprehensive evaluation of the mishap risk being assumed prior to test or operation of a system or at contract completion.

209.2 Task Description. The contractor shall perform and document a safety assessment to identify all safety features of the hardware, software, and system design and to identify procedural hazards that may be present in the system being acquired including specific procedural controls and precautions that should be followed. The safety assessment shall summarize:

a. The safety criteria and methodology used to classify and rank hazards.

b. The analyses and tests performed to identify hazards inherent in the system, including:

1. Those hazards that still have a residual risk, and the actions that have been taken to reduce the associated risk to a level contractually specified as acceptable.

2. Results of tests conducted to validate safety criteria requirements and analyses.

c. The results of the safety program efforts. Include a list of all significant hazards along with specific safety recommendations or precautions required to ensure safety of personnel and property. Categorize the list of hazards as to whether or not they may be expected under normal or abnormal operating conditions.

d. Any hazardous materials generated by or used in the system, including:

1. Identification of material type, quantity, and potential hazards.

2. Safety precautions and procedures necessary during use, storage, transportation, and disposal. Include all explosives hazard classification data developed in accordance with Explosives Hazard Classification Procedures.

3. A copy of the Material Safety Data Sheet (OSHA Form 20 or DD Form 1813).

e. Conclude with a signed statement that all identified hazards have been eliminated or their associated risks controlled to levels contractually specified as acceptable, and that the system is ready to test or operate or proceed to the next acquisition phase. In addition, the contractor shall make

recommendations applicable to hazards at the interface of his system with the other system(s) as contractually required.

209.3. Details to be Specified by the MA (Reference 1.3.2.1).

209.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100 and 209.

b. Format, content, and delivery schedule of any data required.

TASK 210

SAFETY COMPLIANCE ASSESSMENT

210.1 Purpose. The purpose of Task 210 is to perform and document a safety compliance assessment to verify compliance with military, federal, national, and industry codes imposed contractually or by law to ensure safe design of a system, and to comprehensively evaluate the safety risk being assumed prior to test or operation of a system or at contract completion.

210.2 Task Description. The contractor shall perform and document a safety compliance assessment to identify and document compliance with appropriate design and operational safety requirements. The assessment identifies the contractually imposed standards, specifications, and codes appropriate to the safety of the system and documents compliance with these requirements. The assessment includes necessary hazard analysis, design drawing and procedural reviews, and equipment inspections. The assessment shall incorporate the scope and techniques of PHA, SSHA, SHA, and O&SHA to the extent necessary to assure the safe design, operation, maintenance, and support of the system. A safety compliance assessment shall:

a. Identify contractual military, federal, national, and industry safety specifications, standards, and codes applicable to the system and document compliance of the design and procedures with these requirements.

b. Identify and evaluate residual hazards inherent in the system or that arise from system-unique interfaces, installation, test, operation, maintenance, or support.

c. Identify necessary specialized safety design features, devices, procedures, skills, training, facilities, support requirements, and personnel protective equipment.

d. Identify hazardous materials and the precautions and procedures necessary for safe storage, handling, transport, use, and disposal of the material.

210.3 Details to be Specified by the MA (Reference 1.3.2.1).

210.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100 and 210.

b. Format, content, and delivery schedule of any data required.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 211

SAFETY REVIEW OF ENGINEERING CHANGE PROPOSALS AND REQUESTS FOR DEVIATION/WAIVER

211.1. Purpose. The purpose of Task 211 is to perform and document analyses of engineering change proposals (ECPs) and requests for deviation/waiver to determine the safety impact on the system.

211.2 Task Description.

211.2.1 ECP Evaluations. The contractor shall analyze each ECP to determine the hazards associated with it, assess the associated risk, and predict the safety impact of the ECP on the existing system. The basis for determining that no hazards are introduced by the ECP must be explained and any necessary supporting evidence included in the evaluation documentation. When an ECP is determined to decrease the level of safety of the existing system, the MA must be so notified.

211.2.2 Requests for Deviation/Waiver. The contractor shall analyze each request for deviation/waiver to determine the hazards and assess the risk of the proposed deviation from or waiver of a requirement, or a specified method or process. The change in the risk involved in accepting the deviation or waiver shall be identified. When the level of safety of the system will be reduced by deviation from or waiver of the requirement, method, or process, the MA must be so notified.

211.3. Details to be Specified by the MA (Reference 1.3.2.1).

211.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100 and 211.

b. Format, content, and delivery schedule of any data required.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 212

SOFTWARE HAZARD ANALYSIS

212.1 Purpose. The purpose of Task 212 is to perform and document a software hazard analysis to identify hazardous conditions incident to safety critical operator information and command and control functions identified by the PHA, SSHA, SHA, or other efforts.

212.2 Task Description. The contractor shall perform and document software hazard analysis on safety critical software-controlled functions to identify software errors/paths which could cause unwanted hazardous conditions.

212.2.1 Preliminary Software Hazard Analysis. These efforts shall examine software design to identify unsafe inadvertent command/failure-to-command modes for resolution. This effort shall be accomplished by tracing safety critical operator information and commands through flow charts, storage allocation charts, software and hardware specifications, and other applicable documentation.

212.2.2 Follow-on Software Hazard Analysis. These efforts shall examine software and its system interfaces for events, faults, and occurrences such as timing which could cause or contribute to undesired events affecting safety. This effort shall be accomplished by tracing safety critical operator information and commands through source/object code through system simulation and through other applicable documentation. Safety critical programs/modules shall be analyzed for sensitivity to software or hardware failures (bit transformation, register perversion, interface failures, etc.) which could cause the system to operate in a hazardous manner.

212.3 Details to be Specified by the MA (Reference 1.3.2.1).

212.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100 and 212.

(R) b. Definition of safety critical.

c. Format, content, and delivery schedule of any data required.

d. Degree of fault-tolerance for Category I and II hazards.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 213

GFE/GFP SYSTEM SAFETY ANALYSIS

213.1 Purpose. The purpose of Task 213 is to make sure system safety analyses for GFE/GFP are considered for integration into the system.

213.2 Task Description. The contractor shall identify the safety critical performance and design data needed to incorporate the GFE/GFP items.

213.2.1 If the data is available and is to be supplied by the MA, the contractor shall:

a. Identify the system safety analyses that are needed, and when these analyses are needed.

b. Identify to the MA any additional system safety analyses that are needed for interfaces between the GFE/GFP and the rest of the system.

c. Perform the analysis upon receipt of MA approval to do so.

213.2.2 If no previously performed analysis data is available, the contractor shall:

a. Develop and submit to the MA a proposed method for determining needed safety-critical data by analysis, test, and/or inspection.

b. Implement the approved method upon receipt of MA approval to do so.

213.3 Details to be Specified by the MA (Reference 1.3.2.1).

213.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100 and 213.

(R) b. Definition of safety critical.

c. Format, content, and delivery schedule for any data required including minimum hazard severity and probability reporting thresholds.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix A

GUIDANCE FOR IMPLEMENTATION OF SYSTEM SAFETY PROGRAM REQUIREMENTS

10. GENERAL. System safety is the element of systems engineering involving the application of scientific and engineering principles for the timely identification of hazards and initiation of the actions necessary to eliminate hazards or reduce the associated risk to an acceptable level within the system. It draws upon professional knowledge and specialized skills in the mathematical, physical, and related scientific disciplines, together with the principles and methods of engineering design and analysis to specify, predict, and evaluate the safety of the system. The degree of safety achieved in a system is directly dependent upon the emphasis given. This emphasis must be applied by the Government and contractors during all phases of the life cycle. Design safety is a prelude to operational safety and the goal is to produce an inherently safe product that will have the minimum operational safety requirements or restrictions.

10.1 Scope. This appendix provides rationale and guidance for the selection of requirements and tasks to fit the needs of any system safety program, and identifies applicable data items for documenting the results of required tasks.

10.2 Purpose (Reference Paragraph 1.1). Provision for a system safety program as defined by this standard should be included in all applicable contracts negotiated by DoD. These contracts include those negotiated within each DoD agency, by one DoD agency for another, and by DoD for other Government agencies. In addition, each DoD in-house program should conduct a system safety program. This appendix is to be used to tailor system safety requirements in the most cost effective manner that meets established program objectives. However, it is not intended to be referenced or implemented in contractual documents.

10.3 User. The user of this appendix may include the DoD MA, Government in-house activity, prime contractors, associate contractors, or subcontractors, who wish to impose system safety tasks upon their supplier(s).

10.4 Contractual Requirements. This standard is to be tailored and incorporated in the list of compliance documents. Tailored system safety program requirements are specified in the contractual provisions including the SOW, bidders' instructions, contract data requirements list, general and special provision sections, annexes, and other contractual means. An SSPP may be submitted with the contractor's proposal and be subject to contract negotiation. Upon approval by the MA, this SSPP should be attached to the contract, referenced in the SOW, and with applicable portions of this standard become the basis for contractual requirements.

10.5 Managing Activity Responsibilities. The MA will:

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 design requirements that are available and applicable, and the specific risk levels considered acceptable for the system. Acceptable risk levels may be defined in terms of a hazard severity/hazard probability matrix, an overall system mishap rate, or other suitable risk assessment procedures.

2. In the SOW, the system safety requirements that cannot be defined in the system specifications. This would include general design guidelines in paragraph 4.3.

3. In the SOW and contract data requirements list 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.

j. Establish work breakdown structure elements at appropriate levels for system safety program management and engineering.

20. REFERENCED DOCUMENTS. Referenced documents are not included herein. Referenced documents required to supplement this military standard are specified in the system specifications and other contractual documents.

30. SYSTEM SAFETY REQUIREMENTS. Section 4, System Safety Requirements, provides basic system safety requirements most DoD systems and facilities acquisition programs should meet. Task 100, which implements Section 4, must be imposed as a single general task to instruct the contractor to conduct a system safety program. It can be tailored to fit the different types

and sizes of programs. Additional tasks in section 100 and 200 or other specific tasks not in this standard, must also be detailed in the SOW to fulfill specific needs of individual programs.

30.1 System Safety Program Objectives and Design Requirements (Reference paragraphs 4.2 and 4.3). These are very basic program objectives and design requirements needed to meet the objectives, and are applicable to most DoD systems and facilities acquisition programs.

30.2 System Safety Precedence (Reference paragraph 4.4).

30.2.1 The overall goal of a system safety program is to design systems that do not contain hazards. However, the nature of most complex systems makes it impossible or impractical to design them completely hazard-free. As hazard analyses are performed, hazards will be identified that will require resolution. System safety precedence defines the order to be followed for satisfying system safety requirements and reducing risks. The alternatives for eliminating the specific hazard or controlling its associated risk will have to be evaluated so that an acceptable method for risk reduction can be agreed to.

30.2.2 Hazard identification, categorization, and corrective actions will need to proceed through design, development, and testing of all development phases. Assessment of risk will be necessary in determining what corrective actions should be taken. Whatever level of hazard risk reduction is taken must be thoroughly justified in all cases.

30.3 Risk Assessment(Reference paragraph 4.5).

30.3.1 To determine what actions to take to correct identified hazards, a system of determining the level of risk involved must be developed. A good risk assessment model will enable decision makers to properly understand the amount of risk involved relative to what it will cost in schedule and dollars to reduce that risk to an acceptable level.

30.3.2 To eliminate as many hazards as possible, prioritize hazards for corrective action. A categorization of hazards may be conducted according to risk level criteria. Categorization may be based on severity since not all hazards are of equal magnitude or criticality to personnel safety and mission success. In some cases, the anticipated consequences of hazardous events may be minimal, while in others, catastrophic. Hazard categorization may also involve the determination of the likelihood of the hazardous event actually occurring. This may be reported in non-numeric (qualitative) terms, such as frequent, occasional, or impossible; or in numeric (quantitative) terms such as once in ten thousand flights, or 1×10^{-4}/flight. Prioritization may be accomplished either subjectively by qualitative analyses resulting in a comparative hazard risk assessment or through quantification of the probability of occurrence resulting in a numeric priority factor for that hazardous condition. Figures 1 and 2 show two sample matrices for hazard risk assessment which can be applied to provide qualitative priority factors for assigning corrective action. In the first matrix an identified hazard assigned a hazard risk index of 1A, 1B, 1C, 2A, 2B, or 3A might require immediate corrective

FIGURE 1. FIRST EXAMPLE HAZARD RISK ASSESSMENT MATRIX

FREQUENCY OF OCCURRENCE	HAZARD CATEGORIES I CATASTROPHIC	II CRITICAL	III MARGINAL	IV NEGLIGIBLE
(A) FREQUENT	1A	2A	3A	4A
(B) PROBABLE	1B	2B	3B	4B
(C) OCCASIONAL	1C	2C	3C	4C
(D) REMOTE	1D	2D	3D	4D
(E) IMPROBABLE	1E	2E	3E	4E

Hazard Risk Index	Suggested Criteria
1A, 1B, 1C, 2A, 2B, 3A	Unacceptable
1D, 2C, 2D, 3B, 3C	Undesirable (MA decision required)
1E, 2E, 3D, 3E, 4A, 4B	Acceptable with review by MA
4C, 4D, 4E	Acceptable without review

FIGURE 2. SECOND EXAMPLE HAZARD RISK ASSESSMENT MATRIX

FREQUENCY OF OCCURRENCE	HAZARD CATEGORIES I CATASTROPHIC	II CRITICAL	III MARGINAL	IV NEGLIGIBLE
(A) FREQUENT	1	3	7	13
(B) PROBABLE	2	5	9	16
(C) OCCASIONAL	4	6	11	18
(D) REMOTE	8	10	14	19
(E) IMPROBABLE	12	15	17	20

Hazard Risk Index	Suggested Criteria
1 - 5	Unacceptable
6 - 9	Undesirable (MA decision required)
10 - 17	Acceptable with review by MA
18 - 20	Acceptable without review

action. A hazard risk index of 1D, 2C, 2D, 3B, or 3C would be tracked for possible corrective action. A hazard risk index of 1E, 2E, 3D, or 3E might have a lower priority for corrective action and may not warrant any tracking actions. In the second matrix, risk indices of 1 through 20 (1 being highest risk) are assigned somewhat arbitrarily. This matrix design assigns a different index to each frequency-category pair thus avoiding the situation caused by creating indices as products of numbers assigned to frequency and category which causes common results such as 2 X 6 = 3 X 4 = 4 X 3. This situation hides information pertinent to prioritization. These are only examples of a risk assessment methods and do not fit all programs.

30.4 Action on Identified Hazards (Reference paragraph 4.6). The contractor is required to follow the system safety precedence to resolve CATASTROPHIC and CRITICAL hazards, and guard against MARGINAL hazards.

40. TASK SELECTION

40.1 Selection Criteria

40.1.1 A major challenge which confronts all Government and industry organizations responsible for a system safety program is the selection of tasks which can materially aid in attaining program safety requirements. Schedule and funding constraints mandate a cost-effective selection, one that is based on identified program needs. The considerations presented herein are intended to provide guidance and rationale for this selection. They are also intended to jog the memory for lessons learned to provoke questions which must be answered and to encourage dialogue with other engineers, and operations and support personnel so that answers to questions and solutions to problems can be found.

40.1.2 Once appropriate tasks have been selected, the tasks themselves must be tailored and specified as outlined in the "Details To Be Specified By the MA." It is also important to coordinate task requirements with other engineering support groups, such as logistics support, reliability, etc., to eliminate duplication of tasks and to be aware of any additional information of value to system safety which these other groups can provide. Finally, the timing and depth required for each task, as well as action to be taken based on task outcome, are largely dependent on individual experience and program requirements. For these reasons, hard and fast rules are not stated.

40.2 Application Matrix for Program Phases. Tables I and II herein provide general guidance on task selection to establish an acceptable and cost effective system safety program. These tables can be used to initially identify those tasks which typically are included in an effective system safety program for the particular acquisition phase involved. The user of the document can then refer to the particular task referenced by the matrix and determine from the detailed purpose at the beginning of the task if it is appropriate to identify as a program task. The use of this matrix for developing a system safety program is to be considered as optional guidance only and is not to be construed as covering all procurement situations. The provisions of applicable regulations must also be followed.

TABLE 1. APPLICATION MATRIX FOR SYSTEM PROGRAM DEVELOPMENT

TASK	TITLE	TASK TYPE	PROGRAM PHASE			
			CONCEPT	VALID	FSED	PROD
100	System Safety Program	MGT	G	G	G	G
101	System Safety Program Plan	MGT	G	G	G	G
102	Integration/Management of Associate contractors, Subcontractors, and AE Firms	MGT	S	S	S	S
103	System Safety Program Reviews	MGT	S	S	S	S
104	SSG/SSWG Support	MGT	G	G	G	G
105	Hazard Tracking and Risk Resolution	MGT	S	G	G	G
106	Test and Evaluation Safety	MGT	G	G	G	G
107	System Safety Progress Summary	MGT	G	G	G	G
108	Qualifications of Key System Safety Personnel	MGT	S	S	S	S
201	Preliminary Hazard List	ENG	G	S	S	N/A
202	Preliminary Hazard Analysis	ENG	G	G	G	GC
203	Subsystem Hazard Analysis	ENG	N/A	G	G	GC
204	System Hazard Analysis	ENG	N/A	G	G	GC
205	Operating and Support Hazard Analysis	ENG	S	G	G	GC
206	Occupational Health Hazard Assessment	ENG	G	G	G	GC
207	Safety Verification	ENG	S	G	G	S
208	Training	MGT	N/A	S	S	S
209	Safety Assessment	MGT	S	S	S	S
210	Safety Compliance Assessment	MGT	S	S	S	S
211	Safety Review of ECPs and Waivers	MGT	N/A	G	G	G
212	Software Hazard Analysis	ENG	S	G	G	GC
213	GFE/GFP System Safety Analysis	ENG	S	G	G	G

Notes: TASK TYPE

ENG - System Safety Engineering
MGT - Management

PROGRAM PHASE

CONCEPT - Conceptual

VALID - Validation

FSED - Full-Scale Engineering Development

PROD - Production

APPLICABILITY CODES

S - Selectively Applicable

G - Generally Applicable

GC - Generally Applicable To Design Changes Only

N/A - Not Applicable

TABLE 2. APPLICATION MATRIX FOR FACILITIES ACQUISITION

TASK	TITLE	TASK TYPE	PROGRAM PHASE			
			P&R DEV	CON DES	FIN DES	CON
100	System Safety Program	MGT	G	G	G	G
101	System Safety Program Plan	MGT	S	G	G	S
102	Integration/Management of Associate Contractors, Subcontractors, and AE Firms	MGT	S	S	S	S
103	System Safety Program Reviews	MGT	G	G	G	G
104	SSG/SSWG Support	MGT	G	G	G	G
105	Hazard Tracking and Risk Resolution	MGT	G	G	G	G
106	Test and Evaluation Safety	MGT	G	G	G	G
107	System Safety Progress Summary	MGT	S	S	S	S
108	Qualifications of Key System Safety Personnel	MGT	S	S	S	S
201	Preliminary Hazard List	ENG	G	N/A	N/A	N/A
202	Preliminary Hazard Analysis	ENG	G	S	N/A	N/A
203	Subsystem Hazard Analysis	ENG	N/A	S	G	GC
204	System Hazard Analysis	ENG	N/A	G	G	GC
205	Operating and Support Hazard Analysis	ENG	S	G	G	GC
206	Occupational Health Hazard Assessment	ENG	G	S	N/A	N/A
207	Safety Verification	ENG	N/A	S	S	S
208	Training	MGT	S	S	S	S
209	Safety Assessment	MGT	N/A	S	G	S
210	Safety Compliance Assessment	MGT	N/A	S	S	S
211	Safety Review of ECPs and Waivers	MGT	S	S	S	S
212	Software Hazard Analysis	ENG	S	S	S	GC
213	GFE/GFP System Safety Analysis	ENG	S	S	S	S

Notes: TASK TYPE

ENG - System Safety Engineering
MGT - Management

PROGRAM PHASE

P&R DEV - Programming and Requirements Development

CON DES - Concept Design

FIN DES - Final Design

CON - Construction

APPLICABILITY CODES

S - Selectively Applicable

G - Generally Applicable

GC - Generally Applicable To Design/ Construction Changes Only

N/A - Not Applicable

40.3 Task Prioritization. The problem of prioritizing or establishing a baseline group from all the tasks in this document cannot be solved unless variables like system complexity, program phase, availability of funds, schedule, etc., are known. Task 100, System Safety Program, is required, and tailoring should be based on total program cost and complexity. All other tasks require Task 100 as a prerequisite.

40.3.1 Identifying and Quantifying System Safety Needs. The elements of a system safety program must be selected to meet the safety needs. These needs are identifed by higher authority through directives and other documents. Identifying and quantifying these needs must be accomplished prior to the appropriate acquisition phase so that tasks and requirements commensurate with the needs may be included. The tasks and requirements which are included establish the framework for the continuing system safety dialogue between the MA and the proposing contractors, one or more of whom will ultimately be selected to develop the system.

40.3.2 Selecting Tasks to Fit the Needs. In most cases, the need for the tasks is self-evident. While experience plays a key role in task selection, it should be supplemented by analysis and investigation. Once recommendations for task applications have been determined and more detailed equipment requirements identified, tasks and requirements can be prioritized and a "rough order of magnitude" estimate should be made of the time and effort required to complete each task. This information will be of considerable value in selecting the tasks which can be accomplished within schedule and funding constraints.

50. RATIONALE AND GUIDANCE FOR TASK SELECTIONS.

50.1 Task Section 100 - Program Management and Control.

50.1.1 System Safety Program (Task 100). This task is required if MIL-STD-882B is to be imposed. Task 100 requires the contractor to set up and conduct a system safety program to meet the requirements of Section 4. Because of the general nature of Section 4, careful tailoring of the requirements contained therein is necessary for each program, particularly for relatively small efforts.

50.1.2 System Safety Program Plan (Task 101).

50.1.2.1 The system safety program plan is a basic tool used by the MA to assist in managing an effective system safety program. It can be used to evaluate the various contractors' approaches to, understanding of, and execution of their system safety tasks, their depth of planning to make sure their procedures for implementing and controlling system safety tasks are adequate, and their organizational structure to make sure appropriate attention will be focused on system safety activities.

50.1.2.2 An SSPP is normally prepared by the contractor and when approved by the MA, becomes the basis of understanding between the contractor and the MA as to how the system safety program is to be conducted. The SSPP identifies all safety program activities specified by the MA and shows how

the safety program will provide input or preclude duplication of effort. The plan provides specific information to show how the contractor will meet quantitative and/or qualitative safety requirements during development, production, and construction phases. When prepared in response to a request for proposal, the SSPP serves as a thorough cross-index to the safety management and engineering proposals contained in the contractor's response. This plan must clearly reflect the safety features of the response. On small programs, or large programs with several associate contractors where the MA is the integrator, or where the MA has a firm idea of the type and magnitude of the system safety effort required, the MA may prepare the SSPP and attach it to the SOW. This often will save funds since the MA would not need to buy the plan from the contractor, and also informs the contractor just what is expected. Not only does this allow contractors to price the effort in their bids, it eliminates the possibility of entering into rounds of submittal/disapproval/resubmittal by contractors inexperienced in system safety. However, if the contractor does not prepare an SSPP, other than in the proposal itself, the MA obtains no immediate information as to whether the contractor understands the system safety requirements.

50.1.2.3 The format and instructions for preparing an SSPP are specified in Task 101 and DoD Authorized Data Item DI-H-7047A, System Safety Program Plan. This data item must be tailored for each program by requiring certain paragraphs to be listed on the contract data requirements list, DD Form 1423. Preliminary SSPPs are often required to be submitted with the contractor's proposal. This allows for the proposed system safety effort to be considered during source selection. Additionally, if the scope of the effort is too large or small, or misdirected, it provides time to get the contractor to correct the error prior to contract initiation.

50.1.3 Integration/Management of Associate Contractors, Subcontractors and Architect and Engineering Firms (Task 102). Major programs or construction projects will often have multiple associate contractors, integrating contractors, and AE firms under contract. An integrating contractor or a facilities acquisition contractor will often have the responsibility to oversee system safety efforts of associate contractors or AE firms. Task 102 provides the authority for management surveillance needed by the integrating or facilities acquisition contractor by assigning the various system safety roles of associate contractors, subcontractors, integrators, and construction firms. The integrator should be tasked to write an ISSPP according to the requirements outlined in Task 101. The integrator and construction contractor should be tasked to perform system hazard analyses and assessments to cover the interfaces between the various contractors' portions of the system or construction effort. All contractors and AE firms should be made aware of the integrator's or facilities acquisition contractor's role of overall system safety management. The integrator needs to resolve differences between associates in safety-related areas. The MA will aid the integrator in these efforts to make sure all contractors and firms mutually understand the system safety requirements, and their respective responsibilities to comply with them.

50.1.4 System Safety Program Reviews (Task 103).

50.1.4.1 In addition to the system safety reviews required by other DoD or service regulations and MIL-STDs (at milestone design reviews and audits), the MA may require special safety reviews. Early in a major program, system safety reviews should be held at least quarterly and as the program progresses, time between reviews can be extended. In addition to more detailed coverage of those items discussed at milestone design reviews, the reviews should address progress on all system safety tasks specified in the SOW.

50.1.4.2 Special system safety reviews may be needed to fulfill requirements of munitions safety boards, first flight readiness reviews, and other safety certification authorities. These reviews should be specified in the SOW as part of Task 103.

50.1.4.3 All program reviews provide an opportunity to review and assign action items and to explore other areas of concern. A mutually acceptable agenda should be written to make sure all system safety open items are covered and that all participants are prepared for meaningful discussions.

50.1.5 System Safety Group/System Safety Working Group Support (Task 104). Individual service regulations require formation of SSG/SSWGs for acquisition of expensive, complex or critical systems, equipment or major facilities. Contractor support of an SSG/SSWG is very useful and may be necessary to make sure procured hardware or software is acceptably free from hazards that could injure personnel or cause unnecessary damage or loss. The level of support desired from the contractor must be detailed in the contract through imposition of Task 104.

50.1.6 Hazard Tracking and Risk Resolution (Task 105). A method or procedure must be developed to document and track hazards and progress made toward resolution of the associated risk. Each prime or associate contractor may maintain their own hazard log or assessment report, or the integrator or MA will maintain the document. If the contractor is to maintain the log, Task 105 must be imposed. Each hazard that meets or exceeds the threshold specified by the MA should be entered on the log when first identified, and each action taken to eliminate the hazard or reduce the associated risk thoroughly documented. The MA will detail the procedure for closing-out the hazard, or acceptance of any residual risk. The hazard log may be documented and delivered as part of the system safety progress summary using DI-H-7050A, System Safety Engineering Report, or it can be included as part of an overall program engineering/management report.

50.1.7 Test and Evaluation Safety (Task 106). This task provides needed contractor management activities to make sure all test safety requirements are met prior to and during testing. Early planning for test and evaluation must be done to consider testing milestones that will require certain hazard analyses, range or laboratory requirements that may require specially formatted assessments, review of test documents, etc.

50.1.8 System Safety Progress Summary (Task 107). The system safety progress summary provides a periodic written report of the status of system safety engineering and management activities. This status report may be

submitted monthly or quarterly. It can be formatted and delivered according to DI-H-7050A, System Safety Engineering Report, or it can be included as part of an overall program engineering/management report.

50.1.9 Qualifications of Key Contractor System Safety Engineers/Managers (Task 108). Some programs will require that the key system safety engineers and managers possess special qualifications. Some or all qualifications listed in Task 108 may be required, or the MA may specify other minimum qualifications. Care must be exercised in applying Task 108 to assure some opportunity for growth and qualification of neophyte system safety personnel who possess little experience.

50.2 Task Section 200 - Design and Evaluation.

50.2.1 Preliminary Hazard List (Task 201). The PHL provides to the MA a list of hazards that may require special safety design emphasis or hazardous areas where in-depth analyses need to be done. The MA may use the results of the PHL to determine the scope of follow-on hazard analyses (PHA, SSHA, etc.). The PHL may be documented using DI-H-7048A, System Safety Hazard Analysis Report.

50.2.2 Preliminary Hazard Analysis (Task 202).

50.2.2.1 PHA is, as implied by the title, the initial effort in hazard analysis during the system design phase or the programming and requirements development phase for facilities acquisition. It may also be used on an operational system for the initial examination of the state of safety. The purpose of the PHA is not to affect control of all risks but to fully recognize the hazardous states with all of the accompanying system implications.

50.2.2.2 The PHA effort should be commenced during the initial phases of system concept, or in the case of a fully operational system, at the initiation of a safety evaluation. This will help in the use of PHA results in tradeoff studies which are so important in the early phases of system development or, in the case of an operational system, aid in an early determination of the state of safety. The output of the PHA may be used in developing system safety requirements and in preparing performance and design specifications. In addition, the PHA is the basic hazard analysis which establishes the framework for other hazard analyses which may be performed.

50.2.2.3 The PHA should include, but not be limited to, the following activities:

(a) A review of pertinent historical safety experience.

(b) A categorized listing of basic energy sources.

(c) An investigation of the various energy sources to determine the provisions which have been developed for their control.

(d) Identification of the safety requirements and other regulations pertaining to personnel safety, environmental hazards, and toxic substances with which the system will have to comply.

(e) Recommend corrective actions.

50.2.2.4 Since the PHA should be initiated very early in the planning phase, the data available to the analyst may be incomplete and informal. Therefore, structure the analysis to permit continual revision and updating as the conceptual approach is modified and refined. As soon as the subsystem design details are complete enough to allow the analyst to begin the subsystem hazard analysis in detail, terminate the PHA. Provide the analyst performing the PHA with the following reference input information:

(a) Design sketches, drawings, and data describing the system and subsystem elements for the various conceptual approaches under consideration.

(b) Functional flow diagrams and related data describing the proposed sequence of activities, functions, and operations, involving the system elements during the contemplated life span.

(c) Background information related to safety requirements associated with the contemplated testing, manufacturing, storage, repair, and use locations and safety related experiences of similar previous programs or activities.

50.2.2.5 The techniques used to perform this analysis must be carefully selected to minimize problems in performing follow-on analyses. The PHA may be documented as outlined in DI-H-7048A, System Safety Hazard Analysis Report. There are several formats that can be used. Some of these are:

50.2.2.5.1 Narrative format. The narrative format is relatively unstructured and as a result there are many different formats available. The format primarily depends on the analyst and the type of information required from the analysis.

50.2.2.5.2 Matrix format. The matrix format is the most commonly used approach for performing and documenting a PHA. There are numerous varieties of PHA matrix formats in use, most of which are fairly similar.

50.2.2.5.3 Other formats. The format used should be tailored to reflect the nature of the system to be analyzed, the extent of information about the system, and the planned use of the analysis output data. Either format is acceptable and the analyst must determine which can do the job most effectively. The use of system safety design checklists, such as Air Force Systems Command Design Handbook 1-X, in the performance of a PHA can be a very effective method.

50.2.3 Subsystem Hazard Analysis (Task 203).

50.2.3.1 This task would be performed if a system under development contained subsystems or components that when integrated functioned together

as a system. This analysis looks at each subsystem or component and identifies hazards associated with operating or failure modes and is especially intended to determine how operation or failure of components affects the overall safety of the system. This analysis should identify necessary actions, using the system safety precedence to determine how to eliminate or reduce the risk of identified hazards.

50.2.3.2 As soon as subsystems are designed in sufficient detail, or well into concept design for facilities acquisition, the SSHA can begin. It should be updated as the design matures. Design changes to components will also need to be evaluated to determine whether the safety of the system is affected. The techniques used for this analysis must be carefully selected to minimize problems in integrating subsystem hazard analyses into the system hazard analysis. The SSHA may be documented as outlined in DI-H-7048A, System Safety Hazard Analysis Report.

50.2.4 System Hazard Analysis (Task 204).

50.2.4.1 An SHA is accomplished in much the same way as the subsystem hazard analysis. However, as the SSHA examines how component operation or failure affects the system, the SHA determines how system operation and failure modes can affect the safety of the system and its subsystems. The SHA should begin as the system design matures, around the preliminary design review or the facilities concept design review milestone, and should be updated until the design is complete. Design changes will need to be evaluated to determine their effects on the safety of the system and its subsystems. This analysis should contain recommended actions, applying the system safety precedence, to eliminate or reduce the risk of identified hazards.

50.2.4.2 Specifically, the SHA examines all subsystem interfaces for:

(a) Compliance with safety criteria called out in the applicable system/subsystem requirements documents.

(b) Possible combinations of independent or dependent failures that can cause hazards to the system or personnel. Failures of controls and safety devices should be considered.

(c) How normal operations of systems and subsystems can degrade the safety of the system.

(d) Design changes to system, subsystems, or interfaces, logic, and software that can create new hazards to equipment and personnel.

The techniques used to perform this analysis must be carefully selected to minimize problems in integrating the SHA with other hazard analyses. The SHA may be documented as outlined in DI-H-7048A, System Safety Hazard Analysis Report.

50.2.5 Operating and Support Hazard Analysis (O&SHA) (Task 205).

50.2.5.1 The O&SHA is performed primarily to identify and evaluate the hazards associated with the environment, personnel, procedures, and equipment involved throughout the operation of a system/element. The O&SHA may be performed on such activities as testing, installation, modification, maintenance, support, transportation, ground servicing, storage, operations, emergency escape, egress, rescue, post-accident responses, and training. The O&SHA may also be selectively applied to facilities acquisition projects to make sure operation and maintenance manuals properly address safety and health requirements.

50.2.5.2 The O&SHA effort should start early enough to provide inputs to the design and prior to system test and operation. The O&SHA is most effective as a continuing closed-loop iterative process, whereby proposed changes, additions, and formulation of functional activities are evaluated for safety considerations, prior to formal acceptance. The analyst performing the O&SHA should have available:

(a) Engineering descriptions of the proposed system, support equipment and facilities.

(b) Draft procedures and preliminary operating manuals.

(c) PHA, SSHA, and SHA reports.

(d) Related requirements, constraint requirements, and personnel capabilities.

(e) Human factors engineering data and reports.

(f) Lessons learned, including a history of mishaps caused by human error.

50.2.5.3 Timely application of the O&SHA will provide design guidance. The findings and recommendations resulting from the O&SHA may affect the diverse functional responsibilities associated with a given program. Therefore, exercise care in assuring that the analysis results are properly distributed for the effective accomplishment of the O&SHA objectives. The techniques used to perform this analysis must be carefully selected to minimize problems in integrating O&SHAs with other hazard analyses. The O&SHA may be documented using DI-H-7048A, System Safety Hazard Analysis Report.

50.2.6 Occupational Health Hazard Assessment (Task 206).

50.2.6.1 The first step of the occupational health hazard assessment is to identify and determine quantities of potentially hazardous materials or physical agents (noise, radiation, heat stress, cold stress) involved with the system and its logistical support. The next step would be to analyze how these materials or physical agents are used in the system and for its logistical support. Based on the use, quantity, and type of substance/agent, estimate where and how personnel exposures may occur and if possible the degree or frequency of exposure involved. The final step would

include incorporation into the design of the system and its logistical support equipment/facilities cost effective controls to reduce exposures to acceptable levels. The life cycle costs of required controls could be high and consideration of alternative systems may be appropriate.

50.2.6.2 The purpose of this analysis is not to dictate designs based on health protection, but to assure decision makers are aware of the health hazards involved and their impacts so that knowledgeable decisions regarding potential tradeoffs can be made.

50.2.6.3 The following factors associated with the system and the logistical support required to operate and maintain the system should be considered:

(a) Toxicity, quantity, and physical state of materials.

(b) Routine or planned uses and releases of hazardous materials or physical agents.

(c) Accidental exposure potentials.

(d) Hazardous waste generated.

(e) Hazardous material handling, transfer, and transportation requirements.

(f) Protective clothing/equipment needs.

(g) Detection and measurement devices required to quantify exposure levels.

(h) Number of personnel potentially at risk.

(i) Engineering controls that could be used, such as isolation, enclosure, ventilation, noise or radiation barriers, etc.

50.2.6.4 To define the acceptable level of risk for health hazards the MA should require use of chemical substance and physical agent exposure limits found in appropriate regulations and directive documents, or contact a qualified individual in the bioenvironmental engineering or medical community. For hazardous substances or agents with unspecified exposure limits the contractor must provide the rationale for acceptable risk criteria used for the OHHA. The OHHA may be documented using DI-H-7048A, System Safety Hazard Analysis Report.

50.2.7 Safety Verification (Task 207).

50.2.7.1 Many safety requirements, as specified in system specifications, requirements documents, etc., will need to be verified by analysis, inspection, demonstration, or test. Also, during design and development, hazard analyses will identify hazards that will be removed through redesign, controls, safety devices, etc. Imposition of these changes will require verification. Task 207 outlines how safety verification should be performed.

50.2.7.2 Much safety verification will be outlined in system/subsystem test plans and procedures. However, for verification of risk control actions taken on hazards identifed during development, special test plans/procedures will be needed. Safety tests may be documented and reported using DI-H-7050, System Safety Engineering Report, or they may be included in the system/subsystem test reports.

50.2.8 Training (Task 208).

50.2.8.1 Many programs will require certification training of personnel involved with development, test, and operation of the system. A good system safety program can only be carried out if all the players involved understand how to do their part. Contractor design engineers need to understand basic system safety principles to design hazard-free systems. A good training program will include training design engineers as a top priority. Managers need to be educated about the importance of good initial safety designs vs. costly redesign and retrofits. Contractor and Government test personnel need to be trained in safe handling, operation, and testing of equipment. Operational and maintenance personnel need safety training in their functions.

50.2.8.2 Training can be accomplished in different ways. Formal classroom training sessions using a thorough lesson plan containing all the necessary handouts is one of the most effective and efficient methods. Imposing examinations and final certification helps assure the trainees have understood and will hopefully apply the material presented.

50.2.8.3 The contractor's safety training program should be detailed in the SSPP (Task 101).

50.2.9 Safety Assessment (Task 209). The safety assessment, as outlined in the task, can be written by following DI-H-7049A, Safety Assessment Report. The importance of this report is that it tells the user or the test team of all the residual unsafe design or operating characteristics of the system. It also attempts to quantify the risk of any hazards not eliminated, and identifies any controls, inhibits, or safety procedures.

50.2.10 Safety Compliance Assessment (Task 210).

50.2.10.1 A safety compliance assessment is conducted to verify the safe design of a system and to obtain a comprehensive evaluation of the safety risk being assumed prior to test or operation of a system. It can be documented by following DI-H-7049A, Safety Assessment Report. It is an operationally oriented analysis, concerned with the safe use of a system, equipment, or facility. A safety compliance assessment is, therefore, broad in scope, covering almost every aspect of the system, but relatively general in nature, delving into detail only to the extent necessary to verify the system's safety or ascertain the risks and precautions necessary for its safe use. A safety compliance assessment may be the only analysis conducted on a program or it may serve as a pre-test or pre-operational safety review, integrating and summarizing operational safety considerations identified in more detailed hazard analyses.

50.2.10.2 A safety compliance assessment may be the only analysis conducted on a relatively low safety risk program. The low risk can result from several different factors. The system may be an integration of primarily off-the-shelf equipments involving little or no new design. It may be a system which is low risk by nature of its technology or complexity. Compliance with federal, military, national, and industry specifications, standards, and codes may be sufficient to make sure of the basic safety of the system. A safety compliance assessment may also be conducted on higher safety risk systems, such as research or advanced development projects, where the higher risks must be accepted, but for which safe operation is still required and the risks must be recognized and reduced to acceptable levels.

50.2.10.3 This assessment may be conducted during any phase of system development. It should be started as soon as sufficient information becomes available. For example, evaluation of equipment should begin with the design of equipment components or with the receipt of equipment specifications from a subcontractor or vendor. The analysis can also be tailored in the SOW to meet the particular needs of a program.

50.2.10.4 A safety compliance assessment should include, but not be limited to, the following:

(a) Identification of appropriate safety standards and verification of system compliance. Standards may be specified by the procuring agency in a specification or other contractual document. This does not preclude the contractor from identifying additional standards which are appropriate. The contractor should also review available historical safety data from similar systems. Verification may be achieved by several methods, including analysis, use of checklists, inspection, test, independent evaluation, or manufacturer's certification.

(b) Analysis and resolution of system hazards. Systems, even those comprised entirely of equipments in full compliance with appropriate standards, may contain hazards resulting from unique uses, interfaces, installation, etc. Another facet of this assessment is to identify, evaluate, and eliminate any such "residual" hazards or reduce their associated risks to acceptable levels. To accomplish this, the assessment should incorporate the scope and techniques of other hazard analyses to the detail necessary to assure a reasonably safe system.

(c) Identification of specialized safety requirements. The above analysis should lead to safety design features and other necessary precautions. The contractor should identify all safety precautions necessary to safely operate and support the system. This includes applicable precautions external to the system or outside the contractor's responsibility. For example, hazard risk may have to be controlled by specialized safety equipment and training because the contract does not allow for redesign or modification of off-the-shelf equipments, or the contractor may not be responsible for providing necessary emergency lighting, fire protection, or personal safety equipment.

(d) Identification of hazardous materials and the precautions and procedures necessary for the safe handling of the material.

50.2.11 Safety Review of Engineering Change Proposals and Requests for Deviation/Waiver (Task 211). This task may be documented using DI-H-7050A, System Safety Engineering Report. ECPs to the existing design and requests for deviation/waiver from existing requirements must be assessed for any possible safety impacts to the system. Often, correction of a deficiency will introduce other overlooked deficiencies. This task is designed to prevent that occurrence by requiring contractor system safety engineers to examine each ECP or request for deviation/waiver, and investigate all conceivable ways the change or deviation could result in an additional hazard(s). The task specifies that the MA be notified if the ECP or request for deviation/waiver decreases the existing level of safety.

50.2.12 Software Hazard Analysis (Task 212).

50.2.12.1 The purpose of software hazard analysis is to: (a) ensure accurate translation of safety specification requirements into computer program configuration item (CPCI) requirements, (b) ensure the CPCI specifications clearly identify the safety criteria to be used (fail-safe, fail-operational, fail-recovery, etc.) (c) identify programs, routines, modules, or functions which control or influence safety critical functions, (d) analyze those programs, routines, modules, and functions and their system interfaces for events, faults, and environments which could cause or contribute to undesired events affecting safety, and (e) ensure that the actual coded software does not cause identified hazardous functions to occur or inhibit desired functions, thus creating hazardous conditions, and effectively mitigate identified end item hardware hazardous anomalies.

50.2.12.1.1 Some of the current analysis techniques and methodologies that are available to conduct this analysis are: (a) software fault tree, (b) software sneak circuit, (c) software/hardware integrated critical path, and (d) nuclear safety cross-check analysis. Due to the various strengths and weaknesses of each technique, a thorough software hazard analysis may require application of more than one technique on a particular software element. Additionally, the application of good software engineering practices is vital to designing software that is safe and analyzable.

50.2.12.2 Software hazard analysis should begin early in the development phase and should be structured to permit continual revision and updating as the design matures. To insure an effective analysis effort, the following information is needed:

(a) System and subsystem specifications and other allocation documents which describe the system, all of the various interfaces with the software, and normal/abnormal environments which the system could encounter.

(b) Functional flow diagrams and related data describing the proposed sequence of activities, functions, and operations involving the system elements during the contemplated life span.

(c) Computer program functional flow charts (or their functional equivalents) storage allocation charts, and other program structure documents as they become available or change.

(d) Background information related to safety requirements associated with the contemplated testing, manufacturing, storage, repair, anticipated environments as applicable, as well as lessons learned from similar programs or activities.

50.2.12.3 The preliminary software hazard analysis effort begins when the system requirements allocation has been made and will continue until program coding begins. The first task of this effort will be to make sure of an accurate flow-down of system level safety requirements as well as requirements generated from the system PHA into the CPCI design specification. Additionally, the analysis contains recommended actions to eliminate identified hazards or reduce their associated risk to an acceptable level. This effort would generally include the following:

(a) Review of system and subsystem specifications to identify and verify hardware-software, software-software, and operator-software interfaces.

(b) Analysis of functional flow diagrams (or their functional equivalent), storage allocation charts, and other program documentation to make sure specification and safety requirements will be met.

(c) Examination of the software to determine the independence/ dependence and interdependence among modules, tables, variables, etc. Elements of software which directly or indirectly influence safety critical software will be identified as being safety critical function should be analyzed for their undesired effects.

50.2.12.4 Follow-on software hazard analysis expands upon the preliminary software hazard analysis by examining the actual source and object code of safety critical programs, routines, modules, and functions to verify the actual design implementation. This effort should be updated until coding is complete. All design changes and modifications should be evaluated to determine the effect on system safety. This analysis contains recommended actions necessary to eliminate identified hazards or reduce their associated risk to an acceptable level. Specifically, this analysis examines:

(a) Safety critical algorithms, modules, routines and calculations for correctness and for input/output, timing, and multiple event sensitivity.

(b) Programs, routines, modules, or functions for design or coding errors which could cause or contribute to an undesired event affecting safety.

(c) Safety critical programs, routines, modules, or functions for compliance with safety criteria called out in applicable CPCI specifications. Safety critical portions of software must be examined at the source/object code level as appropriate.

(d) Possible combinations of independent or dependent hardware or software failures, unintended program jumps, and single or multiple events that could cause the system to operate in a hazardous manner.

(e) Design changes to the system, subsystems, or interfaces, logic, and software that could create new hazards.

The software hazard analysis may be documented as outlined in DI-H-7048A, System Safety Hazard Analysis Report.

50.2.13 GFE/GFP System Safety Analysis (Task 213).

50.2.13.1 This task should be imposed only if the system under development will contain GFE or GFP that interfaces directly with contractor developed hardware or software.

50.2.13.2 This task permits the contractor to integrate the GFE/GFP items into the system design with full knowledge of the associated hazards and risk controls by requiring acquisition of existing analysis documentation. If no such documentation is available, the contractor must perform the necessary analysis to assure a safe interface. This analysis may be documented and delivered by appropriately tailoring and applying DI-H-7048A, System Safety Hazard Analysis Report.

APPENDIX B

SYSTEM SAFETY PROGRAM REQUIREMENTS RELATED TO LIFE CYCLE PHASES

60. SYSTEM SAFETY PROGRAM REQUIREMENTS RELATED TO LIFE CYCLE PHASES.

60.1 Mission need determination--concept exploration.

60.1.1 Mission Need Determination. The system safety effort will support the justificaion of major system new starts 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.

60.1.2 Concept Exploration/Programing and Requirements Development Phase. System safety tasks applicable to the concept exploration/programing and requirements development phase are those required to evaluate the alternative system concepts under consideration for development and establish the system safety programs consistent with the identified mission needs and life cycle requirements. System safety tasks will include the following:

(a) Prepare an SSPP to describe the proposed integrated system safety effort for the concept exploration phase.

(b) Evaluate all considered materials, design features, maintenance, servicing, operational concepts, and environments which will affect safety throughout the life cycle. Consider hazards which may be encountered in the ultimate disposition of the entire system, or components thereof, or of dedicated support equipment, which encompasses hazardous materials and substances.

(c) Perform a PHA to identify hazards associated with each alternative concept.

(d) Identify possible safety interface problems including problems associated with software-controlled system functions.

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

(d) Review safe and successful designs of similar systems for consideration in alternative concepts.

(e) Define the system safety requirements based on past experience with similar systems.

(f) Identify safety requirements that may require a waiver during the system life cycle.

(g) Identify any safety design analysis, test, demonstration and validation requirements.

(h) Document the system safety analyses, results, and recommendations for each promising alternative system concept.

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

(j) 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.

60.1.3 Demonstration and Validation/Concept Design Phase. System safety tasks during the demonstration and validation/concept design 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/concept design phase.

(b) Participate in tradeoff studies to reflect the impact on system safety requirements and risk. Recommend system design changes based on these studies to make sure the optimum degree of safety is achieved consistent with performance and system requirements.

(c) Perform or update the PHA done during the concept exploration/programing and requirements development phase to evaluate the configuration to be tested. Prepare an SHA report of the test configuration considering the planned test environment and test methods.

(d) Establish system safety requirements for system design and criteria for verifing that these requirements have been met. Identify the requirements for inclusion in the appropriate specifications.

(e) Perform detailed hazard analyses (SSHA or SHA) of the design to assess the risk involved in test operation of the system hardware and software. Obtain and include risk assessment of other contractor's furnished equipment, of GFE, and of all interfacing and ancillary equipment to be used during system demonstration tests. Identify the need for special tests to demonstrate/evaluate safety functions.

(f) Identify critical parts and assemblies, production techniques, assembly procedures, facilities, testing, and inspection requirements which may affect safety and will make sure:

(1) Adequate safety provisions are included in the planning and layout of the production line to establish safety control of the demonstration system within the production processes 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 and manufacturing control data contain required warnings, cautions, and special safety procedures.

(4) Testing and evaluation are performed on early production hardware to detect and correct safety deficiencies at the earliest opportunity.

(5) Minimum risk is involved in accepting and using new design, materials, and production and test techniques.

(g) Establish analysis, inspection and test requirements for GFE or other contractor-furnished equipment (hardware, software, and facilities) to verify prior to use that applicable system safety requirements are satisfied.

(h) Perform operating and support hazard analyses of each test, and review all test plans and procedures. Evaluate the interfaces between the test system configuration and personnel, support equipment, special test equipment, test facilities, and the test environment during assembly, checkout, operation, foreseeable emergencies, disassembly and/or tear-down of the test configuration. Make sure hazards identified by analyses and tests are eliminated or the associated risk is minimized. Identify the need for special tests to demonstrate or evaluate safety of test functions.

(i) Review training plans and programs for adequate safety considerations.

(j) Review system operation and maintenance publications for adequate safety considerations, and ensure the inclusion of applicable Occupational Safety and Health Administration (OSHA) requirements.

(k) Review logistic support publications for adequate safety considerations, and ensure the inclusion of applicable US Department of Transportation (DOT), US Environmental Protection Agency (EPA), and OSHA requirements.

(l) Evaluate results of safety tests, failure analyses, and mishap investigations performed during the demonstration and validation phase. Recommend redesign or other corrective action (this subparagraph does not apply to the facility concept design phase).

(m) Make sure system safety requirements are incorporated into the system specification/design document based on updated system safety studies, analyses, and tests.

(n) Prepare a summary report of the results of the system safety tasks conducted during the demonstration and validation/concept development phase to support the decision-making process.

(o) Continue to tailor the system safety program. Prepare or update the SSPP for the full-scale engineering development phase and production phase.

60.1.4 Full-Scale Engineering Development/Final Design Phase. To provide support to the system engineering program, the system safety tasks during the full-scale engineering development/final design phase will include the following:

(a) Prepare or update as applicable the SSPP for the full-scale engineering development phase. Continue effective and timely implementation of the SSPP during facility final design phase.

(b) Review preliminary engineering designs to make sure safety design requirements are incorporated and hazards identified during the earlier phases are eliminated or the associated risks reduced to an acceptable level.

(c) Update system safety requirements in system specification/design documents.

(d) Perform or update the SSHA, SHA and O&SHA and safety studies concurrent with the design/test effort to identify design and/or operating and support hazards. Recommend any required design changes and control procedures.

(e) Perform an O&SHA for each test, and review all test plans and procedures. Evaluate the interfaces between the test system configuration and personnel, support equipment, special test equipment, test facilities, and the test environment during assembly, check-out, operations, foreseeable emergencies, disassembly, and/or tear-down of the test configuration. Make sure hazards identified by analyses and tests are eliminated or their associated risk controlled. Identify the need for special tests to demonstrate or verify system safety functions. Establish analyses, inspection, and test requirements for other contractors' or GFE/GFP (hardware, software, and facilities) to verify prior to use that applicable system safety requirements are satisfied.

(f) Participate in technical design and program reviews and present results of the SSHA, SHA and/or O&SHA.

(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 safety testing, other system tests, failure analyses and mishap investigations. Recommend redesign or other corrective action.

(i) Identify, evaluate, and provide safety considerations or tradeoff studies.

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

(k) Review logistic support publications for adequate safety considerations, and ensure the inclusion of applicable DOT, EPA, and OSHA requirements.

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

(m) Identify the need for safety training and provide safety inputs to training courses.

(n) Provide system safety surveillance and support of test unit production and of planning for full-scale production and deployment. Identify critical parts and assemblies, production techniques, assembly procedures, facilities, testing, and inspection requirements which may affect safety and will make sure:

(1) Adequate safety provisions are included in the planning and layout of the production line to establish safety control of the demonstration 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 and manufacturing control data contain required warnings, cautions, and special safety procedures.

(4) Testing and evaluation are performed on early production hardware to detect and correct safety deficiencies at the earliest opportunity.

(5) Minimum risk is involved in accepting and using new designs, materials, and production and test techniques.

(o) Make sure procedures developed for system test, maintenance, operation, and servicing provide for safe disposal of expendable hazardous materials. Consider any material or manufactured component (whether or not an identifiable spare part or replenishable component) when access to hazardous material will be required by personnel during planned servicing, teardown, or maintenance activities, or in reasonably foreseeable unplanned events resulting from workplace operations. Safety data developed in SSHAs, SHAs, and O&SHAs, and summarized in safety assessment reports must also identify any hazards which must be considered when the system, or components thereof, are eventually demilitarized and subject to disposal. (Not applicable for facilities construction.)

(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.

60.1.5 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 (this paragraph is not applicable to the facilities construction life cycle.):

(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 make sure:

(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.

(4) Minimum risk is involved in accepting and using new designs, materials, and production and test techniques.

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

(d) Perform O&SHAs of each test, and review all test plans and procedures. Evaluate the interfaces between the test system configuration and personnel, support equipment, special test equipment, test facilities, and the test environment during assembly, checkout, operation, foreseeable emergencies, disassembly and/or tear-down of the test configuration. Make sure hazards identified by analyses and tests are eliminated or their associated risk reduced to an acceptable level.

(e) Review technical data for warnings, cautions, and special procedures identified as requirements in the O&SHA for safe operation, maintenance, servicing, storage, packaging, handling, and transportation.

(f) Perform O&SHAs of deployment operations, and review all deployment plans and procedures. Evaluate the interfaces between the system being deployed with personnel, support equipment, packaging, facilities, and the deployment environment, during transportation, storage, handling, assembly, installation, checkout, and demonstration/test operations. Make sure hazards identified by analyses are eliminated or their associated risk is reduced to an acceptable level.

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

(h) Perform or update hazard analyses to identify any new hazards that may result from design changes. Make sure 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 make sure the procedures, warnings, and cautions are adequate and inherent safety is not degraded. These reviews shall be documented as updates to the O&SHAs.

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

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

(n) Evaluate the adequacy of safety and warning devices, life support equipment, and personnel protective equipment.

60.1.6 Construction Phase. As part of the continuing system safety program for facilities, the system safety tasks for this phase will include the following:

(a) Ensure the application of all relevant building safety codes including OSHA, National Fire Protection Association, and U.S. Army Corps of Engineers safety requirements.

(b) Conduct hazard analyses to determine safety requirements at all interfaces between the facility and those systems planned for installation.

(c) Review equipment installation, operation, and maintenance plans to make sure all design and procedural safety requirements have been met.

(d) Continue the updating of the hazard correction tracking begun during the design phases.

(e) Evaluate mishaps or other losses to determine if they were the result of safety deficiencies or oversight.

(f) Update hazard analyses to identify any new hazards that may result from change orders.

60.2 System safety program requirements for other acquisitions. For programs that do not follow the standard system life cycle phases outlined in the previous paragraphs the responsible activity must carefully integrate the requirements of this standard into the acquisition process being used. Although different, facilities, ship construction, and certain major one-of-a-kind procurements still evolve through a concept/design/assembly/acceptance sequence somewhat analogous to the classic life cycle. The MA should carefully describe what system safety data are to be submitted in the appropriate contractual document, assuring these data are submitted prior to key decision points.

60.3 System Safety Requirements for Technology Development. Consider system safety during development of technology. System safety concerns should be documented. This documentation will provide the system safety background data necessary should a decision be made to implement the technology within a system development program.

APPENDIX C

DATA REQUIREMENTS FOR MIL-STD-882B

70. DATA REQUIREMENTS FOR MIL-STD-882B.

70.1 Data item descriptions and the paragraphs of MIL-STD-882B where their requirements are located are as follows:

Paragraph Location	DID No.
Paragraph 3.1.14 and Task 101	DI-H-7047A
Task 202	DI-H-7048A
Task 203	DI-H-7048A
Task 204	DI-H-7048A
Task 205	DI-H-7048A
Task 206	DI-H-7048A
Task 212	DI-H-7048A
Task 213	DI-H-7048A
Task 210	DI-H-7049A
Task 211	DI-H-7050A

☆ U.S. GOVERNMENT PRINTING OFFICE: 1984-705-040/A-2063

THIS PAGE INTENTIONALLY LEFT BLANK