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

MILITARY STANDARD

MIL-STD-882B SYSTEM SAFETY PROGRAM REQUIREMENTS

AMSC Number F3329 FSC SAFT

NOTICE 1

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 (PLEQ ComSO), Andrews AFB, Washington, DC 20334-5000, by using the self-addressed Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter.

FOREWORD

The principal objective of a system safety program within the Department of Defense (Diet) is to make sure safety, consistent with mission requirements, is designed into systems, subsystems, equipment, and facilities, and their interfaces.

Diet has approved this military standard for all Diet 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 Diet in-house compliance.

CONTENTS

Paragraph		Page
1.	SCOPE	1
1.1	Purpose	1
1.2	Applicability	1
1.3	Application	1
1.3.1	Applying Tasks	1
1.3.2	Tailoring of Task Descriptions	1
1.3.2.1	Details to be Specified	1
1.3.2.2	Application Guidance	1
1.3.2.3	Method of Reference	2
1.3.3	Conflicting Requirements	2
2.	REFERENCED DOCUMENTS	2
3.	DEFINITIONS AND ABBREVIATIONS	2
3.1	Definitions	2
3.1.1	Contractor	2
3.1.2	Damage	2
3.1.3	Hazard	2
3.1.4	Hazardous Event	2
3.1.5	Hazardous Event Probability	2
3.1.6	Hazard Probability	2
3.1.7	Hazard Severity	2
3.1.8	Managing Activity	2
3.1.9	Mishap	2
3.1.10	Off-the-Shelf Item	2
3.1.11	Risk	3
3.1.12	Safety	3
3.1.13	Safety-Critical Computer Software Component	3
3.1.14	Subsystem	3
3.1.15	System	3
3.1.16	System Safety	3
3.1.17	System Safety Engineer	3
3.1.18	System Safety Engineering	3
3.1.19	System Safety Group/Working Group	3
3.1.20	System Safety Management	3
3.1.21	System Safety Manager	3
3.1.22	System Safety Program	4
3.1.23	System Safety Program Plan	4
3.2	Abbreviations	4
4.	SYSTEM SAFETY REQUIREMENTS	4

4.1 System Safety Program 4
4.2 System Safety Program Objectives 4
4.3 System Safety Design Requirements 5
4.4 System Safety Precedence 6
4.5 Risk Assessment 7
4.5.1 Hazard Severity 7
4.5.2 Hazard Probability 7
4.6 Action on Identified Hazards 8

5. TASK DESCRIPTIONS 8

TASK SECTION 100
PROGRAM MANAGEMENT AND CONTROL 100-1

TASK

100 System Safety Program 100-3
101 System Safety Program Plan 101-1
102 Integration/Management of Associate Contractors, Subcontractors, and Architect and Engineering Firms 102-1
103 System Safety Program Reviews 103-1
104 System Safety Group/System Safety Working Group Support 104-1
105 Hazard Tracking and Risk Resolution 105-1
106 Test and Evaluation Safety 106-1
107 System Safety Progress Summary 107-1
108 Qualifications of Key Contractor System Safety Engineers/Managers 108-1

TASK SECTION 200
DESIGN AND EVALUATION 200-1

201 Preliminary Hazard List 201-1
202 Preliminary Hazard Analysis 202-1
203 Subsystem Hazard Analysis 203-1
204 System Hazard Analysis 204-1
205 Operating and Support Hazard Analysis 205-1
206 Occupational Health Hazard Assessment 206-1
207 Safety Verification 207-1
208 Training 208-1
209 Safety Assessment 209-1
210 Safety Compliance Assessment 210-1
211 Safety Review of Engineering Change Proposals and Requests for Deviation/Waiver 211-1
212 RESERVED 212-1
213 GFE/GFP System Safety Analysis 213-1

TASK SECTION 300
SOFTWARE HAZARD ANALYSIS 300-1

301 Software Requirements Hazard Analysis 301-1
302 Top-Level Design Hazard Analysis 302-1
303 Detailed Design Hazard Analysis 303-1
304 Code-Level Software Hazard Analysis 304-1

305	Software Safety Testing	305-1
306	Software/User Interface Analysis	306-1
307	Software Change Hazard Analysis	307-1

APPENDIX A

GUIDANCE FOR IMPLEMENTATION OF SYSTEM SAFETY PROGRAM REQUIREMENTS

Paragraph		Page
10.	GENERAL	A-1
10.1	Scope	A-1
10.2	Purpose	A-1
10.3	User	A-1
10.4	Contractual Requirements	A-1
10.5	Managing Activity Responsibilities	A-1
20.	REFERENCED DOCUMENTS	A-2
30.	SYSTEM SAFETY REQUIREMENTS	A-2
30.1	System Safety Program Objectives and Design Requirements	A-2
30.2	System Safety Precedence	A-3
30.3	Risk Assessment	A-3
30.4	Action on Identified Hazards	A-3
40.	TASK SELECTION	A-5
40.1	Selection Criteria	A-5
40.2	Application Matrix for Program Phases	A-5
40.3	Task Prioritization	A-5
40.3.1	Identifying and Quantifying System Safety Needs	A-8
40.3.2	Selecting Tasks to Fit the Needs	A-8
50.	RATIONALE AND GUIDANCE FOR TASK SELECTIONS	A-8
50.1	Task Section 100 - Program Management and Control	A-8
50.1.1	System Safety Program	A-8
50.1.2	System Safety Program Plan	A-8
50.1.3	Integration/Management of Associate Contractors, Subcontractors and Architect and Engineering Firms	A-9
50.1.4	System Safety Program Reviews	A-9
50.1.5	System Safety Group/System Safety Working Group Support	A-10
50.1.6	Hazard Tracking and Risk Resolution	A-10
50.1.7	Test and Evaluation Safety	A-10
50.1.8	System Safety Progress Summary	A-10
50.1.9	Qualifications of Key Contractor System Safety Engineers/Managers	A-11
50.2	Task Section 200 - Design and Evaluation	A-11
50.2.1	Preliminary Hazard List	A-11
50.2.2	Preliminary Hazard Analysis	A-11
50.2.3	Subsystem Hazard Analysis	A-12

50.2.4 System Hazard Analysis A-13
50.2.5 Operating and Support Hazard Analysis A-13
50.2.6 Occupational Health Hazard Assessment A-14
50.2.7 Safety Verification A-15
50.2.8 Training A-16
50.2.9 Safety Assessment A-16
50.2.10 Safety Compliance Assessment A-16
50.2.11 Safety Review of Engineering Change Proposals and Requests for Deviation/Waiver A-17
50.2.12 - RESERVED - A-18
50.2.13 GFE/GFP System Safety Analysis A-18
50.3 Task Section 300 - Software Hazard Analysis A-18
50.3.1 Software Requirements Hazard Analysis A-20
50.3.2 Top-Level Design Hazard Analysis A-21
50.3.3 Detailed Design Hazard Analysis A-21
50.3.4 Code-Level Software Hazard Analysis A-22
50.3.5 Software Safety Testing A-23
50.3.6 Software/User Interface Analysis A-23
50.3.7 Software Change Hazard Analysis A-24
50.3.8 Documentation A-24

APPENDIX B

SYSTEM SAFETY PROGRAM REQUIREMENTS RELATED TO LIFE CYCLE PHASES

Paragraph Page

60. SYSTEM SAFETY PROGRAM REQUIREMENTS RELATED TO LIFE CYCLE PHASES B-1

60.1 Mission Need Determination - Concept Exploration B-1
60.1.1 Mission Need Determination B-1
60.1.2 Concept Exploration/Programming and Requirements Development Phase B-1
60.1.3 Demonstration and Validation/ Concept Design Phase B-2
60.1.4 Full-Scale Engineering Development/Final Design Phase B-4
60.1.5 Production and Deployment Phase B-5
60.1.6 Construction Phase B-7
60.2 System Safety Program Requirements for Other Acquisitions B-7

60.3 System Safety Requirements for Technology Requirements B-8

APPENDIX C

DATA REQUIREMENTS FOR MIL-STD-882B

Paragraph Page

70. DATA REQUIREMENTS FOR MIL-STD-882 C-1

TABLES

Number		Page
1	APPLICATION MATRIX FOR SYSTEM PROGRAM DEVELOPMENT	A-6
2	APPLICATION MATRIX FOR FACILITIES ACQUISITION	A-7
3	RELATIONSHIPS BETWEEN THE MIL-STD-882D SOFTWARE HAZARD ANALYSES, THE MIL-STD-1521B REVIEWS AND AUDITS, AND THE DOD-STD-2167 SOFTWARE DEVELOPMENT PROCESS A-25	A-25

FIGURES

1	FIRST EXAMPLE HAZARD RISK ASSESSMENT MATRIX	A-4
2	SECOND EXAMPLE HAZARD RISK ASSESSMENT MATRIX	A-4

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 Diet 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 Diet in-house programs.

1.3 Application.

1.3.1 Applying Tasks. Tasks described in this standard are to be selectively applied in Diet 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 system, 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 notifiation, 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 Diet 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 Diet 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 (Diet, 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 Safety-Critical Computer Software Components. Those computer software components (processes, functions, values or computer program states) whose errors (inadvertent or unauthorized occurrence, failure to occur when required, occurrence out of sequence, occurrence in combination with other functions, or erroneous value) can result in a potential hazard, or loss of predictability or control of a system.

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

3.1.15 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.

3.1.16 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.

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

3.1.18 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.

3.1.19 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.

3.1.20 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.

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

3.1.22 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.

3.1.23 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:

AU	Architect and Engineering Firm
CPCI	Computer Program Configuration Item
CSHA	Code-Level Software Hazard Analysis
DDHA	Detailed Design Hazard Analysis
DID	Data Item Description
DDD	Diet Department of Defense
DOT	Department of Transportation
ECP	Engineering Change Proposal
EPA	Environmental Protection Agency
GFE	Government-Furnished Equipment
GFP	Government-Furnished Property
ISSPP	Integrated System Safety Program Plan
MA	Managing Activity
OHHA	Occupational Health Hazard Assessment
O&SHA	Operating & Support Hazard Analysis
OSHA	Occupational Safety and Health Administration
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
RFP	Request for Proposal
SCCSC	Safety-Critical Computer Software Components
SCHA	Software Change Hazard Analysis
SHA	System Hazard Analysis
SOW	Statement of Work
SRHA	Software Requirements Hazard Analysis
SSG	System Safety Group
SSHA	Subsystem Hazard Analysis
SSPP	System Safety Program Plan
SSWG	System Safety Working Group
TDHA	Top-Level Design Hazard Analysis

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 eliminate 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:

Hazard Severity

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.

There 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:

Hazard Probability

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 occurrence may not possible	Unlikely to occur, but be experienced

(*)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 - AVG Preparing Activity
Navy - AS Air Force - 10
Project No. - SAFT-0002

Reviewing Activities:

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

TASK SECTION 100

PROGRAM MANAGEMENT AND CONTROL

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.

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 andengineering. 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 described 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' (AU) 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 additional 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, including software 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 Eke and Engineering Firms. The AU shall be responsible for conducting facility hazard analyses and other facility SSPP functions as specified in the SOW. The AU 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 AU shall assure that design subcontractors or consultants maintain and provide suitable documentation of any safety analyses performed.

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.

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 (Auk) and system safety working groups (Auk) 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/Auk. 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 or 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.

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 or 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.

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.

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.

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

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.

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). This shall include consideration of the potential contribution by software (including software developed by other contractors) to subsystem/system mishaps. Safety design criteria to control safety-critical software commands and responses (e.g., inadvertent command, failure to command, untimely command or responses, or MA-designated undesired events) shall be identified and appropriate action taken to incorporate them in the software (and related hardware) specifications.

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, aec, 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 subsystem 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:

a. 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.

b. Of potential contribution of software (including that which is developed by other contractors) events, faults, and occurrences (such as improper timing) on the safety of the subsystem.

c. That the safety design criteria in the software specification(s) have been satisfied.

d. That the method of implementation of software design requirements and corrective actions has not impaired or decreased the safety of the subsystem nor has introduced any new hazards.

If no specific analysis techniques are directed, the contractor shall obtain MA approval of technique(s) to be used prior to performing the analysis. When software to be used in conjunction with the subsystem is being developed under DOD-STD-2167/2168, the contractor performing the SSHA shall monitor, obtain and use the output of each phase of the formal software development process in evaluating the software contribution to the SSHA. Problems identified which require the reaction of the software developer shall be reported to the MA in time to support the ongoing phase of the software development process. The contractor shall update the SSHA when needed as a result of any system design changes, including software design changes which affect system safety.

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 subsystem to be analyzed.

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

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.

f. Determination:

(1) Of potential contribution of software (including that which is developed by other contractors) events, faults and occurrences (such as improper timing) on safety of the system.

(2) That the safety design criteria in the software specification(s) have been satisfied.

(3) That the method of implementation of the software design requirements and corrective actions has not impaired or degraded the safety of the system nor has introduced any new hazards.

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. When software to be used

in conjunction with the system is being developed under DOD-STD-2167/2168, the contractor performing the SHA shall monitor, obtain, and use the output of each phase of the formal software development process in evaluating the software contribution to the SHA. Problems identified which require the reaction of the software developer shall be reported to the MA in time to support the ongoing phase of the software development process. The contractor shall update the SHA when needed as a result of any system design changes, including software design changes which affect system safety.

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.

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, including software-controlled automatic test 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.), including those necessitated by failure of a software-controlled operation to produce the expected and required safe result or indication.

e. Requirements for handling, storage, transportation, 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.

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 and 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.

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.

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 and 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.

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.

TASK 212

RESERVED

For Software Hazard Analyses see the 300 series tasks.

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.

TASK SECTION 300

SOFTWARE SYSTEM SAFETY

300. Software System Safety.

300.1 Software System Safety is an integral part of the total System Safety Program. The 300 series of tasks are to be used in concert with the following documents;

a. DOD-STD-2167, Defense System Software Development,

b. DOD-STD-2168, Software Quality Evaluation.

c. MIL-STD-e, Configuration Management Practices for Systems, Equipment, Munitions, and Computer Programs,

d. MIL-STD-1521B, Reviews and Audits for Systems, Equipment, and Computer Programs

e. DOD-HDBK-287, Defense System Software Development Handbook,

These documents should also be referenced for definitions unique to software development.

300.2 The 300 series of tasks are recommended for programs which involve large or complicated software packages normally developed under the above documents. For other programs, for which these tasks are not appropriate, the software can be considered within selected 200 series tasks.

TASK 301

SOFTWARE REQUIREMENTS HAZARD ANALYSIS

301.1 Purpose. The purpose of Task 301 is to require the contractor to perform and document a Software Requirements Hazard Analysis (SRHA). The contractor shall examine system and software requirements and design in order to identify unsafe modes for resolution, such as out-of-sequence, wrong event, inappropriate magnitude, inadvertent command, adverse environment, deadlocking, failure-to-command modes, etc.

As input, the SRHA uses the PHL (Task 201) and system level PHA (Task 202). The analysis shall examine Safety-Critical Computer Software Components (SCCSC) at a gross level to obtain an initial safety evaluation of the software system. The output of the SRHA is used as input to other safety analyses. SCCSCs shall be subject to further analysis by the Top-Level and Detailed Design analyses. A draft SCCSC shall be presented at the System Requirements Review, and updated at the System Design Review. The final results of the analysis shall be presented at the Software Specifications Review.

301.2 Task Description:

301.2.1 Safety Requirement Tracking. The contractor shall develop a tracking system within the configuration management structure for software safety requirements and their flow through the documentation. A description of the implementation of each requirement is desirable.

301.2.2 Analyze Software Requirements Specifications. The contractor shall analyze the System/Segment Specification (SEAWAYS) and Software Requirements Specification (SRS), to include the following sub-tasks;

a. Review Specification Documents. The contractor shall assure that the System Safety Requirements are correctly and completely specified, that they have been properly translated in to software requirements, and that the software safety requirements will appropriately influence the software design and the development of the operator, user, and diagnostic manuals. To do this the contractor shall review, as a minimum, the following documents:

(1) System/Segment Specification and Subsystem Specifications

(2) Software Requirements Specifications

(3) Interface Requirements Specifications and other interface documents

(4) Functional Flow Diagrams and related data

(5) Storage allocation and program structure documents

(6) Background information relating to safety requirements associated with the contemplated testing, manufacturing, storage, repair, use, and final disposition.

(7) Information concerning system energy, toxic and other hazardous event sources, especially ones which may be controlled directly or indirectly by software (e.g., System PHA)

(8) Software Development Plan, Software Quality Evaluation Plan, and Software Configuration Management Plan

(9) Historical data

b. Identify Hazards Related to Specifications. The contractor shall identify hazards related to any of the specifications or documents listed above.

301.2.3 Develop Recommendations, Design and Testing Requirements. The contractor shall develop safety related recommendations, and design and testing requirements and shall incorporate them in the Software Top-Level and Software Detailed Design Documents, and the Software Test Plan. The following subtasks shall be accomplished:

a. Develop Specification Change Recommendations. The contractor shall develop safety-related change recommendations to the specification documents listed above, including means of verification.

b. Develop Design Requirements. The contractor shall develop safety related design requirements for incorporation into the Software Top-Level Design Document and Software Detailed Design Document. In addition, safety-related recommendations regarding hardware design or selection shall also be made.

c. Develop Testing Requirements. The contractor shall develop safety related test plans, test descriptions, test procedures, and test case requirements for incorporation into the corresponding test documents.

301.2.4 Support the System Design Review and Software Specification Review. The contractor shall support the System Design Review (SDR) and Software Specification Review (SURE) from a software safety viewpoint.

301.3 Details to be specified by the Managing Agency: Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100, 201, 202, and 301.

(R) b. Definition of Safety Critical within the context of the system, subsystem, or component under analysis.

(R) c. Level of contractor support required for design reviews.

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

TASK 302

TOP-LEVEL DESIGN HAZARD ANALYSIS

302.1 Purpose. The purpose of Task 302 is to require the contractor to perform and document a Top-Level Design Hazard Analysis (TDHA). The contractor shall analyze the Top-Level Design, using the results of the SRHA (Task 301), if previously accomplished.

This hazard analysis shall include: the definition and subsequent analysis of Safety-Critical Computer Software Components (SCCSC), identifying the degree of risk involved, and the design and test plan to be implemented. The TDHA shall be substantially complete before the Software Detailed Design is started. The results of the TDHA shall be presented at the Preliminary Design Review.

302.2 Task Description:

302.2.1 Conduct a Hazard Risk Assessment. The contractor shall perform a safety hazard risk assessment to identify those SCCSs that warrant further analysis beyond the preliminary design level.

a. Relate Hazards to Software Elements. The contractor shall relate identified hazards from the PHA, SSHA, and SRHA to the Computer Software Components (CSCs) and lower-level software units which may affect or control the hazards. These software components, and any others which may be specifically designated, are the SCCSCs.

b. Evaluate Independence/Dependence and Interdependence in Top-level Design. The contractor shall evaluate available design documentation to determine the independence/ dependence and interdependence of SCCSCs to both safety-critical and non-safety-critical CSCs. Those CSCs which are found to affect the output of SCCSCs are also SCCSCs.

302.2.2 Analyze Top-level Design. The contractor shall analyze the Top-Level Design of those SCCSs identified above to ensure that all safety requirements are correctly and completely specified in the Top-Level design. The contractor shall determine where in the Top-Level Design, and under what conditions, unacceptable hazards may occur. Input/output timing, multiple event, out-of-sequence event, failure of event, wrong event, inappropriate magnitude, adverse environmental, deadlocking, hardware failure sensitivities, etc., shall be included in the analysis.

302.2.3 Develop Design Change Recommendations. Based on the results of the PHA, SSHA, SRHA, and TDHA, the contractor shall make changes to the Software Top-Level Design Document to eliminate or reduce to an acceptable level the risk of the hazards.

302.2.4 Integrate Safety Requirements Into the Software Test Plan. The contractor shall integrate safety requirements and include the testing of safety-critical CSCs and conditions in the Software Test Plan. The contractor shall incorporate safety-specific tests in the Software Test Plan, the System Test Plan, and the overall system testing program. These test plans shall contain provisions for testing under both simulated and operational conditions.

302.2.5 Support Preliminary Design Review. The contractor shall support the Preliminary Design Review (PDR) from a software safety viewpoint.

302.3 Details to be specified by the Managing Agency: Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100, 203, 301, and 302.

(R) b. Definition of Safety Critical within the context of the system, subsystem, or component under analysis.

(R) c. Level of contractor support required for design reviews.

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

required.

TASK 303

DETAILED DESIGN HAZARD ANALYSIS

303.1 Purpose. The purpose of Task 303 is to require the contractor to perform and document a Detailed Design Hazard Analysis (DDHA). The contractor shall analyze the Software Detailed Design, using the results of the SRHA (Task 301) and TDHA (Task 302) (if previously accomplished) to verify the correct incorporation of safety requirements and to analyze the Safety-Critical Computer Software Components (SCCSCs). This analysis shall be substantially complete before coding of the software is started. The results of the DDHA shall be presented at the Critical Design Review.

303.2 Task Description:

303.2.1 Hazard Risk Assessment. The contractor shall perform a hazard risk assessment to determine which software elements warrant further analysis.

a. Relate Hazards to Software Components. The contractor shall relate hazards identified from the PHA, SRHA, and TDHA to lower level software components defined in the Software Detailed Design. These components shall be identified as SCCSCs and shall be designated as configuration items in accordance with DOD-STD-2167 and MIL-STD-483 (or DOD-STD-2168). Identification of SCCSCs shall be carried to the lowest level practical through analysis of the Detailed Design.

b. Evaluate Independence/Dependence and Interdependence in Detailed Design. The contractor shall evaluate the Software Detailed Design Document and other Detailed Design documentation to determine the independence/dependence and interdependence of safety-critical and other designated software at the Computer Software Configuration Item (CSCI), Computer Software Component (CSC) and lower unit levels, (including subroutines, data bases, data files, tables, and variables).

303.2.2 Analyze Detailed Design. The contractor shall conduct a safety analysis on the Software Detailed Design, of software components identified as safety-critical by the hazard risk assessments, to ensure that all safety requirements are correctly and completely specified and included in the design. The contractor shall determine where in the detailed design, and under what conditions, unacceptable hazards will or may occur.

Potential errors attributable to input/output timing, multiple event, out-of-sequence event, failure of event, wrong event, inappropriate magnitude, adverse environment, deadlocking, and hardware failure sensitivities shall be included in the analysis.

303.2.3 Develop Design Recommendations. Based on the results of the Detailed Design Safety Analyses, the contractor shall make change recommendations to the detailed design to eliminate or reduce the severity of the hazards to an acceptable level. The precedence for resolving hazards shall be in accordance with Paragraph 4.4 of this Standard.

303.2.4 Develop Test Requirements. The contractor shall

participate in the continuing development of changes and requirements to test plans, descriptions, and procedures. The contractor shall develop test descriptions and procedures for SCCSCs.

303.2.5 Develop User, Operator and Diagnostic Manual Requirements. The contractor shall develop safety-related information (e.g., Caution and Warning Notes) for inclusion in the Computer System Diagnostic, Computer System Operator, Firmware Support, and Software User's Manuals, and in other manuals as appropriate.

303.2.6 Identify Safety-Critical Computer Software Components to Code Developers. The contractor shall identify safety-critical computer software units to the code developers, and provide them with explicit safety-related coding recommendations and safety requirements from the top-level specifications and design documents.

303.2.7 Support Critical Design Review. The contractor shall support the Critical Design Review (CDR) from a software safety viewpoint. The contractor shall report the results of the Software Safety Analyses at CDR. The presentation shall include top-level design safety requirements and their implementation, supporting analyses and the methodology used, and any unresolved hazards or issues.

303.3 Details to be specified by the Managing Agency: Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100, 204, 301, 302, and 303.

(R) b. Definition of Safety Critical within the context of the system, subsystem, or component under analysis.

(R) c. Level of contractor support required for design reviews.

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

TASK 304

CODE-LEVEL SOFTWARE HAZARD ANALYSIS

304.1 Purpose: The purpose of Task 304 is to require the contractor to perform and document a Code-Level Software Hazard Analysis (CSHA). Using the results of the DDHA (Task 303), if previously accomplished, the contractor shall analyze program code and system interfaces for events, faults, and conditions which could cause or contribute to undesired events affecting safety. This analysis shall start when coding begins, and shall continue throughout the system life cycle.

304.2 Task Description:

304.2.1 Component Analysis. The contractor shall perform a hazard analysis of all safety-critical computer software components, to include the following subtasks:

a. Analyze:

(1) Safety-Critical Computer Software Components for

correctness and completeness, and for input-output timing, multiple event, out-of-sequence event, failure of event, adverse environment, deadlocking, wrong event, inappropriate magnitude, hardware failure sensitivities, etc.

(2) Software implementation of safety criteria called out in the system specifications and requirements documents.

(3) Possible combinations of hardware failures, software failures, transient errors, and other events that could cause the system to operate in a hazardous manner.

(4) Proper error default handling for special characters or inappropriate or unexpected data in the input data stream.

(5) Fail-safe and fail-soft modes.

(6) Input overload or out-of-bound conditions.

b. Perform a Process Flow Analysis. Perform an internal path and control process flow analysis on safety-critical computer software components.

c. Propose Change Recommendations. Propose design, coding, and testing change recommendations in the specification, design, and test documents to the Government.

d. Support Informal Reviews. Support informal reviews of each safety-critical computer software component.

304.2.2 Review Code Documentation. The contractor shall ensure all safety-critical computer software components and all source code are thoroughly and accurately documented and commented in such a way that future changes by programmers unfamiliar with the original code can be made with a reduced chance of introducing new software safety hazards.

304.2.3 Support the Test Readiness Review. The contractor shall support the Test Readiness Review (TRR) from a software safety viewpoint.

304.3 Details to be specified by the Managing Agency: Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100, 204, 301, 303, and 304.

(R) b. Definition of Safety Critical within the context of the system, subsystem, or component under analysis.

(R) c. Level of contractor support required for design reviews.

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

TASK 305

SOFTWARE SAFETY TESTING

305.1 Purpose. The purpose of Task 305 is to require the contractor to perform and document Software Safety Testing.

305.2 Task Description: The contractor shall test the software to ensure that all hazards have been eliminated or controlled to an acceptable level of risk. The contractor shall include the following in the testing of the software and system: safety-related test descriptions, procedures, and cases, and the associated qualification criteria. Implementation of safety requirements (inhibits, traps, interlocks, assertions, etc.) shall be verified. The contractor shall verify that the software functions safely both within its specified environment, and under abnormal conditions. The following subtasks shall be included:

305.2.1 Component, Integration, Acceptance, and System Testing. The contractor shall participate in the testing of safety-critical computer software components at all levels of testing, including informal testing, system integration testing, and Software Acceptance testing.

a. Enforce Test Discipline. The contractor software safety personnel shall ensure that tests of safety-critical components are conducted in strict accordance with the approved test plans, descriptions, procedures, and cases, and that the results are accurately logged, recorded, documented, analyzed, and reported. The contractor shall ensure that deficiencies and discrepancies are corrected and retested.

b. Support Abnormal Condition Testing. In addition to testing under normal conditions, the software shall be tested to show that unsafe states cannot be generated by the software as the result of feasible single or multiple erroneous inputs. This shall include those outputs which might result from failures associated with the entry into, and execution of, safety-critical computer software components. Negative and No-Go testing shall also be employed, and the contractor shall assure that the software only performs those functions for which it is intended, and no extraneous functions.

c. System Integration and Acceptance Testing. The contractor shall ensure that the software performs properly and safely during system integration stress testing, and system acceptance testing. System acceptance testing shall be conducted under actual operating conditions.

305.2.2 Commercial Software. Commercial software included in the system shall be analyzed and tested unless specifically excluded by the Managing Agency. Commercial software includes commercially developed, commercially acquired, proprietary, and other software not specifically developed for the system. These analyses and tests shall be performed whether this software is modified or not.

305.2.3 Government Furnished Software. The contractor shall subject any Government Furnished software (unless specifically excluded by the Managing Agency), whether modified by the contractor or not, to the same software safety analysis and testing requirements as the software that was developed under the contract which invokes this task.

305.2.4 Hazard Correction. The contractor shall correct the software to eliminate or reduce to an acceptable level of risk any safety hazards discovered during system integration testing or acceptance testing. The corrected software shall be retested under identical conditions to ensure that these hazards have been eliminated, and that other hazards do not occur.

305.3 Details to be specified by the Managing Agency: Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100, 301, and 305.

(R) b. Definition of Safety Critical within the context of the system, subsystem, or component under analysis.

(R) c. Level of contractor support required for design reviews.

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

TASK 306

SOFTWARE/USER INTERFACE ANALYSIS

306.1 Purpose. The purpose of Task 306 is to require the contractor to perform and document a Software/User Interface Analysis and the development of Software Users Procedures.

306.2 Task Description:

306.2.1 The system and its software shall be designed in accordance with the system safety precedence listed in Paragraph 4.4 of this Standard. Identified hazards not eliminated or controlled by the system design and implementation shall be analyzed and design change recommendations made (with corresponding operator procedures) that:

(a) Provide for the detection of a hazard condition.

(b) Provide for a safe survival and recovery methodology from a detected critical hazard condition.

(c) Incorporate an operator warning feature to alert the operator/pilot of software errors that results in non-conformance or equipment malfunctions (e.g., "X function unavailable").

(d) Provide for safe cancellation of processing or of an event.

(e) Provide for the unambiguous and complete display of the status of safety-critical systems or components. Overrides of overridable potential safety critical faults or clearing of the status data should not be permitted until all of the data has been displayed. (e.g., a system has a series of faults that my be safety overridden if they occur singly. However, multiple faults could result in loss of the aircraft or system. The pilot or operator should be made aware of all safety critical faults prior to issuing an override command or resetting a status display.)

306.3 Details to be specified by the Managing Agency: Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100, 301, and 306.

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

TASK 307

SOFTWARE CHANGE HAZARD ANALYSIS

307.1 Purpose. The purpose of Task 307 is to require the contractor to perform and document the Software Change Hazard Analysis.

307.2 Task Description: The contractor shall analyze all changes, modifications, and patches made to the software for safety hazards, to include the following:

307.2.1 Perform Software Hazard Analysis. All changes to specifications, requirements, design, code, systems, equipment, and test plans, descriptions, procedures, cases, or criteria shall be subjected to software hazard analysis and testing, unless it can be shown to be unnecessary due to the nature of the change. The beginning point of this change hazard analysis shall be the highest level within the documentation or system that is affected by the change being proposed.

307.2.2 Resolution of Safety Considerations. The contractor shall show that the change or patch does not create a hazard, does not impact on a hazard that has previously been resolved, does not make a currently existing hazard more severe, and does not adversely affect any safety-critical computer software component or related and interfacing code.

307.2.3 Updating Documentation. The contractor shall review the affected documentation, and ensure that it correctly reflects all safety-related changes that have been made in the software.

307.2.4 Software Configuration Management Plan. The contractor shall include the methods, procedures, and other information on how this task will be performed in the Software Configuration Management Plan.

307.3 Details to be specified by the Managing Agency: Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 100, 301, and 307.

(R) b. Definition of Safety Critical within the context of the system, subsystem, or component under analysis.

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

NOTICE 1

(NOTE: Pages A1 - A4 are missing. Refer to hardcopy. The following text begins page A-5.)

action. A hazard risk index of ID, 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.

307.4 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

TABLE 2. APPLICATION MATRIX FOR FACILITIES ACQUISITION

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 identified 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-SAFT-80100, 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-SAFT-80105, 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-SAFT-80105, 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-SAFT-80101, 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-SAFT-80101, 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 of 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-SAFT-80101, 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-SAFT-80101, 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 effected 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-SAFT-80101, 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-SAFT-80106, Occupational Health Hazard Assessment 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 identified during development, special test plans/procedures will be needed. Safety tests may be documented and reported using DI-SAFT-80102, Safety Assessment 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 operations 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 difference 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-SAFT-80102, Safety Assessment Report. The importance of this report is that it tells the user or the test team of all the residual unsafe design of 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-SAFT-80102, 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-SAFT-80103, Engineering Change Proposal System Safety Report, and DI-SAFT-80104, Waiver or Deviation System Safety 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 RESERVED. For Software Hazard Analysis see 50.3.

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-SAFT-80101, System Safety Hazard Analysis Report.

50.3.0 Software System Safety. The purpose of Software System Safety is to:

(a) Develop safety requirements for the system and the software within the system.

(b) Ensure accurate translation of safety specification requirements into System/Segment Specification (SSS) and Software Requirements Specification (SRS) requirements, and accurate translation of the SSS and SRS safety requirements into the design and code of the software.

(c) Ensure that the SSS and SRSs clearly identify the safety criteria to be used (fail-safe, fail-fire, fail-soft, fail-operational, fail-recovery, etc.)

(d) Identify programs, Computer Software Components (CSCs), routines, modules, or functions and their interfaces which control or influence safety critical hardware functions. These shall be designated Safety Critical Computer Software Components (SCCSC).

(e) Analyze those Safety Critical Computer Software Components and their system interfaces as designed or implemented for events, faults, and environments which could cause or contribute to undesired events affecting safety.

(f) Analyze the implementation of safety design requirements to ensure that it accomplishes the intent of the requirement. The analysis should verify that there are no single point or likely multiple failures that could compromise the safety feature. Implementation of safety requirements should not introduce new hazards or adversely affect other safety requirements.

(g) Ensure that the actual coded software does not cause identified or unidentified hazardous functions to occur or inhibit desired functions, thus creating hazardous conditions.

(h) Effectively mitigate end item hardware hazardous anomalies.

(i) Ensure that safety design requirements are thoroughly tested including fault testing.

The relationships between the various system, hardware, and software safety analyses of MIL-STD-882B; the various reviews and audits of MIL-STD-1521B; and the software documentation required by DOD-STD-2167 are given in Table 3.

50.3.0.1 Some of the current analysis techniques and methodologies that are available to conduct this analysis are:

(a) Software fault tree analysis

(b) Software sneak analysis

(c) Design walk-throughs

(d) Code walk-throughs

(e) Petri net analysis

(f) Software/Hardware integrated critical path analysis.

(g) Nuclear safety cross-check analysis

(h) Cross reference listing analysis

Due to the various strengths and weaknesses of each technique, a thorough software hazard analysis will require application of more than one of these techniques on a particular software element. Additionally, the application of good software engineering practices is vital to designing software that is safe and analyzable.

50.3.0.2 Software System Safety must begin early in the concept phase and must be structured to permit continual revision and updating as the design matures. To ensure an effective analysis effort, the following information is needed:

(a) System/Segment Specifications (SSSs), Software Requirements Specifications (SRSs), Interface Requirements Specifications (IRSs), and other allocation documents which describe the system, all of the various software-software, software-hardware, and software-operator interfaces, and both normal and abnormal environments which the system could encounter.

(b) Functional flow diagrams, timing diagrams, and related data describing the proposed sequence and timing of activities, functions, and operations involving the system elements throughout the life cycle of the system.

(c) Computer program functional flow charts, or their functional equivalents, The Program Design Language (PDL) for the program, storage and timing allocation charts, and other program structure documents as they become available, or when they change.

(d) Background information related to safety requirements associated with the planned testing, manufacturing, shipping, handling, storage, repair, anticipated operational and support environments, as well as lessons learned from similar programs or activities.

(e) Known hazardous event sources, including energy and toxic sources, especially those which may be controlled by software.

(f) The Software Development Plan, Software Quality Evaluation Plan, Software Configuration Management Plan, and other system and subsystem development planning documents.

(g) The System Test Plan, Software Test Plan, and other test documentation.

50.3.1 Software Requirements Hazard Analysis (SRHA - Task 301).

The SRHA effort begins while the system requirements allocation

is being made. The SRHA first establishes a software safety requirements tracking system within the configuration management system. The SRHA also performs a thorough review and analysis of software requirements aimed at identifying existing requirements (as well as requirements generated from the PHL and system PHA) and assuring an accurate flow down of those requirements into the Software Requirements Specification.

Additionally, the analysis produces required and recommended actions to eliminate identified hazards, or reduce their associated risk to an acceptable level, and to make preliminary testing requirements. This effort generally includes the following:

(a) Review of the System/Segment Specification, Subsystem Specifications, Software Requirements Specifications, Interface Requirements Specification, and other system concept and requirements documents to assure that:

(1) safety requirements have been allocated to the software system;

(2) hazards from the PHL and system PHA have been identified; and

(3) traceability of safety requirements exist from the system specification to the detail software requirements specifications.

(b) Analysis of functional flow diagrams (or their functional equivalent), PDL, data flow diagrams, storage and timing allocation charts, and other program documentation to assure that specification and safety requirements will be met.

The results of the SRHA are presented at, and are a part of, the System Requirements Review (SRR), the System Design Review (SDR), and the Software Specification Review.

50.3.2 Top-level Design Hazard Analysis (THDA - Task 302). The THDA begins after the Software Specifications Review, and it expands upon the SRHA. This analysis includes:

(a) Relating those hazards identified in the PHL, PHA, and SRHA to specific CSC items, and identifying those CSCIs which control or affect the hazards as Safety-Critical Computer Software Components (SCCSCs).

(b) Examining the software to determine the independence/dependence and interdependence among Computer Software Components (CSCs), modules, tables, variables, etc. Elements of software which directly or indirectly influence SCCSCs will be identified as also being SCCSCs, which should be analyzed for their undesired effects.

(c) Analyzing the top-level design of the SCCSCs for compliance with the safety requirements, and passing the results to the software designers and program manager.

The results of the TDA are presented at, and are a part of, the Preliminary Design Review (PDR).

50.3.3 Detailed Design Hazard Analysis (DDHA - Task 303). The DDHA begins after the PDR, and it expands upon and is a follow-

on to the Top-Level Software Hazard Analysis. This analysis includes the following:

(a) Relating those hazards identified in the PHA, SRHA, and TDHA to specific low level CSC components, and identifying those components which control of affect the hazards as SCCSCs, which must be analyzed for correctness and undesired effects.

(b) Examining the software to determine the independence/ dependence and interdependence among low level components, modules, tables, variables, etc. Elements of software which directly or indirectly influence SCCSCs will also be identified as being SCCSCs, which must be analyzed for correctness and undesired effects.

(c) Analyzing the detailed design of the SCCSCs for compliance with the safety requirements, and passing the results to the Software designers and program manager.

(d) Developing requirements for inclusion in test plans, descriptions, and procedures.

(e) Developing requirements for inclusion in the Computer System Operator's Manual, Software User's Manual, Computer System Diagnostic Manual, and Firmware Support Manual, and other manuals as appropriate.

(f) Ensure that the code developers know which are the SCCSCs. Also, provide the code developers with safety-related coding recommendations and requirements.

The results of the DDHA, and all other previously conducted safety analyses, are presented at, and are a part of, the Critical Design Review (CDR).

50.3.4 Code-level Software Hazard Analysis (CSHA - Task 304). This analysis examines the actual source and object code of SCCSCs and other CSCs to verify the actual design implementation. This effort must start when coding commences, and be updated until testing is complete. This analysis identifies actions required to eliminate identified hazards or reduce their associated risk to an acceptable level. The analyst shall participate in code reviews and walk-throughs and should participate in peer reviews of code. Specifically, this analysis examines:

(a) SCCSCs (algorithms, components, modules, routines, and calculations) for correctness and for input/output, timing, multiple event, wrong event, out-of-sequence, adverse environment, deadlocking, inappropriate magnitude, and other types of sensitivities.

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

(c) SCCSCs for compliance with safety criteria called out in applicable SSSs or SRSs. Safety critical portions of software must be examined at the source and object code level as well as at the top level and detailed design levels.

(d) SCCSCs for implementation of safety design requirements to ensure that the intent of the requirement is met. The analyst shall determine that single point or likely multiple failures on inputs from external hardware or other modules cannot result in compromise of the safety features. Tests should be designed to test the safety features including fault mode and no-go path testing.

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

(f) Single or multiple combinations of out-of-bounds or overloading input conditions.

Additionally, this task requires a review of the software documentation being developed to ensure that the safety features and requirements of the software are included. The results of the CSHA are presented, and are a part of, the Test Readiness Review (TRR). However, results of the CSHA for lower level units must be given to the programmers while the codes is being developed.

50.3.5 Software Safety Testing (Task 305). Testing of the lower level units of the software begins almost immediately after coding of the unit has been completed. System level testing of the software begins after a successful TRR. Testing, and support of testing, by the contractor's safety personnel includes the following:

(a) Ensuring that the identified safety hazards have been eliminated or reduced to an acceptable level of risk by submitting SCCSCs to appropriate safety testing.

(b) Providing appropriate test procedures, cases, and inputs to test personnel to test the SCCSCs for safe and proper operation.

(c) Ensuring that all of the SCCSCs are tested in accordance with the approved test procedures, and that the test results are accurately recorded.

(d) Testing the software under abnormal environmental and input conditions, as well as normal conditions, and ensuring that it performs properly and safely under these conditions.

(e) Subjecting the software to stress testing and acceptance testing to ensure that it performs properly and safely under stress conditions.

(f) Ensuring that commercially-developed, commercially-available, proprietary, and other software that was not specifically developed under this contract but that will be included in the system performs properly and safely. This applies whether the software is used as-is or is modified by the contractor.

(g) Ensuring that any Government Furnished Software, whether modified or not, that will be used in the system performs properly and safely.

(h) Ensuring that safety hazards, and other deficiencies and discrepancies, that are discovered during system integration and system acceptance testing will be corrected and retested to be sure that they are no longer a problem.

50.3.6 Software/User Interface Analysis (Task 306). The user/operator interface to a program must be developed to ensure that the system will be operated in a safe manner. Further, even after all of the safety analyses and design changes are done, there still may be safety hazards in the system which cannot be eliminated or controlled strictly in the design. Procedures must be developed that will do the following:

(a) Provide for the detection of the onset of a hazardous or potentially hazardous condition in order to prevent the hazard from occurring.

(b) Control the hazard so that it occurs only in specific instances and on specific command from the operator.

(c) Provide a warning to the operator, user, and other personnel indicating that a potentially hazardous situation is about to occur or is occurring.

(d) Ensure that the system will survive if hazard occurs.

(e) Provide damage control and recovery procedures should a hazard occur, or if prevention and control procedures fail.

(f) Provide survival and recovery procedures from critical hazard conditions.

(g) Provide the capability to safely abort or cancel an event, process, or program if required.

(h) Provide a warning to the operator to alert him of system or software malfunctions or failures, and ensure that the operator is made of all such failures existing at one time. This may change the manner in which failures are cleared or overridden.

(i) Ensure that the display of hazard data is unambiguous and provides the operator all necessary data to make safety critical decisions.

50.3.7 Software Change Hazard Analysis (Task 307). Change Analysis is the examining and analyzing of changes, modifications, and patches to specifications, requirements, equipment, software, design, and source and object code for safety impact. If a change has not been analyzed, the system cannot be assumed to be safe. This analysis includes the following:

(a) Analyzing design changes and modifications, and code changes and patches to the system, subsystem, interfaces, logic, procedures, and software for safety impact ensuring that the change does not create new hazards, does not affect a hazard that has previously been resolved, does not make a currently-existing hazard more severe than it currently is, and does not adversely affect any related or interfacing design or code.

(b) Testing the changes to ensure that the new software does not contain safety hazards, whether these hazards are previously known or not.

(c) Ensuring that the change is properly and correctly incorporated into the code.

(d) Reviewing and updating the documentation to reflect these changes.

(e) Incorporating the methods and procedures for performing this task in the Software Configuration Management Plan.

50.3.8 Documentation. The Software Hazard Analysis is documented as part of the System Safety Hazard Analysis Report, using DI-SAFT-80101, tailored as required.

TABLE 3. Relationships

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 justification 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/Programming and Requirements Development Phase. System safety tasks applicable to the concept exploration/programming 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.

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

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

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

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

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

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

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

(l) 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/programming 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 verifying 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 Environment 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 plan 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 analyzes 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 is 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 replentishable 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 or 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 hazard 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.
Task 100	N/A
Task 101	DI-SAFT-80100
Task 102	DI-SAFT-80100
Task 103	As per CDRL
Task 104	As per CDRL
Task 105	DI-SAFT-80105
Task 106	As per CDRL
Task 107	DI-SAFT-80105
Task 108	As per CDRL
Task 201	DI-SAFT-80101
Task 202	DI-SAFT-80101
Task 203	DI-SAFT-80101
Task 204	DI-SAFT-80101
Task 205	DI-SAFT-80101
Task 206	DI-SAFT-80106
Task 207	DI-SAFT-80102
Task 208	As per CDRL
Task 209	DI-SAFT-80102
Task 210	DI-SAFT-80102
Task 211	DI-SAFT-80103/DI-SAFT-80104
Task 212 - RESERVED -	N/A
Task 213	DI-SAFT-80101
Task 301	DI-SAFT-80101
Task 302	DI-SAFT-80101
Task 303	DI-SAFT-80101
Task 304	DI-SAFT-80101
Task 305	DI-SAFT-80101
Task 306	DI-SAFT-80101
Task 307	DI-SAFT-80101

NOTE: The latest version of each data item description required will be used unless otherwise directed by the MA.

SPECIFICATIONS AND STANDARDS REQUISITION

Form Approved
OMB No. 0704-0230
Expires Dec 31, 1991

Public reporting burden for this collection of information is estimated to average 30 minutes per response including the time for reviewing instructions, searching existing data sources gathering and maintaining the data needed and completing and reviewing the collection of information. Send comments regarding this burden estimate of any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0230) Washington, DC 20503. Please DO NOT RETURN your form to either of these addresses. Send your completed form to address in item 9 of instructions

1. CUSTOMER NUMBER (Mandatory for Repeat Orders to expedite requests), CAGE CODE, OR UIC NUMBER

2. YOUR ADDRESS (Print or Type)

[ ] IF YOUR ADDRESS HAS CHANGED, X THIS BLOCK.

3. ATTENTION:

4. DOCUMENTS REQUESTED

a. STANDARDIZATION DOCUMENT NUMBER (Restricted to 5) (From Dod Index of Specifications and Standards) b. QUANTITY c. TITLE

INSTRUCTIONS

1. PRINT OR TYPE ALL INFORMATION.

2. Enter your customer number, CAGE (formerly FSCM), or UIC number at the top of this form. It will expedite your order.

3. If you have a customer number, use the Telephone Order Entry System (TOES) for telephone orders: (215)697-1187 between the hours of 8 a.m. and 8 p.m. Eastern Standard Time, Monday through Friday. See "Guide to Private Industry" for details.

4. Documents ordered must appear in the DoD Index of Specifications and Standards (DODISS) or DODISS Notice. Requests submitted on this form will speed service. Reorder forms will be enclosed with each shipment.

5. Requests for Official Use Documents or documents without Distribution Statement "A" must be submitted via cognizant DoD Inspection Officer or Contract Administrator for certification of "need to know."

6. Non Government Standardization Documents will not be furnished to commercial concerns. Copies may be purchased from the appropriate Non Government Standards Body.

7. Questions concerning documents not listed in the Department of Defense Index of Specifications and Standards (DODISS) or DODISS Notice should be directed to NPFC Attn: Code 105. Telephone: (215)697-2667 or (215)697-2179.

8. Further information may be obtained from NPFC "Guide to Private Industry." Order as GUIDE-1.
