Downloaded from http://www.everyspec.com

NOT MEASUREMENT SENSITIVE

MIL-STD-882E
11 May 2012

SUPERSEDING
MIL-STD-882D
10 February 2000

DEPARTMENT OF DEFENSE STANDARD PRACTICE

SYSTEM SAFETY



AMSC N/A **AREA SAFT**

Downloaded from http://www.everyspec.com

FOREWORD

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

2. This system safety standard practice is a key element of Systems Engineering (SE) that provides a standard, generic method for the identification, classification, and mitigation of hazards.

3. DoD is committed to protecting personnel from accidental death, injury, or occupational illness and safeguarding defense systems, infrastructure, and property from accidental destruction, or damage while executing its mission requirements of national defense. Within mission requirements, the DoD will also ensure that the quality of the environment is protected to the maximum extent practical. Integral to these efforts is the use of a system safety approach to identify hazards and manage the associated risks. A key DoD objective is to expand the use of this system safety methodology to integrate risk management into the overall SE process rather than addressing hazards as operational considerations. It should be used not only by system safety professionals, but also by other functional disciplines such as fire protection engineers, occupational health professionals, and environmental engineers to identify hazards and mitigate risks through the SE process. It is not the intent of this document to make system safety personnel responsible for hazard management in other functional disciplines. However, all functional disciplines using this generic methodology should coordinate their efforts as part of the overall SE process because mitigation measures optimized for only one discipline may create hazards in other disciplines.

4. This system safety standard practice identifies the DoD approach for identifying hazards and assessing and mitigating associated risks encountered in the development, test, production, use, and disposal of defense systems. The approach described herein conforms to Department of Defense Instruction (DoDI) 5000.02. DoDI 5000.02 defines the risk acceptance authorities.

5. This revision incorporates changes to meet Government and industry requests to reinstate task descriptions. These tasks may be specified in contract documents. When this Standard is required in a solicitation or contract, but no specific task is identified, only Sections 3 and 4 are mandatory. The definitions in 3.2 and all of Section 4 delineate the minimum mandatory definitions and requirements for an acceptable system safety effort for any DoD system. This revision aligns the standard practice with current DoD policy; supports DoD strategic plans and goals; and adjusts the organizational arrangement of information to clarify the basic elements of the system safety process, clarify terminology, and define task descriptions to improve hazard management practices. This Standard strengthens integration of other functional disciplines into SE to ultimately improve consistency of hazard management practices across programs. Specific changes include:

a. Reintroduced task descriptions:

(1) 100-series tasks – Management.
(2) 200-series tasks – Analysis.

Downloaded from http://www.everyspec.com

(3) 300-series tasks – Evaluation.
(4) 400-series tasks – Verification.

b. Emphasized the identification of applicable technical requirements.

c. Included additional tasks:

(1) Hazardous Materials Management Plan.
(2) Functional Hazard Analysis.
(3) Systems-of-Systems Hazard Analysis.
(4) Environmental Hazard Analysis.

d. Applied increased dollar values for losses in severity descriptions.

e. Added “Eliminated” level for probability.

f. Added software system safety techniques and practices.

g. Updated appendices.

6. Comments, suggestions, or questions on this document should be addressed to Headquarters Air Force Materiel Command/SES (System Safety Office), 4375 Chidlaw Road, Wright-Patterson Air Force Base, OH 45433-5006 or emailed to afmc.se.mailbox@wpafb.af.mil. Since contact information can change, you may want to verify the currency of this address information using the Acquisition Streamlining and Standardization Information System (ASSIST) online database at https://assist.dla.mil.

Downloaded from http://www.everyspec.com

CONTENTS

PARAGRAPH **PAGE**

FOREWORD ii

1. SCOPE 1
1.1 Scope 1

2. APPLICABLE DOCUMENTS 1
2.1 General 1
2.2 Government documents 1
2.2.1 Specifications, standards, and handbooks 1
2.2.2 Other Government documents, drawings, and publications 2
2.3 Order of precedence 2

3. DEFINITIONS 2
3.1 Acronyms 2
3.2 Definitions 4

4. GENERAL REQUIREMENTS 9
4.1 General 9
4.2 System safety requirements 9
4.3 System safety process 9
4.3.1 Document the system safety approach 10
4.3.2 Identify and document hazards 10
4.3.3 Assess and document risk 10
4.3.4 Identify and document risk mitigation measures 12
4.3.5 Reduce risk 13
4.3.6 Verify, validate, and document risk reduction 13
4.3.7 Accept risk and document 13
4.3.8 Manage life-cycle risk 14
4.4. Software contribution to system risk 14
4.4.1 Software assessments 14
4.4.2 Software safety criticality matrix 16
4.4.3 Assessment of software contribution to risk 17

5. DETAILED REQUIREMENTS 18
5.1 Additional information 18
5.2 Tasks 18
5.3 Task structure 18

6. NOTES 18
6.1 Intended use 18
6.2 Acquisition requirements 18
6.3 Associated Data Item Descriptions (DIDs) 19

Downloaded from http://www.everyspec.com

CONTENTS

PARAGRAPH **PAGE**

6.4 Subject term (key word) listing 19
6.5 Changes from previous issue 20

TASK SECTION 100 - MANAGEMENT

TASK 101 HAZARD IDENTIFICATION AND MITIGATION EFFORT USING THE SYSTEM SAFETY METHODOLOGY 22
TASK 102 SYSTEM SAFETY PROGRAM PLAN 24
TASK 103 HAZARD MANAGEMENT PLAN 30
TASK 104 SUPPORT OF GOVERNMENT REVIEWS/AUDITS 36
TASK 105 INTEGRATED PRODUCT TEAM/WORKING GROUP SUPPORT 37
TASK 106 HAZARD TRACKING SYSTEM 38
TASK 107 HAZARD MANAGEMENT PROGRESS REPORT 40
TASK 108 HAZARDOUS MATERIALS MANAGEMENT PLAN 41

TASK SECTION 200 - ANALYSIS

TASK 201 PRELIMINARY HAZARD LIST 44
TASK 202 PRELIMINARY HAZARD ANALYSIS 46
TASK 203 SYSTEM REQUIREMENTS HAZARD ANALYSIS 49
TASK 204 SUBSYSTEM HAZARD ANALYSIS 51
TASK 205 SYSTEM HAZARD ANALYSIS 54
TASK 206 OPERATING AND SUPPORT HAZARD ANALYSIS 57
TASK 207 HEALTH HAZARD ANALYSIS 60
TASK 208 FUNCTIONAL HAZARD ANALYSIS 68
TASK 209 SYSTEM-OF-SYSTEMS HAZARD ANALYSIS 71
TASK 210 ENVIRONMENTAL HAZARD ANALYSIS 73

TASK SECTION 300 - EVALUATION

TASK 301 SAFETY ASSESSMENT REPORT 78
TASK 302 HAZARD MANAGEMENT ASSESSMENT REPORT 80
TASK 303 TEST AND EVALUATION PARTICIPATION 82
TASK 304 REVIEW OF ENGINEERING CHANGE PROPOSALS, CHANGE NOTICES, DEFICIENCY REPORTS, MISHAPS, AND REQUESTS FOR DEVIATION/WAIVER 84

TASK SECTION 400 - VERIFICATION

TASK 401 SAFETY VERIFICATION 86
TASK 402 EXPLOSIVES HAZARD CLASSIFICATION DATA 88
TASK 403 EXPLOSIVE ORDNANCE DISPOSAL DATA 89

Downloaded from http://www.everyspec.com

CONTENTS

PARAGRAPH **PAGE**

APPENDIX A GUIDANCE FOR THE SYSTEM SAFETY EFFORT 90
APPENDIX B SOFTWARE SYSTEM SAFETY ENGINEERING AND ANALYSIS 92

FIGURES **PAGE**
1. Eight elements of the system safety process 9

B-1. Assessing software's contribution to risk 95

TABLES **PAGE**
I. Severity categories 11
II. Probability levels 11
III. Risk assessment matrix 12
IV. Software control categories 15
V. Software safety criticality matrix 16
VI. Relationship between SwCI, risk level, LOR tasks, and risk 17

A-I. Task application matrix 90
A-II. Example probability levels 91

B-I. Software hazard causal factor risk assessment criteria 96

Downloaded from http://www.everyspec.com

1. SCOPE

1.1 Scope. This system safety standard practice identifies the Department of Defense (DoD) Systems Engineering (SE) approach to eliminating hazards, where possible, and minimizing risks where those hazards cannot be eliminated. DoD Instruction (DoDI) 5000.02 defines the risk acceptance authorities. This Standard covers hazards as they apply to systems / products / equipment / infrastructure (including both hardware and software) throughout design, development, test, production, use, and disposal. When this Standard is required in a solicitation or contract but no specific task is identified, only Sections 3 and 4 are mandatory. The definitions in 3.2 and all of Section 4 delineate the minimum mandatory definitions and requirements for an acceptable system safety effort for any DoD system.

2. APPLICABLE DOCUMENTS

2.1 General. The documents listed in this section are specified in Sections 3, 4, or 5 of this Standard. This section does not include documents cited in other sections of this Standard or recommended for additional information or as examples. While every effort has been made to ensure the completeness of this list, document users are cautioned that they must meet all specified requirements of documents cited in sections 3, 4, or 5 of this standard, whether or not they are listed.

2.2 Government documents.

2.2.1 Specifications, standards, and handbooks. The following specifications, standards, and handbooks form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those cited in the solicitation or contract.

INTERNATIONAL STANDARDIZATION AGREEMENTS

AOP 52	-	North Atlantic Treaty Organization (NATO) Allied Ordnance Publication (AOP) 52, Guidance on Software Safety Design and Assessment of Munitions Related Computing Systems

(Copies of this document are available online at https://assist.dla.mil/quicksearch/ or from the Standardization Document Order Desk, 700 Robbins Avenue, Building 4D, Philadelphia, PA 19111-5094.)

DEPARTMENT OF DEFENSE HANDBOOKS

No Designator	-	Joint Software Systems Safety Engineering Handbook

(Copies of this document are available online at http://www.system-safety.org/links/)

Downloaded from http://www.everyspec.com

2.2.2 Other Government documents, drawings, and publications. The following other Government documents, drawings, and publications form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those cited in the solicitation or contract.

DEPARTMENT OF DEFENSE INSTRUCTIONS

DoDI 5000.02	-	Operation of the Defense Acquisition System
DoDI 6055.07	-	Mishap Notification, Investigation, Reporting, and Record Keeping

(Copies of these document are available online at http://www.dtic.mil/whs/directives/)

2.3 Order of precedence. In the event of a conflict between the text of this document and the references cited herein, the text of this document takes precedence, with the exception of DoDI 5000.02. Nothing in this document supersedes applicable laws and regulations unless a specific exemption has been obtained.

3. DEFINITIONS

3.1 Acronyms.

AFOSH	Air Force Occupational Safety and Health
ANSI	American National Standards Institute
AOP	Allied Ordnance Publication
AMSC	Acquisition Management Systems Control
ASSIST	Acquisition Streamlining and Standardization Information System
ASTM	American Society for Testing and Materials
AT	Autonomous
CAS	Chemical Abstract Service
CDR	Critical Design Review
CFR	Code of Federal Regulations
COTS	Commercial-Off-the-Shelf
DAEHCP	Department of Defense Ammunition and Explosives Hazard Classification Procedures
DID	Data Item Description
DoD	Department of Defense
DoDI	Department of Defense Instruction
DODIC	Department of Defense Identification Code
DOT	Department of Transportation
DT	Developmental Testing
E3	Electromagnetic Environmental Effects
ECP	Engineering Change Proposal
EHA	Environmental Hazard Analysis
EMD	Engineering and Manufacturing Development
EO	Executive Order

Downloaded from http://www.everyspec.com

EOD	Explosive Ordnance Disposal
ESD	Electrostatic Discharge
ESOH	Environment, Safety, and Occupational Health
FHA	Functional Hazard Analysis
FMECA	Failure Modes and Effects Criticality Analysis
FTA	Fault Tree Analysis
GFE	Government-Furnished Equipment
GFI	Government-Furnished Information
GOTS	Government-Off-the-Shelf
HAZMAT	Hazardous Material
HERO	Hazards of Electromagnetic Radiation to Ordnance
HHA	Health Hazard Analysis
HMAR	Hazard Management Assessment Report
HMMP	Hazardous Materials Management Plan
HMP	Hazard Management Plan
HSI	Human Systems Integration
HTS	Hazard Tracking System
IEEE	Institute of Electrical and Electronics Engineers
IM	Insensitive Munitions
IMS	Integrated Master Schedule
IPT	Integrated Product Team
ISO	International Organization for Standardization
IV&V	Independent Verification and Validation
JCIDS	Joint Capabilities Integration and Development System
LOR	Level of Rigor
MANPRINT	Manpower and Personnel Integration
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
MSDS	Material Safety Data Sheet
NATO	North Atlantic Treaty Organization
NAVMC	Navy and Marine Corps
NDI	Non-Developmental Item
NEPA	National Environmental Policy Act
NSI	No Safety Impact
NSN	National Stock Number
O&SHA	Operating and Support Hazard Analysis
OSH	Occupational Safety and Health
OSHA	Occupational Safety and Health Administration
OT	Operational Testing
PESHE	Programmatic Environment, Safety, and Occupational Health Evaluation
PDR	Preliminary Design Review
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PM	Program Manager
PPE	Personal Protective Equipment
RAC	Risk Assessment Code

Downloaded from http://www.everyspec.com

RF	Radio Frequency
RFP	Request for Proposal
RFR	Radio Frequency Radiation
RFT	Redundant Fault Tolerant
SAR	Safety Assessment Report
SAT	Semi-Autonomous
SCC	Software Control Category
SCF	Safety-Critical Function
SCI	Safety-Critical Item
SDP	Software Development Plan
SE	Systems Engineering
SEMP	Systems Engineering Management Plan
SHA	System Hazard Analysis
SMCC	Special Material Content Code
SoS	System-of-Systems
SOW	Statement of Work
SRHA	System Requirements Hazard Analysis
SRF	Safety-Related Function
SRI	Safety-Related Items
SRR	System Requirements Review
SSF	Safety-Significant Function
SSCM	Software Safety Criticality Matrix
SSHA	Subsystem Hazard Analysis
SSPP	System Safety Program Plan
SSSF	Safety-Significant Software Function
STP	Software Test Plan
SwCI	Software Criticality Index
T&E	Test and Evaluation
TEMP	Test and Evaluation Master Plan
TES	Test and Evaluation Strategy
WDSSR	Waiver or Deviation System Safety Report
WG	Working Group

3.2 Definitions. The following mandatory definitions apply when using this Standard.

3.2.1 Acceptable Risk. Risk that the appropriate acceptance authority (as defined in DoDI 5000.02) is willing to accept without additional mitigation.

3.2.2 Acquisition program. A directed, funded effort that provides a new, improved, or continuing materiel, weapon, or information system or service capability in response to an approved need.

3.2.3 Causal factor. One or several mechanisms that trigger the hazard that may result in a mishap.

Downloaded from http://www.everyspec.com

3.2.4 Commercial-off-the-shelf (COTS). Commercial items that require no unique Government modifications or maintenance over the life-cycle of the product to meet the needs of the procuring agency.

3.2.5 Contractor. An entity in private industry that enters into contracts with the Government to provide goods or services. In this Standard, the word also applies to Government-operated activities that develop or perform work on acquisition defense programs.

3.2.6 Environmental impact. An adverse change to the environment wholly or partially caused by the system or its use.

3.2.7 ESOH. An acronym that refers to the combination of disciplines that encompass the processes and approaches for addressing laws, regulations, Executive Orders (EO), DoD policies, environmental compliance, and hazards associated with environmental impacts, system safety (e.g., platforms, systems, system-of-systems, weapons, explosives, software, ordnance, combat systems), occupational safety and health, hazardous materials management, and pollution prevention.

3.2.8 Event risk. The risk associated with a hazard as it applies to a specified hardware/software configuration during an event. Typical events include Developmental Testing/Operational Testing (DT/OT), demonstrations, fielding, post-fielding tests.

3.2.9 Fielding. Placing the system into operational use with units in the field or fleet.

3.2.10 Firmware. The combination of a hardware device and computer instructions or computer data that reside as read-only software on the hardware device. The software cannot be readily modified under program control.

3.2.11 Government-furnished equipment (GFE). Property in the possession of or acquired directly by the Government, and subsequently delivered to or otherwise made available to the contractor for use.

3.2.12 Government-furnished information (GFI). Information in the possession of or acquired directly by the Government, and subsequently delivered to or otherwise made available to the contractor for use. Government furnished information may include items such as lessons learned from similar systems or other data that may not normally be available to non-Government agencies.

3.2.13 Government-off-the-shelf (GOTS). Hardware or software developed, produced, or owned by a government agency that requires no unique modification over the life-cycle of the product to meet the needs of the procuring agency.

3.2.14 Hazard. A real or potential condition that could lead to an unplanned event or series of events (i.e. mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

Downloaded from http://www.everyspec.com

3.2.15 Hazardous material (HAZMAT). Any item or substance that, due to its chemical, physical, toxicological, or biological nature, could cause harm to people, equipment, or the environment.

3.2.16 Human systems integration (HSI). The integrated and comprehensive analysis, design, assessment of requirements, concepts, and resources for system manpower, personnel, training, safety and occupational health, habitability, personnel survivability, and human factors engineering.

3.2.17 Initial risk. The first assessment of the potential risk of an identified hazard. Initial risk establishes a fixed baseline for the hazard.

3.2.18 Level of rigor (LOR). A specification of the depth and breadth of software analysis and verification activities necessary to provide a sufficient level of confidence that a safety-critical or safety-related software function will perform as required.

3.2.19 Life-cycle. All phases of the system's life, including design, research, development, test and evaluation, production, deployment (inventory), operations and support, and disposal.

3.2.20 Mishap. An event or series of events resulting in unintentional death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. For the purposes of this Standard, the term "mishap" includes negative environmental impacts from planned events.

3.2.21 Mitigation measure. Action required to eliminate the hazard or when a hazard cannot be eliminated, reduce the associated risk by lessening the severity of the resulting mishap or lowering the likelihood that a mishap will occur.

3.2.22 Mode. A designated system condition or status (e.g., maintenance, test, operation, storage, transport, and demilitarization).

3.2.23 Monetary Loss. The summation of the estimated costs for equipment repair or replacement, facility repair or replacement, environmental cleanup, personal injury or illness, environmental liabilities, and should include any known fines or penalties resulting from the projected mishap.

3.2.24 Non-developmental item (NDI). Items (hardware, software, communications/ networks, etc.) that are used in the system development program, but are not developed as part of the program. NDIs include, but are not limited to, COTS, GOTS, GFE, re-use items, or previously developed items provided to the program "as is".

3.2.25 Probability. An expression of the likelihood of occurrence of a mishap.

3.2.26 Program Manager (PM). The designated Government individual with responsibility for and authority to accomplish program objectives for development, production,

Downloaded from http://www.everyspec.com

and sustainment of the system/product/equipment to meet the user's operational needs. The PM is accountable for credible cost, schedule, and performance reporting to the Milestone Decision Authority.

3.2.27 Re-use items. Items previously developed under another program or for a separate application that are used in a program.

3.2.28 Risk. A combination of the severity of the mishap and the probability that the mishap will occur.

3.2.29 Risk level. The characterization of risk as either High, Serious, Medium, or Low.

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

3.2.31 Safety-critical. A term applied to a condition, event, operation, process, or item whose mishap severity consequence is either Catastrophic or Critical (e.g., safety-critical function, safety-critical path, and safety-critical component).

3.2.32 Safety-critical function (SCF). A function whose failure to operate or incorrect operation will directly result in a mishap of either Catastrophic or Critical severity.

3.2.33 Safety-critical item (SCI). A hardware or software item that has been determined through analysis to potentially contribute to a hazard with Catastrophic or Critical mishap potential, or that may be implemented to mitigate a hazard with Catastrophic or Critical mishap potential. The definition of the term "safety-critical item" in this Standard is independent of the definition of the term "critical safety item" in Public Laws 108-136 and 109-364.

3.2.34 Safety-related. A term applied to a condition, event, operation, process, or item whose mishap severity consequence is either Marginal or Negligible.

3.2.35 Safety-significant. A term applied to a condition, event, operation, process, or item that is identified as either safety-critical or safety-related.

3.2.36 Severity. The magnitude of potential consequences of a mishap to include: death, injury, occupational illness, damage to or loss of equipment or property, damage to the environment, or monetary loss.

3.2.37 Software. A combination of associated computer instructions and computer data that enable a computer to perform computational or control functions. Software includes computer programs, procedures, rules, and any associated documentation pertaining to the operation of a computer system. Software includes new development, complex programmable logic devices (firmware), NDI, COTS, GOTS, re-used, GFE, and Government-developed software used in the system.

Downloaded from http://www.everyspec.com

3.2.38 Software control category. An assignment of the degree of autonomy, command and control authority, and redundant fault tolerance of a software function in context with its system behavior.

3.2.39 Software re-use. The use of a previously developed software module or software package in a software application for a developmental program.

3.2.40 Software system safety. The application of system safety principles to software.

3.2.41 System. The organization of hardware, software, material, facilities, personnel, data, and services needed to perform a designated function within a stated environment with specified results.

3.2.42 System-of-systems (SoS). A set or arrangement of interdependent systems that are related or connected to provide a given capability.

3.2.43 System safety. The application of engineering and management principles, criteria, and techniques to achieve acceptable risk within the constraints of operational effectiveness and suitability, time, and cost throughout all phases of the system life-cycle.

3.2.44 System safety engineering. An engineering discipline that employs specialized knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify hazards and then to eliminate the hazards or reduce the associated risks when the hazards cannot be eliminated.

3.2.45 System safety management. All plans and actions taken to identify hazards; assess and mitigate associated risks; and track, control, accept, and document risks encountered in the design, development, test, acquisition, use, and disposal of systems, subsystems, equipment, and infrastructure.

3.2.46 System/subsystem specification. The system-level functional and performance requirements, interfaces, adaptation requirements, security and privacy requirements, computer resource requirements, design constraints (including software architecture, data standards, and programming language), software support, precedence requirements, and developmental test requirements for a given system.

3.2.47 Systems engineering. The overarching process that a program team applies to transition from a stated capability to an operationally effective and suitable system. Systems Engineering involves the application of SE processes across the acquisition life-cycle (adapted to every phase) and is intended to be the integrating mechanism for balanced solutions addressing capability needs, design considerations, and constraints. SE also addresses limitations imposed by technology, budget, and schedule. SE processes are applied early in material solution analysis and continuously throughout the total life-cycle.

3.2.48 Target risk. The projected risk level the PM plans to achieve by implementing mitigation measures consistent with the design order of precedence described in 4.3.4.

Downloaded from http://www.everyspec.com

3.2.49 User representative. For fielding events, a Command or agency that has been formally designated in the Joint Capabilities Integration and Development System (JCIDS) process to represent single or multiple users in the capabilities and acquisition process. For non-fielding events, the user representative will be the Command or agency responsible for the personnel, equipment, and environment exposed to the risk. For all events, the user representative will be at a peer level equivalent to the risk acceptance authority.

4. GENERAL REQUIREMENTS

4.1 General. When this Standard is required in a solicitation or contract, but no specific tasks are included, only Sections 3 and 4 apply. The definitions in 3.2 and all of Section 4 delineate the minimum mandatory definitions and requirements for an acceptable system safety effort for any DoD system.

4.2 System safety requirements. Section 4 defines the system safety requirements throughout the life-cycle for any system. When properly applied, these requirements should enable the identification and management of hazards and their associated risks during system developmental and sustaining engineering activities. It is not the intent of this document to make system safety personnel responsible for hazard management in other functional disciplines. However, all functional disciplines using this generic methodology should coordinate their efforts as part of the overall SE process because mitigation measures optimized for only one discipline may create hazards in other disciplines.

4.3 System safety process. The system safety process consists of eight elements. Figure 1 depicts the typical logic sequence of the process. However, iteration between steps may be required.

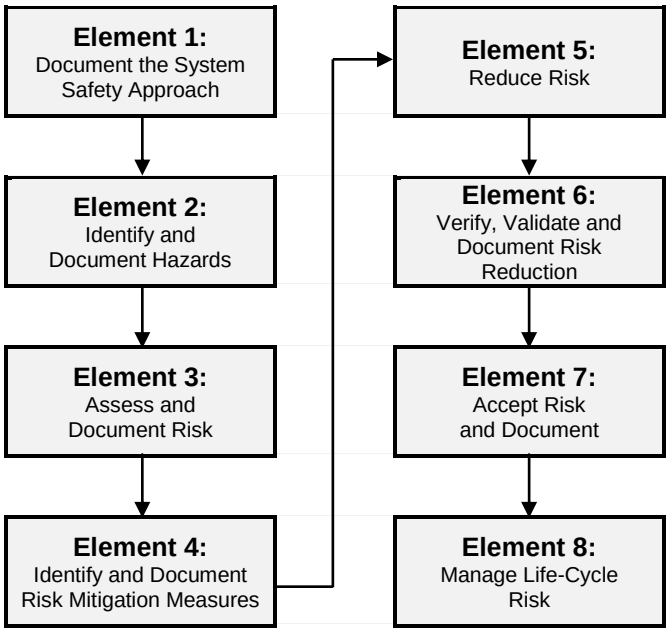


FIGURE 1. Eight elements of the system safety process

Downloaded from http://www.everyspec.com

4.3.1 Document the system safety approach. The PM and contractor shall document the system safety approach for managing hazards as an integral part of the SE process. The minimum requirements for the approach include:

a. Describing the risk management effort and how the program is integrating risk management into the SE process, the Integrated Product and Process Development process, and the overall program management structure.

b. Identifying and documenting the prescribed and derived requirements applicable to the system. Examples include Insensitive Munitions (IM) requirements, Electromagnetic Environmental Effects (E3) requirements, pollution prevention mandates, design requirements, technology considerations, and occupational and community noise standards. Once the requirements are identified, ensure their inclusion in the system specifications and the flow-down of applicable requirements to subcontractors, vendors, and suppliers.

c. Defining how hazards and associated risks are formally accepted by the appropriate risk acceptance authority and concurred with by the user representative in accordance with DoDI 5000.02.

d. Documenting hazards with a closed-loop Hazard Tracking System (HTS). The HTS will include, as a minimum, the following data elements: identified hazards, associated mishaps, risk assessments (initial, target, event(s)), identified risk mitigation measures, selected mitigation measures, hazard status, verification of risk reductions, and risk acceptances. Both the contractor and Government shall have access to the HTS with appropriate controls on data management. The Government shall receive and retain "government purpose rights" of all the data recorded in the HTS and any other items (i.e., studies, analyses, test data, notes or similar data) generated in the performance of the contract with respect to the HTS.

4.3.2 Identify and document hazards. Hazards are identified through a systematic analysis process that includes system hardware and software, system interfaces (to include human interfaces), and the intended use or application and operational environment. Consider and use mishap data; relevant environmental and occupational health data; user physical characteristics; user knowledge, skills, and abilities; and lessons learned from legacy and similar systems. The hazard identification process shall consider the entire system life-cycle and potential impacts to personnel, infrastructure, defense systems, the public, and the environment. Identified hazards shall be documented in the HTS.

4.3.3 Assess and document risk. The severity category and probability level of the potential mishap(s) for each hazard across all system modes are assessed using the definitions in Tables I and II.

a. To determine the appropriate severity category as defined in Table I for a given hazard at a given point in time, identify the potential for death or injury, environmental impact, or monetary loss. A given hazard may have the potential to affect one or all of these three areas.

Downloaded from http://www.everyspec.com

TABLE I. Severity categories

SEVERITY CATEGORIES		
Description	**Severity Category**	**Mishap Result Criteria**
Catastrophic	**1**	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding $10M.
Critical	**2**	Could result in one or more of the following: permanent partial disability,injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding $1M but less than $10M.
Marginal	**3**	Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding $100K but less than $1M.
Negligible	**4**	Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact, or monetary loss less than $100K.

b. To determine the appropriate probability level as defined in Table II for a given hazard at a given point in time, assess the likelihood of occurrence of a mishap. Probability level F is used to document cases where the hazard is no longer present. No amount of doctrine, training, warning, caution, or Personal Protective Equipment (PPE) can move a mishap probability to level F.

TABLE II. Probability levels

PROBABILITY LEVELS			
Description	**Level**	**Specific Individual Item**	**Fleet or Inventory**
Frequent	**A**	Likely to occur often in the life of an item.	Continuously experienced.
Probable	**B**	Will occur several times in the life of an item.	Will occur frequently.
Occasional	**C**	Likely to occur sometime in the life of an item.	Will occur several times.
Remote	**D**	Unlikely, but possible to occur in the life of an item.	Unlikely, but can reasonably be expected to occur.
Improbable	**E**	So unlikely, it can be assumed occurrence may not be experienced in the life of an item.	Unlikely to occur, but possible.
Eliminated	**F**	Incapable of occurence. This level is used when potential hazards are identified and later eliminated.	Incapable of occurence. This level is used when potential hazards are identified and later eliminated.

(1) When available, the use of appropriate and representative quantitative data that defines frequency or rate of occurrence for the hazard, is generally preferable to qualitative analysis. The Improbable level is generally considered to be less than one in a million. See Appendix A for an example of quantitative probability levels.

Downloaded from http://www.everyspec.com

(2) In the absence of such quantitative frequency or rate data, reliance upon the qualitative text descriptions in Table II is necessary and appropriate.

c. Assessed risks are expressed as a Risk Assessment Code (RAC) which is a combination of one severity category and one probability level. For example, a RAC of 1A is the combination of a Catastrophic severity category and a Frequent probability level. Table III assigns a risk level of High, Serious, Medium, or Low for each RAC.

TABLE III. Risk assessment matrix

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

d. The definitions in Tables I and II, and the RACs in Table III shall be used, unless tailored alternative definitions and/or a tailored matrix are formally approved in accordance with DoD Component policy. Alternates shall be derived from Tables I through III.

e. The Program shall document all numerical definitions of probability used in risk assessments as required by 4.3.1. Assessed risks shall be documented in the HTS.

4.3.4 Identify and document risk mitigation measures. Potential risk mitigation(s) shall be identified, and the expected risk reduction(s) of the alternative(s) shall be estimated and documented in the HTS. The goal should always be to eliminate the hazard if possible. When a hazard cannot be eliminated, the associated risk should be reduced to the lowest acceptable level within the constraints of cost, schedule, and performance by applying the system safety design order of precedence. The system safety design order of precedence identifies alternative mitigation approaches and lists them in order of decreasing effectiveness.

Downloaded from http://www.everyspec.com

a. Eliminate hazards through design selection. Ideally, the hazard should be eliminated by selecting a design or material alternative that removes the hazard altogether.

b. Reduce risk through design alteration. If adopting an alternative design change or material to eliminate the hazard is not feasible, consider design changes that reduce the severity and/or the probability of the mishap potential caused by the hazard(s).

c. Incorporate engineered features or devices. If mitigation of the risk through design alteration is not feasible, reduce the severity or the probability of the mishap potential caused by the hazard(s) using engineered features or devices. In general, engineered features actively interrupt the mishap sequence and devices reduce the risk of a mishap.

d. Provide warning devices. If engineered features and devices are not feasible or do not adequately lower the severity or probability of the mishap potential caused by the hazard, include detection and warning systems to alert personnel to the presence of a hazardous condition or occurrence of a hazardous event.

e. Incorporate signage, procedures, training, and PPE. Where design alternatives, design changes, and engineered features and devices are not feasible and warning devices cannot adequately mitigate the severity or probability of the mishap potential caused by the hazard, incorporate signage, procedures, training, and PPE. Signage includes placards, labels, signs and other visual graphics. Procedures and training should include appropriate warnings and cautions. Procedures may prescribe the use of PPE. For hazards assigned Catastrophic or Critical mishap severity categories, the use of signage, procedures, training, and PPE as the only risk reduction method should be avoided.

4.3.5 Reduce risk. Mitigation measures are selected and implemented to achieve an acceptable risk level. Consider and evaluate the cost, feasibility, and effectiveness of candidate mitigation methods as part of the SE and Integrated Product Team (IPT) processes. Present the current hazards, their associated severity and probability assessments, and status of risk reduction efforts at technical reviews.

4.3.6 Verify, validate, and document risk reduction. Verify the implementation and validate the effectiveness of all selected risk mitigation measures through appropriate analysis, testing, demonstration, or inspection. Document the verification and validation in the HTS.

4.3.7 Accept risk and document. Before exposing people, equipment, or the environment to known system-related hazards, the risks shall be accepted by the appropriate authority as defined in DoDI 5000.02. The system configuration and associated documentation that supports the formal risk acceptance decision shall be provided to the Government for retention through the life of the system. The definitions in Tables I and II, the RACs in Table III, and the criteria in Table VI for software shall be used to define the risks at the time of the acceptance decision, unless tailored alternative definitions and/or a tailored matrix are formally approved in accordance with DoD Component policy. The user representative shall be part of this process throughout the life-cycle of the system and shall provide formal concurrence before

Downloaded from http://www.everyspec.com

all Serious and High risk acceptance decisions. After fielding, data from mishap reports, user feedback, and experience with similar systems or other sources may reveal new hazards or demonstrate that the risk for a known hazard is higher or lower than previously recognized. In these cases, the revised risk shall be accepted in accordance with DoDI 5000.02.

NOTE: A single system may require multiple event risk assessments and acceptances throughout its life-cycle. Each risk acceptance decision shall be documented in the HTS.

4.3.8 Manage life-cycle risk. After the system is fielded, the system program office uses the system safety process to identify hazards and maintain the HTS throughout the system's life-cycle. This life-cycle effort considers any changes to include, but not limited to, the interfaces, users, hardware and software, mishap data, mission(s) or profile(s), and system health data. Procedures shall be in place to ensure risk management personnel are aware of these changes, e.g., by being part of the configuration control process. The program office and user community shall maintain effective communications to collaborate, identify, and manage new hazards and modified risks. If a new hazard is discovered or a known hazard is determined to have a higher risk level than previously assessed, the new or revised risk will need to be formally accepted in accordance with DoDI 5000.02. In addition, DoD requires program offices to support system-related Class A and B (as defined in Department of Defense Instruction 6055.07) mishap investigations by providing analyses of hazards that contributed to the mishap and recommendations for materiel risk mitigation measures, especially those that minimize human errors.

4.4 Software contribution to system risk. The assessment of risk for software, and consequently software-controlled or software-intensive systems, cannot rely solely on the risk severity and probability. Determining the probability of failure of a single software function is difficult at best and cannot be based on historical data. Software is generally application-specific and reliability parameters associated with it cannot be estimated in the same manner as hardware. Therefore, another approach shall be used for the assessment of software's contributions to system risk that considers the potential risk severity and the degree of control that software exercises over the hardware.

4.4.1 Software assessments. Tables IV through VI shall be used, unless tailored alternative matrices are formally approved in accordance with DoD Component policy. The degree of software control is defined using the Software Control Categories (SCC) in Table IV (or approved tailored alternative). Table V provides the Software Safety Criticality Matrix (SSCM) based on Table I severity categories (or approved tailored severity categories) and Table IV SCCs. The SSCM establishes the Software Criticality Indices (SwCIs) used to define the required LOR tasks. Table VI provides the relationship between the SwCI, the LOR tasks, and how not meeting the LOR task requirements affects software's contribution to risk.

a. All SCCs should be re-evaluated if legacy software functions are included in a SoS environment. The legacy functions should be evaluated at both the functional and physical interfaces for potential influence or participation in top-level SoS mishap and hazard causal factors.

Downloaded from http://www.everyspec.com

b. The system safety and software system safety hazard analysis processes identify and mitigate the exact software contributors to hazards and mishaps. The successful execution of pre-defined LOR tasks increases the confidence that the software will perform as specified to software performance requirements, while reducing the number of contributors to hazards that may exist in the system. Both processes are essential in reducing the likelihood of software initiating a propagation pathway to a hazardous condition or mishap. Appendix B provides guidance for developing acceptable LOR tasks.

TABLE IV. Software control categories

SOFTWARE CONTROL CATEGORIES		
Level	**Name**	**Description**
1	**Autonomous (AT)**	• Software functionality that exercises autonomous control authority over potentially safety-significant hardware systems, subsystems, or components without the possibility of predetermined safe detection and intervention by a control entity to preclude the occurrence of a mishap or hazard. *(This definition includes complex system/software functionality with multiple subsystems, interacting parallel processors, multiple interfaces, and safety-critical functions that are time critical.)*
2	**Semi-Autonomous (SAT)**	• Software functionality that exercises control authority over potentially safety-significant hardware systems, subsystems, or components, allowing time for predetermined safe detection and intervention by independent safety mechanisms to mitigate or control the mishap or hazard. *(This definition includes the control of moderately complex system/software functionality, no parallel processing, or few interfaces, but other safety systems/mechanisms can partially mitigate. System and software fault detection and annunciation notifies the control entity of the need for required safety actions.)* • Software item that displays safety-significant information requiring immediate operator entity to execute a predetermined action for mitigation or control over a mishap or hazard. Software exception, failure, fault, or delay will allow, or fail to prevent, mishap occurrence. *(This definition assumes that the safety-critical display information may be time-critical, but the time available does not exceed the time required for adequate control entity response and hazard control.)*
3	**Redundant Fault Tolerant (RFT)**	• Software functionality that issues commands over safety-significant hardware systems, subsystems, or components requiring a control entity to complete the command function. The system detection and functional reaction includes redundant, independent fault tolerant mechanisms for each defined hazardous condition. *(This definition assumes that there is adequate fault detection, annunciation, tolerance, and system recovery to prevent the hazard occurrence if software fails, malfunctions, or degrades. There are redundant sources of safety-significant information, and mitigating functionality can respond within any time-critical period.)* • Software that generates information of a safety-critical nature used to make critical decisions. The system includes several redundant, independent fault tolerant mechanisms for each hazardous condition, detection and display.
4	**Influential**	• Software generates information of a safety-related nature used to make decisions by the operator, but does not require operator action to avoid a mishap.
5	**No Safety Impact (NSI)**	• Software functionality that does not possess command or control authority over safety-significant hardware systems, subsystems, or components and does not provide safety-significant information. Software does not provide safety-significant or time sensitive data or information that requires control entity interaction. Software does not transport or resolve communication of safety-significant or time sensitive data.

Downloaded from http://www.everyspec.com

4.4.2 Software Safety Criticality Matrix. The SSCM (Table V) uses Table I severity categories for the columns and Table IV software control categories for the rows. Table V assigns SwCI numbers to each cross-referenced block of the matrix. The SSCM shall define the LOR tasks associated with the specific SwCI. Although it is similar in appearance to the Risk Assessment Matrix (Table III), the SSCM is not an assessment of risk. The LOR tasks associated with each SwCI are the minimum set of tasks required to assess the software contributions to the system-level risk.

TABLE V. Software safety criticality matrix

SOFTWARE SAFETY CRITICALITY MATRIX				
	SEVERITY CATEGORY			
SOFTWARE CONTROL CATEGORY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
1	SwCI 1	SwCI 1	SwCI 3	SwCI 4
2	SwCI 1	SwCI 2	SwCI 3	SwCI 4
3	SwCI 2	SwCI 3	SwCI 4	SwCI 4
4	SwCI 3	SwCI 4	SwCI 4	SwCI 4
5	SwCI 5	SwCI 5	SwCI 5	SwCI 5

SwCI	Level of Rigor Tasks
SwCI 1	Program shall perform analysis of requirements, architecture, design, and code; and conduct in-depth safety-specific testing.
SwCI 2	Program shall perform analysis of requirements, architecture, and design; and conduct in-depth safety-specific testing.
SwCI 3	Program shall perform analysis of requirements and architecture; and conduct in-depth safety-specific testing.
SwCI 4	Program shall conduct safety-specific testing.
SwCI 5	Once assessed by safety engineering as Not Safety, then no safety specific analysis or verification is required.

NOTE: Consult the Joint Software Systems Safety Engineering Handbook and AOP 52 for additional guidance on how to conduct required software analyses.

Downloaded from http://www.everyspec.com

4.4.3 Assessment of software contribution to risk. All software contributions to system risk, including any results of Table VI application, shall be documented in the HTS.

a. The Table V LOR tasks shall be performed to assess the software contributions to the system-level risk. Results of the LOR tasks provide a level of confidence in safety-significant software and document causal factors and hazards that may require mitigation. Results of the LOR tasks shall be included in the risk management process. Appendix B provides an example of how to assign a risk level to software contributions to system risk identified by completing the LOR analysis.

b. If the required LOR tasks are not performed, then the system risk(s) contributions associated with unspecified or incomplete LOR tasks shall be documented according to Table VI. Table VI depicts the relationship between SwCI, risk levels, completion of LOR tasks, and risk assessment.

c. All software contributions to system risk, including any results of Table VI application, shall be documented in the HTS. Perform risk acceptance in accordance with DoDI 5000.02.

TABLE VI. Relationship between SwCI, risk level, LOR tasks, and risk

RELATIONSHIP BETWEEN SwCI, RISK LEVEL, LOR Tasks, AND RISK		
Software Criticality Index (SwCI)	**Risk Level**	**Software LOR Tasks and Risk Assessment/Acceptance**
SwCI 1	**High**	• If SwCI 1 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as HIGH and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 1 LOR tasks or prepare a formal risk assessment for acceptance of a HIGH risk.
SwCI 2	**Serious**	• If SwCI 2 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as SERIOUS and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 2 LOR tasks or prepare a formal risk assessment for acceptance of a SERIOUS risk.
SwCI 3	**Medium**	• If SwCI 3 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as MEDIUM and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 3 LOR tasks or prepare a formal risk assessment for acceptance of a MEDIUM risk.
SwCI 4	**Low**	• If SwCI 4 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as LOW and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 4 LOR tasks or prepare a formal risk assessment for acceptance of a LOW risk.
SwCI 5	**Not Safety**	• No safety-specific analyses or testing is required.

Downloaded from http://www.everyspec.com

5. DETAILED REQUIREMENTS

5.1 Additional information. Individual tasks, Appendix A, and Appendix B contain optional information for developing program-specific requirements.

5.2 Tasks. The tasks in this Standard can be selectively applied to fit a tailored system safety effort. The 100-series tasks apply to management. The 200-series tasks apply to analysis. The 300-series tasks apply to evaluation. The 400-series tasks apply to verification. Each desired task shall be specifically called out in a contract because the task descriptions do not include requirements for any other tasks.

5.3 Task structure. Each individual task is divided into three parts—purpose, task description, and details to be specified.

a. The purpose explains the rationale for performing the task.

b. The task description describes the work a contractor shall perform if the task is placed on contract. When preparing proposals, the contractor may recommend inclusion of additional tasks or deletion of specified tasks with supporting rationale for each addition/deletion.

c. The details to be specified in each task description lists specific information, additions, modifications, deletions, or options to the requirements of the task that should be considered when requiring a task. This information is then included in the contractual document along with the task number. The list provided with each task is not necessarily complete and may be supplemented. Any task selected should be specifically imposed by task number in the Request for Proposal (RFP) and Statement of Work (SOW). The details to be specified that are annotated with an "(R)" are required. The Government provides these details to the contractor for proper implementation of the task.

6. NOTES

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

6.1 Intended use. This system safety standard practice is intended to be used as a key element of SE that provides a standard, generic method for the identification, classification, and mitigation of hazards. It should be used not only by system safety professionals, but also by other functional disciplines such as fire protection engineers, occupational health professionals, and environmental engineers.

6.2 Acquisition requirements. Acquisition documents should specify the following:

a. Title, number, and date of the standard.

Downloaded from http://www.everyspec.com

6.3 Associated Data Item Descriptions (DIDs). DIDs that may be applicable to a system safety effort include:

DID Number	DID Title
DI-ADMIN-81250	Conference Minutes
DI-MISC-80043	Ammunition Data Card
DI-MISC-80370	Safety Engineering Analysis Report
DI-ILSS-81495	Failure Mode Effects and Criticality Analysis Report
DI-SAFT-80101	System Safety Hazard Analysis Report
DI-SAFT-80102	Safety Assessment Report (SAR)
DI-SAFT-80103	Engineering Change Proposal System Safety Report
DI-SAFT-80104	Waiver or Deviation System Safety Report (WDSSR)
DI-SAFT-80105	System Safety Program Progress Report
DI-SAFT-80106	Health Hazard Assessment Report
DI-SAFT-80184	Radiation Hazard Control Procedures
DI-SAFT-80931	Explosive Ordnance Disposal Data
DI-SAFT-81065	Safety Studies Report
DI-SAFT-81066	Safety Studies Plan
DI-SAFT-81299	Explosive Hazard Classification Data
DI-SAFT-81300	Mishap Risk Assessment Report
DI-SAFT-81626	System Safety Program Plan

The Acquisition Streamlining and Standardization Information System (ASSIST) database should be researched at https://assist.dla.mil/quicksearch to ensure that only current and approved DIDs are cited on the DD Form 1423.

6.4 Subject term (key word) listing.

Environment
Environmental impact
ESOH
Hazard
Hazardous material
HAZMAT
Health hazard
Life-cycle
Mishap
NEPA
Occupational health
PESHE
PPE
Probability
Risk
Severity
Software safety

Downloaded from http://www.everyspec.com

System safety engineering
Systems Engineering

6.5 Changes from previous issue. Marginal notations are not used in this revision to identify changes with respect to the previous issue due to the extent of the changes.

Downloaded from http://www.everyspec.com

TASK SECTION 100 - MANAGEMENT

Downloaded from http://www.everyspec.com

TASK 101
HAZARD IDENTIFICATION AND MITIGATION EFFORT USING THE SYSTEM SAFETY METHODOLOGY

101.1 Purpose. Task 101 is to integrate hazard identification and mitigation into the Department of Defense (DoD) acquisition Systems Engineering (SE) process using the system safety methodology. The goal should always be to eliminate the hazard if possible. When a hazard cannot be eliminated, the associated risk should be reduced to the lowest acceptable level within the constraints of cost, schedule, and performance by applying the system safety design order of precedence.

101.2 Task description. The contractor shall:

101.2.1 Establish and execute a hazard identification and mitigation effort within SE that meets the system safety requirements of Section 4, General Requirements, and all other tasks and requirements designated by the Program Manager (PM).

101.2.2 Plan for executing the hazard identification and mitigation effort, including the identification and allocation of adequate manpower and funding resources.

101.2.3 Define roles and responsibilities and interrelationships, as well as lines of communication within the program organization and with associated organizations. Define the interrelationship of the various hazard identification and mitigation efforts with the other SE functional disciplines (to include configuration control and data management, reliability, maintainability, Human Systems Integration (HSI)) and with the other functional elements of the program, including program management, test and evaluation, logistics, financial, and contracting.

101.2.4 Ensure the flow down of applicable requirements to subcontractors, associate contractors, vendors, and suppliers. These requirements include defining the required hazard analyses, risk assessment inputs, and verification data and documentation (including format and methodology) to be developed by the subcontractors, associate contractors, vendors, and suppliers.

101.2.5 Report on assessment and status of hazards at system, subsystem, and component technical reviews, such as the System Requirements Review (SRR), Preliminary Design Review (PDR), Critical Design Review (CDR), Test Readiness Review, and Production Readiness Review.

101.2.6 Use a closed-loop Hazard Tracking System (HTS) that includes subcontractor, vendor, and supplier hazard tracking data. The minimum data elements for this task for the tracking system are hazard, system, subsystem, applicability, requirements references, system mode, causal factor, effects, mishap, initial risk, event risk, target risk, mitigation measures, and hazard status, verification and validation method, acting person(s), record of risk acceptance(s), and hazard management log.

Downloaded from http://www.everyspec.com

101.2.7 The definitions in Tables I and II, and the RACs in Table III shall be used, unless tailored alternative definitions and/or a tailored matrix are formally approved in accordance with DoD Component policy.

101.2.8 As a minimum, report the following:

a. Hazards and associated risks.

b. Functions, items, and materials associated with hazards.

c. Recommended requirements for operation, maintenance, sustainment, and disposal.

d. Recommended mitigation measures.

101.2.9 Identify and provide inputs to the Integrated Master Schedule on event-driven reviews, approvals, certifications, analyses, releases, and documentation.

101.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 101. (R)

b. Identification of functional discipline(s) to be addressed by this task. (R)

c. Requirements for incident processing.

d. Requirements and methodology for reporting on this task.

e. Qualification requirements for key personnel responsible for implementing the hazard identification and mitigation effort.

f. Other specific hazard identification and mitigation requirements, e.g., specific risk definitions and matrix (if they differ from Section 4) to be used on this program.

Downloaded from http://www.everyspec.com

TASK 102
SYSTEM SAFETY PROGRAM PLAN

102.1 Purpose. Task 102 is to develop a System Safety Program Plan (SSPP) that documents the system safety methodology for the identification, classification, and mitigation of safety hazards as part of the overall Systems Engineering (SE) process. The SSPP should be an integral part of the Systems Engineering Management Plan (SEMP). The SSPP shall detail the tasks and activities that are required to implement a systematic approach of hazard analysis, risk assessment, and risk management. The goal should always be to eliminate the hazard if possible. When a hazard cannot be eliminated, the associated risk should be reduced to the lowest acceptable level within the constraints of cost, schedule, and performance by applying the system safety design order of precedence.

102.2 Task description. The contractor shall develop an SSPP to provide a basis of understanding between the contractor and the Program Manager (PM) on how the safety hazard management effort will be integrated into the SE process. The SSPP shall include the following sections:

102.2.1 Scope and objectives. The SSPP shall describe, at a minimum: (1) the scope of the effort in terms of the system and its life-cycle, (2) the overall approach for accomplishing the General Requirements in Section 4 and other contractually required tasks, (3) integration of those efforts into SE and other Program Office management processes in order to support overall program objectives, and (4) resource requirements (funding, qualified personnel, and tools) to execute the SSPP. This Section shall account for all contractual hazard management requirements by providing a matrix that correlates these contractual requirements to the location(s) in the SSPP where each requirement is addressed.

102.2.2 SSPP interfaces. The SSPP shall:

a. Identify the functional disciplines covered by the SSPP.

b. Describe the SSPP interfaces between:

(1) SE.

(2) Other involved disciplines (e.g., logistics, maintainability, quality assurance, reliability, human factors engineering, transportability engineering, and medical support (health hazard assessments)).

102.2.3 Organization. The SSPP shall describe, at a minimum:

a. The organization or function of the system safety efforts within the SE process. Use charts to show the organizational and functional relationships and lines of communication.

b. The staffing (manpower loading and schedule) of the system safety efforts by each of the involved functional disciplines and organizational units for the duration of the contract. The

Downloaded from http://www.everyspec.com

SSPP will identify responsibility and authority of each person and organizational unit involved in executing each of the contractual system safety requirements. The SSPP will also identify key personnel, and provide a summary of the qualifications and credentials of the key system safety personnel. The SSPP will describe how and when the Contractor shall notify the Government prior to changes of key system safety personnel.

c. The procedures the contractor will use to integrate system-level and System-of-Systems (SoS) level hazard management efforts to the extent covered in the contract. These will include:

(1) Defining the roles of each associate contractor and subcontractor (and suppliers and vendors as applicable) to integrate safety requirements for the total system.

(2) Defining the safety interfaces between each associate contractor and subcontractor (and suppliers and vendors as applicable), e.g. integrating hazard analyses.

(3) Establishing Integrated Product Teams (IPTs) or Working Groups (WGs) with representatives from each associate contractor and subcontractor (and suppliers and vendors as applicable).

(4) Describing any specific SoS integration roles and responsibilities.

(5) Integrating hardware and software provided by the Government.

(6) Assigning requirements to action organizations and subcontractors.

(7) Coordinating subcontractor system safety engineering efforts.

(8) Facilitating safety reviews.

(9) Recommending mitigation measures; assessing feasibility, cost, and effectiveness of the measures; and allocating implementation responsibility to associate contractors and subcontractors.

(10) Reporting on program safety status and metrics.

(11) Describing procedures for addressing safety issues between associate contractors and subcontractors.

d. The process through which contractor management decisions will be made including timely notification of hazards with Catastrophic and Critical severity levels, as well as High and Serious risks to the Government; determining actions necessary in the event of mishaps, incidents, or malfunctions; and requesting waivers for safety requirements and program deviations.

102.2.4 Milestones. The SSPP shall, at a minimum:

Downloaded from http://www.everyspec.com

a. Provide a schedule of system safety activities including required inputs and outputs, and start and completion dates that support the SE process.

b. Relate the system safety activities to integrated system-level activities (e.g., design analyses, tests, and demonstrations), technical reviews, program reviews, and major program milestones by recommending their inclusion in the Integrated Master Schedule (IMS).

c. Identify the schedules for subsystem, component, and software activities applicable to the system safety activities but specified in other engineering studies and development efforts.

d. Include a schedule of technical meetings between associate contractors and subcontractors to discuss, review, and integrate the safety effort.

102.2.5 General safety requirements and criteria. The SSPP shall:

a. List the standards and system specifications containing safety requirements that the contractor shall use in the execution of the contract. Include titles, dates, and where applicable, paragraph numbers.

b. Describe general engineering requirements and design criteria for safety risk management during system design and development.

c. Identify safety risk management requirements, to include procedures, for test, operations and support, and disposal.

d. Describe the method for ensuring flow-down of hazard identification and mitigation functions as well as associated requirements to subcontractors/suppliers.

102.2.6 Hazard analysis. At a minimum, the SSPP shall:

a. Describe the processes for hazard identification, risk assessment, risk mitigation, risk communication, and support to risk acceptance.

(1) For hazard identification, the SSPP shall describe the systematic identification process that evaluates the system throughout its life-cycle. This evaluation should include as a minimum system hardware and software, system interfaces (to include human interfaces), the intended use or application and operational environment, and disposal.

(2) For risk assessment, the SSPP shall list the severity categories, probability levels, and Risk Assessment Codes (RACs) that shall be followed. The definitions in Tables I and II, and the RACs in Table III shall be used, unless tailored alternative definitions and/or a tailored matrix are formally approved in accordance with Department of Defense (DoD) Component policy.

Downloaded from http://www.everyspec.com

(3) For risk mitigation, the SSPP shall describe how decisions will be made within the overall SE process. The SSPP shall emphasize that the goal should always be to eliminate the hazard if possible. When a hazard cannot be eliminated, the SSPP should describe the process for determining how the associated risk could be reduced to the lowest acceptable level within the constraints of cost, schedule, and performance by applying the system safety design order of precedence described in Section 4 of this Standard. SE process decisions on which mitigations to pursue will be the result of trade-off discussions between the involved technical disciplines.

(4) For risk acceptance, the SSPP shall describe the plan to address Government risk acceptance to include the procedures for communicating to the Government that a risk acceptance decision is required and providing the risk assessment documentation. In addition, the plan should include the procedures the Government has provided on how the Government will communicate to the Contractor the results of the proposed risk acceptance decision. In accordance with Department of Defense Instruction (DoDI) 5000.02, the Government may have to accept an event risk at multiple points in the life-cycle.

b. Describe the approach for applying safety risk management to the use of Commercial-Off-the-Shelf (COTS), Government-Off-the-Shelf (GOTS), Non-Developmental Item (NDI), Government-Furnished Equipment (GFE), and Government-Furnished Information (GFI).

c. Describe closed-loop procedures for tracking and reporting identified hazards and associated risks, including those involving COTS, GOTS, NDI, GFE, and GFI. Include a detailed description of the Hazard Tracking System (HTS).

d. Describe the process for determining whether a qualitative or quantitative risk assessment is appropriate for a given hazard.

e. Identify the hazard analyses to be performed (e.g., Preliminary Hazard Analysis [PHA], Subsystem Hazard Analysis [SSHA]), analytical techniques to be used (e.g., Fault Tree Analysis [FTA], Failure Modes and Effects Criticality Analysis [FMECA]), and documentation of the results in the HTS.

f. Identify the scope of each analysis, integration of associate contractor and subcontractor hazard analyses with overall system hazard analyses, and the depth within the system that each analytical technique will be used.

g. When conducting SoS hazard analyses, the plan shall describe how analysis of the integrated system design, operations, and the interfaces between the products of each associate contractor or subcontractor and the end item will be executed. Data or analyses provided by associate contractors and subcontractors (and suppliers and vendors as applicable) shall be used in the conduct of this effort.

h. Describe the efforts to identify and control hazards associated with materials used during the system’s life-cycle.

i. Describe a systematic software system safety approach to:

Downloaded from http://www.everyspec.com

(1) Identify and describe the software contributions to system hazards.

(2) Identify safety-significant (safety-critical and safety-related) software functions and software requirements.

(3) Identify the safety requirements associated with safety-significant software components and safety-related items.

(4) Identify and assign the Software Criticality Index (SwCI) for each safety-significant software function (SSSF) and its associated requirements.

102.2.7 Supporting data. At a minimum, the SSPP shall:

a. Describe the approach for collecting and processing pertinent hazard, mishap, and lessons learned data. This should include both historical data from similar or legacy systems used to assist in hazard identification and associated risk assessment, and current system data, e.g., the HTS.

b. Identify all documents or other media incorporating hazard management data by title, contract number, date(s) of delivery, and proposed means of delivery (hard copy, electronic, or real-time access) intended to be delivered to the Government under this contract, including documents or other media with other than unlimited rights for the Government. At a minimum, deliverable data shall include HTS data provided during contract execution and at contract closeout.

102.2.8 Verification and validation. At a minimum, the SSPP shall document how the safety risk management effort will:

a. Verify, validate, and document effectiveness of mitigation measures in reducing risk through test, analysis, inspection, etc.

b. Verify, validate, and document that hardware, software, and procedures comply with identified hazard management requirements.

c. Identify requirements for certifications, independent review board evaluations, and special testing (e.g., insensitive munitions tests and render-safe/emergency disposal procedures).

d. Ensure procedures are in place to transmit verification and validation information to the Government.

102.2.9 Audit program. The SSPP shall describe the techniques and procedures to be employed by the contractor to make sure the requirements of the system safety process, as described in Section 4 of this Standard, are being accomplished.

Downloaded from http://www.everyspec.com

102.2.10 Training. The SSPP shall describe the awareness training for the personnel involved with the system safety process.

102.2.11 Incident reporting. The contractor shall describe in the SSPP the incident (especially mishap and malfunction) alerting, investigation, and reporting processes, including notification of the Government.

102.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 102. (R)

b. Identification of functional discipline(s) to be addressed by this task. (R)

c. Identification of any SoS requirements covered by this task, to include interfacing hardware and software provided by the Government. (R)

d. Requirements and methodology for submittal, review, and approval of this plan. (R)

e. Procedures for communicating formal Governmental risk acceptance to the contractor.

f. Qualification requirements for key functional personnel.

g. Other specific safety risk management requirements, e.g., specific risk definitions and matrix to be used on this program.

Downloaded from http://www.everyspec.com

TASK 103
HAZARD MANAGEMENT PLAN

103.1 Purpose. Task 103 is to develop a Hazard Management Plan (HMP) that documents a standard, generic system safety methodology for the identification, classification, and mitigation of hazards as part of the overall Systems Engineering (SE) process. The HMP should be an integral part of the Systems Engineering Management Plan (SEMP). The HMP shall detail the tasks and activities that are required to implement a systematic approach of hazard analysis, risk assessment, and risk management. The goal should always be to eliminate the hazard if possible. When a hazard cannot be eliminated, the associated risk should be reduced to the lowest acceptable level within the constraints of cost, schedule, and performance by applying the system safety design order of precedence.

103.2 Task description. The contractor shall develop an HMP to provide a basis of understanding between the contractor and the Program Manager (PM) on how the hazard management effort will be integrated into the SE process. The HMP shall include the following sections:

103.2.1 Scope and objectives. The HMP shall describe, at a minimum: (1) the scope of the effort in terms of the system and its life-cycle, (2) the overall approach for accomplishing the General Requirements in Section 4 and other contractually required tasks, (3) integration of those efforts into SE and other Program Office management processes in order to support overall program objectives, and (4) resource requirements (funding, qualified personnel, and tools) to execute the HMP. This Section shall account for all contractual hazard management requirements by providing a matrix that correlates these contractual requirements to the location(s) in the HMP where each requirement is addressed.

103.2.2 HMP interfaces. The HMP shall:

a. Identify the functional disciplines covered by the HMP.

b. Describe the HMP interfaces between:

(1) SE.

(2) Functional disciplines using the system safety methodology as described in Section 4 of this Standard (e.g., system safety, range safety, fire protection engineering, environmental engineering, explosive and ordnance safety, chemical and biological safety, directed energy, laser and radio-frequency safety, software system safety, industrial hygiene, occupational health, and Human Systems Integration (HSI)).

(3) Other involved disciplines (e.g., logistics, maintainability, quality control, reliability, software development, system integration, and test, etc.).

103.2.3 Organization. The HMP shall describe, at a minimum:

Downloaded from http://www.everyspec.com

a. The organization or function of the HMP efforts within the SE process. Use charts to show the organizational and functional relationships and lines of communication.

b. The staffing (manpower loading and schedule) of the HMP efforts by each of the involved functional disciplines and organizational units for the duration of the contract. The HMP will identify responsibility and authority of each person and organizational unit involved in executing each of the contractual HMP requirements. The HMP will also identify key personnel, and provide a summary of their qualifications and credentials. The HMP will describe how and when the Contractor shall notify the Government prior to changes to key personnel implementing the HMP .

c. The procedures the contractor will use to integrate system-level and System-of-Systems (SoS) level hazard management efforts to the extent covered in the contract. These will include:

(1) Defining the roles of each associate contractor and subcontractor (and suppliers and vendors as applicable) to integrate HMP requirements for the total system.

(2) Defining the HMP interfaces between each associate contractor and subcontractor (and suppliers and vendors as applicable), e.g. integrating hazard analyses.

(3) Establishing Integrated Product Teams (IPTs) or Working Groups (WGs) with representatives from each associate contractor and subcontractor (and suppliers and vendors as applicable).

(4) Describing any specific SoS integration roles and responsibilities.

(5) Integrating hardware and software provided by the Government.

(6) Assigning requirements to action organizations and subcontractors.

(7) Coordinating subcontractor HMP engineering efforts.

(8) Recommending mitigation measures; assessing feasibility, cost, and effectiveness of the measures; and allocating implementation responsibility to associate contractors and subcontractors.

(9) Reporting on hazard management status and metrics.

(10) Describing procedures for addressing hazard management issues between associate contractors and subcontractors.

d. The process through which contractor management decisions will be made including timely notification of High and Serious risks to the Government; determining actions necessary in the event of mishaps, incidents, or malfunctions; and requesting waivers for hazard management requirements and program deviations.

Downloaded from http://www.everyspec.com

103.2.4 Milestones. The HMP shall, at a minimum:

a. Provide a schedule of hazard management activities including required inputs and outputs, and start and completion dates that support the SE process.

b. Relate the hazard management activities to integrated system-level activities (e.g., design analyses, tests, and demonstrations), technical reviews, program reviews, and major program milestones by recommending their inclusion in the Integrated Master Schedule (IMS).

c. Identify the schedules for subsystem, component, and software activities applicable to the hazard management activities but specified in other engineering studies and development efforts.

d. Include a schedule of technical meetings between associate contractors and subcontractors to discuss, review, and integrate the safety effort.

103.2.5 General HMP requirements and criteria. The HMP shall:

a. List the standards and system specifications containing hazard management requirements that the contractor shall use in the execution of the contract. Include titles, dates, and where applicable, paragraph numbers.

b. Describe general engineering requirements and design criteria for hazard management during system design and development.

c. Identify hazard management requirements, to include procedures, for test, operations and support, and disposal.

d. Describe the method for ensuring flow-down of hazard identification and mitigation functions as well as associated requirements to subcontractors/suppliers.

103.2.6 Hazard analysis. At a minimum, the HMP shall:

a. Describe the processes for hazard identification, risk assessment, risk mitigation, risk communication, and support to risk acceptance.

(1) For hazard identification, the HMP shall describe the systematic identification process that evaluates the system throughout its life-cycle. This evaluation should include as a minimum system hardware and software, system interfaces (to include human interfaces), the intended use or application and operational environment, and disposal.

(2) For risk assessment, the HMP shall list the severity categories, probability levels, and Risk Assessment Codes (RACs) that shall be followed. The definitions in Tables I and II, and the RACs in Table III shall be used, unless tailored alternative definitions and/or a tailored

Downloaded from http://www.everyspec.com

matrix are formally approved in accordance with Department of Defense (DoD) Component policy.

(3) For risk mitigation, the HMP shall describe how decisions will be made within the overall SE process. The HMP shall emphasize that the goal should always be to eliminate the hazard if possible. When a hazard cannot be eliminated, the HMP should describe the process for determining how the associated risk could be reduced to the lowest acceptable level within the constraints of cost, schedule, and performance by applying the system safety design order of precedence described in Section 4 of this Standard. SE process decisions on which mitigations to pursue will be the result of trade-off discussions between the involved technical disciplines.

(4) For risk acceptance, the HMP shall describe the plan to address Government risk acceptance to include the procedures for communicating to the Government that a risk acceptance decision is required and providing the risk assessment documentation. In addition, the plan should include the procedures the Government has provided on how the Government will communicate to the Contractor the results of the proposed risk acceptance decision. In accordance with Department of Defense Instruction (DoDI) 5000.02, the Government may have to accept an event risk at multiple points in the life-cycle.

b. Describe the approach for applying safety risk management to the use of Commercial-Off-the-Shelf (COTS), Government-Off-the-Shelf (GOTS), Non-Developmental Item (NDI), Government-Furnished Equipment (GFE), and Government-Furnished Information (GFI).

c. Describe closed-loop procedures for tracking and reporting identified hazards and associated risks, including those involving COTS, GOTS, NDI, GFE, and GFI. Include a detailed description of the Hazard Tracking System (HTS).

d. Describe the process for determining whether a qualitative or quantitative risk assessment is appropriate for a given hazard.

e. Identify the hazard analyses to be performed (e.g., Preliminary Hazard Analysis [PHA], Subsystem Hazard Analysis [SSHA]), analytical techniques to be used (e.g., Fault Tree Analysis [FTA], Failure Modes and Effects Criticality Analysis [FMECA]), and documentation of the results in the HTS.

f. Identify the scope of each analysis, integration of associate contractor and subcontractor hazard analyses with overall system hazard analyses, and the depth within the system that each analytical technique will be used (e.g., system level, subsystem level, component level).

g. When conducting SoS hazard analyses, the plan shall describe how analysis of the integrated system design, operations, and the interfaces between the products of each associate contractor or subcontractor and the end item will be executed. Data or analyses provided by associate contractors and subcontractors (and suppliers and vendors as applicable) shall be used in the conduct of this effort.

Downloaded from http://www.everyspec.com

h. Describe the efforts to identify and control hazards associated with materials used during the system's life-cycle.

i. Describe a systematic software system safety approach to:

(1) Identify and describe the software contributions to system hazards.

(2) Identify safety-significant (safety-critical and safety-related) software functions and software requirements.

(3) Identify the safety requirements associated with safety-significant software components and safety-related items.

(4) Identify and assign the Software Criticality Index (SwCI) for each safety-significant software function (SSSF) and its associated requirements.

103.2.7 Supporting data. At a minimum, the HMP shall:

a. Describe the approach for collecting and processing pertinent hazard, mishap, and lessons learned data. This should include both historical data from similar or legacy systems used to assist in hazard identification and associated risk assessment, and current system data, e.g., the HTS.

b. Identify all documents or other media incorporating hazard management data by title, contract number, date(s) of delivery, and proposed means of delivery (hard copy, electronic, or real-time access) intended to be delivered to the Government under this contract, including documents or other media with other than unlimited rights for the Government. At a minimum, deliverable data shall include HTS data provided during contract execution and at contract closeout.

103.2.8 Verification and validation. At a minimum, the HMP shall document how the hazard management effort will:

a. Verify, validate, and document effectiveness of mitigation measures in reducing risk through test, analysis, inspection, etc.

b. Verify, validate, and document that hardware, software, and procedures comply with identified hazard management requirements.

c. Identify requirements for certifications, independent review board evaluations, and special testing (e.g., insensitive munitions tests, Hazards of Electromagnetic Radiation to Ordnance (HERO), Electrostatic Discharge (ESD), and render-safe /emergency disposal procedures).

d. Ensure procedures are in place to transmit verification and validation information to the Government.

Downloaded from http://www.everyspec.com

103.2.9 Audit program. The HMP shall describe the techniques and procedures to be employed by the contractor to make sure the requirements of the system safety process, as described in Section 4 of this Standard, are being accomplished.

103.2.10 Training. The HMP shall describe the awareness training for the personnel involved with hazard management on the HMP process.

103.2.11 Incident reporting. The contractor shall describe in the HMP the incident (especially mishap and malfunction) alerting, investigation, and reporting processes, including notification of the Government.

103.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 103. (R)

b. Identification of functional discipline(s) to be addressed by this task. (R)

c. Identification of any SoS requirements covered by this task, to include interfacing hardware and software provided by the Government. (R)

d. Requirements and methodology for submittal, review, and approval of this plan. (R)

e. Procedures for communicating formal Governmental risk acceptance to the contractor.

f. Qualification requirements for key functional personnel.

g. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program,

Downloaded from http://www.everyspec.com

TASK 104
SUPPORT OF GOVERNMENT REVIEWS/AUDITS

104.1 Purpose. Task 104 is to support reviews, certifications, boards, and audits performed by or for the Government.

104.2 Task description. The contractor shall:

104.2.1 Support Government reviews, audits, and boards such as, but not limited to, program and technical reviews, munitions safety boards, laser safety boards, nuclear safety boards, mission readiness reviews, flight readiness reviews, test readiness reviews, launch readiness reviews, flight safety review boards, and National Environmental Policy Act (NEPA) document public hearings.

104.2.2 Provide technical support to mishap investigations.

104.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 104. (R)

b. Identification of functional discipline(s) to be addressed by this task. (R)

c. Frequency, duration, and probable location(s) of reviews, audits, and boards to be supported, as well as any instructions. (R)

d. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.

Downloaded from http://www.everyspec.com

TASK 105
INTEGRATED PRODUCT TEAM/WORKING GROUP SUPPORT

105.1 Purpose. Task 105 is to provide support to designated program office Integrated Product Teams (IPTs) or Working Groups (WGs).

105.2 Task description. The contractor shall participate as a member of designated IPTs or WGs. Such participation shall include, but is not limited to, the following activities:

a. Summarizing hazard analyses and the status of associated risk reduction efforts.

b. Identifying issues or problems associated with risk mitigations.

c. Working toward agreement on the effectiveness of implemented mitigation measures and associated reduction of risks.

d. Presenting incident (especially mishaps and malfunctions of the system being acquired) assessment results, including recommendations and actions taken to prevent recurrences.

e. Responding to action items assigned by the designated IPT or WG.

f. Reviewing and validating risk reduction requirements, criteria, and constraints applicable to the system.

g. Planning and coordinating support for required reviews and certification processes.

h. Requiring selected subcontractors, associate contractors, suppliers or vendors to participate in the designated IPTs or WGs.

105.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 105. (R)

b. Identification of functional discipline(s) to be addressed by this task. (R)

c. Designated IPTs and WGs to be supported by the contractor. (R)

d. Contractor membership requirements and role assignments, to include preparation and distribution of agendas and minutes as specified. (R)

e. Frequency or total number of IPT or WG meetings and probable location(s). (R)

Downloaded from http://www.everyspec.com

TASK 106
HAZARD TRACKING SYSTEM

106.1 Purpose. Task 106 is to establish and maintain a closed-loop Hazard Tracking System (HTS).

106.2 Task description. The contractor shall establish and maintain an HTS that shall contain, at a minimum for this task:

a. Hazard.

b. System.

c. Subsystem (if applicable).

d. Applicability (version specific hardware designs or software releases).

e. Requirements references.

f. System mode.

g. Causal factor (e.g., hardware, software, human, operational environment).

h. Effects.

i. Mishap.

j. Initial risk assessment code.

k. Target risk assessment code.

l. Event risk assessment code(s).

m. Mitigation measures (identified and selected with traceability to version specific hardware designs or software releases).

n. Hazard status.

o. Verification and validation method.

p. Action person(s) and organizational element.

q. Record of risk acceptance(s) - risk acceptance authority (and user concurrence authority, as applicable) by title and organization, date of acceptance, and location of the signed risk acceptance document(s).

Downloaded from http://www.everyspec.com

r. Hazard management log (record of hazard entry and changes made to any part of the hazard record during the system's life-cycle).

s. Hazardous Material (HAZMAT) data elements as specified by the Government.

106.2.1 The Government shall have access to the HTS with appropriate controls on data management.

106.2.2 Task 108 (Hazardous Materials Management Plan), Task 204 (Subsystem Hazard Analysis), Task 205 (System Hazard Analysis), Task 206 (Operating and Support Hazard Analysis), Task 207 (Health Hazard Analysis), and Task 210 (Environmental Hazard Analysis) may include additional requirements for the HTS.

106.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 106. (R)

b. Identification of functional discipline(s) to be addressed by this task. (R)

c. Government access to the HTS and data rights to all hazard management data. (R)

d. Procedures for communicating formal Governmental risk acceptance to the contractor.

e. Any special data elements, format, or data reporting requirements.

f. Current planned system life-cycle to allow projection of HAZMAT usage or generation if applicable.

g. HAZMAT management exceptions, exemptions, or thresholds if applicable.

h. Additional HAZMAT data elements and report requirements.

i. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.

Downloaded from http://www.everyspec.com

TASK 107
HAZARD MANAGEMENT PROGRESS REPORT

107.1 Purpose. Task 107 is to submit periodic progress reports summarizing the pertinent hazard management and engineering activities that occurred during the reporting period.

107.2 Task description. The contractor shall prepare periodic progress reports summarizing general progress made on hazard management efforts during the specified reporting period and forecasting projected work for the next reporting period. The report will contain, at a minimum, the following information:

a. A brief summary of the activities, progress, and status of the hazard management efforts relative to the scheduled program milestones. The summary shall highlight significant achievements and issues.

b. Identification of newly recognized hazards and significant changes in controlling the risk of known hazards.

c. Implementation status of recommended mitigation measures.

d. Significant cost, schedule, and performance changes impacting the hazard management effort.

e. Discussion of contractor documentation reviewed during the reporting period. The discussion shall include document titles and any significant issues.

107.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 107. (R)

b. Identification of functional discipline(s) to be addressed by this task. (R)

c. Progress reporting period. (R)

d. Special data elements, format, or data reporting requirements.

e. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.

Downloaded from http://www.everyspec.com

TASK 108
HAZARDOUS MATERIALS MANAGEMENT PLAN

108.1 Purpose. Task 108 is to implement a Hazardous Materials Management Plan (HMMP) which shall be made available to the Government on request. Hazardous Material (HAZMAT) management is an integral part of the risk management effort within the program's System Engineering (SE) process using this Standard's methodology.

108.2 Task description. The contractor shall use the HMMP to define contractor roles, responsibilities, and procedures needed to accomplish HAZMAT management and tracking. The plan shall account for contractually required HAZMAT management tasks and responsibilities. At a minimum, the HMMP shall identify the following:

a. The processes to properly identify, analyze, and control HAZMAT risks to protect human health, safety, and the environment, as well as to support end user needs.

b. Procedures for tracking and reporting HAZMAT.

108.2.1 HAZMAT identification. A HAZMAT is defined as any item or substance that, due to its chemical, physical, toxicological, or biological nature, could cause harm to people, equipment, or the environment.

108.2.2 HAZMAT Categorization. Following contract award, a list of HAZMAT within the delivered hardware and/or required for system operation and support, categorized as prohibited, restricted, or tracked, will be mutually agreed upon by the Government and contractor.

a. Prohibited HAZMAT require the contractor to obtain Government approval before those materials can be included in the system, subsystems, and support equipment or planned for system operation or support.

b. Restricted HAZMAT are those materials that the contractor will target for elimination or minimization.

c. Tracked HAZMAT are those materials that do not require specific contractor action other than tracking and reporting.

d. HAZMAT used for production or manufacturing will only be included in the HMMP when mutually agreed upon by both the Government and contractor.

108.2.3 Modification of HAZMAT list or categorizations. Proposed changes to the HAZMAT list or categorization will be mutually agreed upon by the Government and contractor.

108.2.4 HAZMAT data tracking. The contractor will be required to track and report all prohibited, restricted, and tracked HAZMAT included in the delivered system, subsystems, and

Downloaded from http://www.everyspec.com

support equipment or planned for system operation or support. The minimum data elements required for HAZMAT tracking and reporting will include:

a. HAZMAT item or substance name.

b. HAZMAT Category (prohibited, restricted, or tracked).

c. Special Material Content Code (SMCC) as designated in DoD 4100.39-M, Volume 10.

d. Location of HAZMAT within the system.

e. Quantity of HAZMAT within the system with traceability, as applicable, to version specific hardware designs.

f. Application, process, or activity whereby quantities of HAZMAT are embedded in the system, or used during operations, and support of the system.

g. Reasonably anticipated HAZMAT (whether categorized or not) generated during the system's life-cycle (e.g., installation, Government test and evaluation, normal use, and maintenance or repair of the system).

h. Reasonably anticipated HAZMAT (whether categorized or not) generated during mishap occurence.

i. Special HAZMAT control, training, handling measures, and Personal Protective Equipment (PPE) needed, including provision of required Material Safety Data Sheets (MSDSs).

108.3. Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 108 to establish contractual HAZMAT management requirements as early in the program life-cycle as possible. (R)

b. Identification of the Government HAZMAT review and approval authority(ies). (R)

c. Listing of proposed prohibited, restricted, and tracked materials.

d. Special data elements, format, or data reporting requirements.

e. System life-cycle phases included in the projection of HAZMAT usage or generation.

f. Listing of HAZMAT management assumptions, limitations, exceptions, exemptions, or thresholds.

g. Requirement to report HAZMAT used by the contractor for production or manufacturing processes.

Downloaded from http://www.everyspec.com

TASK SECTION 200 - ANALYSIS

Downloaded from http://www.everyspec.com

TASK 201
PRELIMINARY HAZARD LIST

201.1 Purpose. Task 201 is to compile a list of potential hazards early in development.

201.2 Task description. The contractor shall:

201.2.1 Examine the system shortly after the materiel solution analysis begins and compile a Preliminary Hazard List (PHL) identifying potential hazards inherent in the concept.

201.2.2 Review historical documentation on similar and legacy systems, including but not limited to:

a. Mishap and incident reports.

b. Hazard tracking systems.

c. Lessons learned.

d. Safety analyses and assessments.

e. Health hazard information.

f. Test documentation.

g. Environmental issues at potential locations for system testing, training, fielding/basing, and maintenance (organizational and depot).

h. Documentation associated with National Environmental Policy Act (NEPA) and Executive Order (EO) 12114, Environmental Effects Abroad of Major Federal Actions.

i. Demilitarization and disposal plans.

201.2.3 The contractor shall document identified hazards in the Hazard Tracking System (HTS). Contents and formats will be as agreed upon between the contractor and the Program Office. Unless otherwise specified in 201.3.d, minimum content shall included:

a. A brief description of the hazard.

b. The causal factor(s) for each identified hazard.

201.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 201. (R)

Downloaded from http://www.everyspec.com

b. Identification of functional discipline(s) to be addressed by this task. (R)

c. Guidance on obtaining access to Government documentation.

d. Content and format requirements for the PHL.

e. Concept of operations.

f. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.

g. References and sources of hazard identification.

Downloaded from http://www.everyspec.com

TASK 202
PRELIMINARY HAZARD ANALYSIS

202.1 Purpose. Task 202 is to perform and document a Preliminary Hazard Analysis (PHA) to identify hazards, assess the initial risks, and identify potential mitigation measures.

202.2 Task description. The contractor shall perform and document a PHA to determine initial risk assessments of identified hazards. Hazards associated with the proposed design or function shall be evaluated for severity and probability based on the best available data, including mishap data (as accessible) from similar systems, legacy systems, and other lessons learned. Provisions, alternatives, and mitigation measures to eliminate hazards or reduce associated risk shall be included.

202.2.1 The contractor shall document the results of the PHA in the Hazard Tracking System (HTS).

202.2.2 The PHA shall identify hazards by considering the potential contribution to subsystem or system mishaps from:

a. System components.

b. Energy sources.

c. Ordnance.

d. Hazardous Materials (HAZMAT).

e. Interfaces and controls.

f. Interface considerations to other systems when in a network or System-of-Systems (SoS) architecture.

g. Material compatibilities.

h. Inadvertent activation.

i. Commercial-Off-the-Shelf (COTS), Government-Off-the-Shelf (GOTS), Non-Developmental Items (NDIs), and Government-Furnished Equipment (GFE).

j. Software, including software developed by other contractors or sources. Design criteria to control safety-significant software commands and responses (e.g., inadvertent command, failure to command, untimely command or responses, and inappropriate magnitude) shall be identified, and appropriate action shall be taken to incorporate these into the software (and related hardware) specifications.

k. Operating environment and constraints.

Downloaded from http://www.everyspec.com

l. Procedures for operating, test, maintenance, built-in-test, diagnostics, emergencies, explosive ordnance render-safe and emergency disposal.

m. Modes.

n. Health hazards.

o. Environmental impacts.

p. Human factors engineering and human error analysis of operator functions, tasks, and requirements.

q. Life support requirements and safety implications in manned systems, including crash safety, egress, rescue, survival, and salvage.

r. Event-unique hazards.

s. Built infrastructure, real property installed equipment, and support equipment.

t. Malfunctions of the SoS, system, subsystems, components, or software.

202.2.3 For each identified hazard, the PHA shall include an initial risk assessment. The definitions in Tables I and II, and the Risk Assessment Codes (RACs) in Table III shall be used, unless tailored alternative definitions and/or a tailored matrix are formally approved in accordance with Department of Defense (DoD) Component policy.

202.2.4 For each identified hazard, the PHA shall identify potential risk mitigation measures using the system safety design order of precedence specified in 4.3.4.

202.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 202. (R)

b. Identification of functional discipline(s) to be addressed by this task. (R)

c. Special data elements, format, or data reporting requirements (consider Task 106, Hazard Tracking System).

d. Identification of hazards, hazardous areas, or other specific items to be examined or excluded.

e. Technical data on COTS, GOTS, NDIs, and GFE to enable the contractor to accomplish the defined task.

Downloaded from http://www.everyspec.com

f. Concept of operations.

g. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.

Downloaded from http://www.everyspec.com

TASK 203
SYSTEM REQUIREMENTS HAZARD ANALYSIS

203.1 Purpose. Task 203 is to perform and document a System Requirements Hazard Analysis (SRHA) to determine the design requirements to eliminate hazards or reduce the associated risks for a system, to incorporate these requirements into the appropriate system documentation, and to assess compliance of the system with these requirements. The SRHA addresses all life-cycle phases and modes.

203.2 Task description. The contractor shall perform and document an SRHA to:

203.2.1 Determine system design requirements to eliminate hazards or reduce the associated risks by identifying applicable policies, regulations, standards, etc. and analyzing identified hazards.

a. The contractor shall identify applicable requirements by reviewing military and industry standards and specifications; historical documentation on similar and legacy systems; Department of Defense (DoD) requirements (to include risk mitigation technology requirements); system performance specifications; other system design requirements and documents; applicable Federal, military, State, and local regulations; and applicable Executive Orders (EOs) and international agreements.

b. The contractor shall recommend appropriate system design requirements to eliminate hazards or reduce the associated risks identified in accordance with Section 4 of this Standard.

c. The contractor shall define verification and validation approaches for each design requirement to eliminate hazards or reduce associated risk.

203.2.2 Incorporate approved design requirements into the engineering design documents, and hardware, software, and system test plans, as appropriate. As the design evolves, ensure applicable design requirements flow down into the system and subsystem specifications, preliminary hardware configuration item development specifications, software requirements specifications, interface requirements specifications, and equivalent documents. As appropriate, use engineering change proposals to incorporate applicable design requirements into these documents.

203.2.3 Assess compliance of the development of the system hardware and associated software with the identified requirements. The contractor shall:

a. Address requirements at all contractually required technical reviews, including design reviews (such as Preliminary Design Review (PDR) and Critical Design Review (CDR)) and the Software Specification Review. The contractor shall address the hazards, mitigation measures, means of verification and validation, and recommendations.

Downloaded from http://www.everyspec.com

b. Review test plans and results for verification and validation of hardware and software compliance with requirements. This includes verification and validation of the effectiveness of risk mitigation measures.

c. Ensure that hazard mitigation information are incorporated into the operator, maintenance, user, training, logistics, diagnostic, and demilitarization and disposal manuals and plans.

203.3. Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 203. (R)

b. Identification of functional discipline(s) design requirements to be addressed by this task. (R)

c. Contractor level of effort support required for design, technical, and other program reviews. (R)

d. Tailor 203.2.2 and 203.2.3 as appropriate to reflect the contractual relationship with the contractor responsible for design. (R)

e. Concept of operations.

f. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.

Downloaded from http://www.everyspec.com

TASK 204
SUBSYSTEM HAZARD ANALYSIS

204.1 Purpose. Task 204 is to perform and document a Subsystem Hazard Analysis (SSHA) to verify subsystem compliance with requirements to eliminate hazards or reduce the associated risks; to identify previously unidentified hazards associated with the design of subsystems; and, to recommend actions necessary to eliminate identified hazards or mitigate their associated risks.

204.2 Task description. The contractor shall perform and document an SSHA to identify hazards and mitigation measures in components and equipment. This analysis shall include Commercial-Off-the-Shelf (COTS), Government-Off-the-Shelf (GOTS), Government-Furnished Equipment (GFE), Non-Developmental Items (NDI), and software. Areas to consider include performance, performance degradation, functional failures, timing errors, design errors or defects, and inadvertent functioning. While conducting this analysis, the human shall be considered a component within a subsystem, receiving both inputs and initiating outputs.

204.2.1 At a minimum, the analysis shall:

a. Verify subsystem compliance with requirements to eliminate hazards or reduce the associated risks.

(1) Validate applicable flow-down of design requirements from top-level specifications to detailed design specifications for the subsystem.

(2) Ensure design criteria in the subsystem specifications have been satisfied and that verification and validation of subsystem mitigation measures have been included in test plans and procedures.

b. Identify previously unidentified hazards associated with the design of subsystems.

(1) Ensure implementation of subsystem design requirements and mitigation measures have not introduced any new hazards.

(2) Determine modes of failure, including component failure modes and human errors, single point and common mode failures, the effects when failures occur in subsystem components, and from functional relationships between components and equipment comprising each subsystem. Consider the potential contribution of subsystem hardware and software events (including those developed by other contractors/sources, COTS, GOTS, NDIs, and GFE hardware or software), faults, and occurrences (such as improper timing).

c. Recommend actions necessary to eliminate previously unidentified hazards or mitigate their associated risk. Ensure system-level hazards attributed to the subsystem are analyzed and adequate mitigations of the potential hazards are implemented in the design.

Downloaded from http://www.everyspec.com

204.2.2 If no specific analysis techniques are directed or if the contractor recommends a different technique than that specified by the Program Manager (PM), the contractor shall obtain PM approval of techniques to be used before performing the analysis.

204.2.3 When software to be used in conjunction with the subsystem is developed under a separate software development effort, 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. Hazards identified that require mitigation action by the software developer shall be reported to the PM in order to request appropriate direction be provided to the software developers.

204.2.4 The contractor shall update, as necessary, the SSHA following system design changes, including software design changes.

204.2.5 The contractor shall prepare a report that contains the results from the task described in paragraph 204.2 and includes:

a. System description. This summary describes the physical and functional characteristics of the system, a list of its subsystems, and a detailed description of the subsystem(s) being analyzed, including its boundaries. Reference to more detailed system and subsystem descriptions, including specifications and detailed review documentation, shall be supplied when such documentation is available.

b. Hazard analysis methods and techniques. Provide a description of each method and technique used in conduct of the analysis. Include a description of assumptions made for each analysis and the qualitative or quantitative data used.

c. Hazard analysis results. Contents and formats may vary according to the individual requirements of the program and methods and techniques used. As applicable, analysis results should be captured in the Hazard Tracking System (HTS).

204.3. Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 204. (R)

b. Identification of functional discipline(s) to be addressed by this task. (R)

c. Identification of subsystem(s) to be analyzed.

d. Desired analysis methodologies and technique(s), and any special data elements, format, or data reporting requirements (consider Task 106, Hazard Tracking System).

e. Selected hazards, hazardous areas, or other specific items to be examined or excluded.

Downloaded from http://www.everyspec.com

f. COTS, GOTS, NDI, and GFE technical data to enable the contractor to accomplish the defined task.

g. Concept of operations.

h. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.

Downloaded from http://www.everyspec.com

TASK 205
SYSTEM HAZARD ANALYSIS

205.1 Purpose. Task 205 is to perform and document a System Hazard Analysis (SHA) to verify system compliance with requirements to eliminate hazards or reduce the associated risks; to identify previously unidentified hazards associated with the subsystem interfaces and faults; identify hazards associated with the integrated system design, including software and subsystem interfaces; and to recommend actions necessary to eliminate identified hazards or mitigate their associated risks.

205.2 Task description. The contractor shall perform and document an SHA to identify hazards and mitigation measures in the integrated system design, including software and subsystem and human interfaces. This analysis shall include interfaces associated with Commercial-Off-the-Shelf (COTS), Government-Off-the-Shelf (GOTS), Government-Furnished Equipment (GFE), Non-Developmental Items (NDI), and software. Areas to consider include performance, performance degradation, functional failures, timing errors, design errors or defects, and inadvertent functioning. While conducting this analysis, the human shall be considered a component within the system, receiving both inputs and initiating outputs.

205.2.1 This analysis shall include a review of subsystems interrelationships for:

a. Verification of system compliance with requirements to eliminate hazards or reduce the associated risks.

b. Identification of previously unidentified hazards associated with design of the system. Recommend actions necessary to eliminate these hazards or mitigate their associated risk.

c. Possible independent, dependent, and simultaneous events, including system failures, failures of safety devices, common cause failures, and system interactions that could create a hazard or result in an increase in risk.

d. Degradation of a subsystem or the total system.

e. Design changes that affect subsystems.

f. Effects of human errors.

g. Determination:

(1) Of potential contribution of hardware and software events (including those that are developed by other contractors/sources, COTS, GOTS, NDIs, and GFE hardware or software), faults, and occurrences (such as improper timing) on the potential for mishaps.

(2) Of whether design requirements in the system specifications have been satisfied.

Downloaded from http://www.everyspec.com

(3) Of whether the methods of implementing the system design requirements and mitigation measures have introduced any new hazards.

205.2.2 If no specific analysis techniques are directed or if the contractor recommends a different technique than the one specified by the Program Manager (PM), the contractor shall obtain PM approval of techniques to be used before performing the analysis.

205.2.3 When software to be used within the system is being developed under a separate software development effort, 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. Hazards identified that require mitigation action by the software developer shall be reported to the PM in order to request appropriate direction be provided to the software developers.

205.2.4 The contractor shall evaluate system design changes, including software design changes, and update the SHA as necessary.

205.2.5. The contractor shall prepare a report that contains the results from the task described in paragraph 205.2 and includes:

a. System description. The system description provides the physical and functional characteristics of the system and its subsystem interfaces. Reference to more detailed system and subsystem descriptions, including specifications and detailed review documentation, shall be supplied when such documentation is available.

b. Hazard analysis methods and techniques. Provide a description of each method and technique used in conduct of the analysis. Include a description of assumptions made for each analysis and the qualitative or quantitative data used.

c. Hazard analysis results. Contents and formats may vary according to the individual requirements of the program and methods and techniques used. As applicable, analysis results should be captured in the Hazard Tracking System (HTS).

205.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 205. (R)

b. Identification of functional discipline(s) to be addressed by this task. (R)

c. Desired analysis methodologies and technique(s) and any special data elements, format, or data reporting requirements (consider Task 106, Hazard Tracking System).

d. Selected hazards, hazardous areas, or other specific items to be examined or excluded.

Downloaded from http://www.everyspec.com

e. COTS, GOTS, NDI, and GFE technical data to enable the contractor to accomplish the defined task.

f. Concept of operations.

g. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.

Downloaded from http://www.everyspec.com

TASK 206
OPERATING AND SUPPORT HAZARD ANALYSIS

206.1 Purpose. Task 206 is to perform and document an Operating and Support Hazard Analysis (O&SHA) to identify and assess hazards introduced by operational and support activities and procedures; and to evaluate the adequacy of operational and support procedures, facilities, processes, and equipment used to mitigate risks associated with identified hazards.

206.2 Task description. The contractor shall perform and document an O&SHA that typically begins during Engineering and Manufacturing Development (EMD) and builds on system design hazard analyses. The O&SHA shall identify the requirements (or alternatives) needed to eliminate hazards or mitigate the associated risks for hazards that could not be eliminated. The human shall be considered an element of the total system, receiving both inputs and initiating outputs within the analysis.

206.2.1 The O&SHA considers the following:

a. Planned system configuration(s)

b. Facility/installation interfaces to the system

c. Planned operation and support environments

d. Supporting tools or other equipment

e. Operating and support procedures

f. Task sequence, concurrent task effects, and limitations

g. Human factors, regulatory, or contractually specified personnel requirements

h. Potential for unplanned events, including hazards introduced by human errors

i. Past evaluations of related legacy systems and their support operations

206.2.2 At a minimum, the analysis shall identify:

a. Activities involving known hazards; the time periods, approximate frequency, and numbers of personnel involved; and the actions required to minimize risk during these activities.

b. Changes needed in functional or design requirements for system hardware, software, facilities, tooling, or support/test equipment to eliminate hazards or mitigate the associated risks for hazards that could not be eliminated.

c. Requirements for engineered features, devices, and equipment to eliminate hazards or reduce risk.

Downloaded from http://www.everyspec.com

d. Requirements for Personal Protective Equipment (PPE), to include its limitations.

e. Warnings, cautions, and special emergency procedures.

f. Requirements for packaging, handling, storage, and transportation to eliminate hazards or reduce risk.

g. Requirements for packaging, handling, storage, transportation, and disposal of Hazardous Materials (HAZMAT) and hazardous wastes.

h. Training requirements.

i. Effects of Commercial-Off-the-Shelf (COTS), Government-Off-the-Shelf (GOTS), Government-Furnished Equipment (GFE) and Non-Developmental Item (NDI) hardware and software across interfaces with other system components or subsystems.

j. Potentially hazardous system modes under operator control.

k. Related legacy systems, facilities, and processes which may provide background information relevant to operating and supporting hazard analysis.

206.2.3 If no specific analysis techniques are directed or if the contractor recommends a different technique than the one specified by the Program Manager (PM), the contractor shall obtain PM approval of the technique(s) to be used before performing the analysis.

206.2.4 The contractor shall update the O&SHA following system design or operational changes as necessary.

206.2.5 The contractor shall document the results of the analysis to include the following information:

a. System description. This summary describes the physical and functional characteristics of the system and its subsystems. Reference to more detailed system and subsystem descriptions, including specifications and detailed review documentation, shall be supplied when such documentation is available.

b. Hazard analysis methods and techniques. Provide a description of each method and technique used in conduct of the analysis. Include a description of assumptions made for each analysis and the qualitative or quantitative data used.

c. Hazard analysis results. Contents and formats may vary according to the individual requirements of the program and methods and techniques used. As applicable, analysis results should be captured in the Hazard Tracking System (HTS). Ensure the results include a complete list of warnings, cautions, and procedures required in operating and maintenance manuals and for training courses.

Downloaded from http://www.everyspec.com

206.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 206. (R)

b. Identification of functional discipline(s) to be addressed by this task. (R)

c. Minimum reporting requirements. (R)

d. Desired analysis methodologies and technique(s) and any special data elements, format, or data reporting requirements (consider Task 106, Hazard Tracking System).

e. Selected hazards, hazardous areas, or other specific items to be examined or excluded.

f. COTS, GOTS, NDI, and GFE technical data to enable the contractor to accomplish the defined task.

g. Legacy and related processes and equipment and associated hazard analyses to be reviewed.

h. How information reported in this task will be correlated with tasks and analyses that may provide related information, such as Task 207 (Health Hazard Analysis).

i. Concept of operations.

j. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.

Downloaded from http://www.everyspec.com

TASK 207
HEALTH HAZARD ANALYSIS

207.1 Purpose. Task 207 is to perform and document a Health Hazard Analysis (HHA) to identify human health hazards, to evaluate proposed hazardous materials and processes using such materials, and to propose measures to eliminate the hazards or reduce the associated risks when the hazards cannot be eliminated.

207.2 Task description. The contractor shall perform and document a HHA that includes evaluations of the potential effects resulting from exposure to hazards. HHAs incorporate the identification, assessment, characterization, control, and communication of hazards in the workplace or environment. Following this systems approach, evaluations should consider the total health impact of all stressors contacting the human operator or maintainer. Whenever possible, HHAs should consider the synergistic effects of all agents present. An HHA shall also evaluate the hazards and costs due to system component materials, evaluate alternative materials for those components, and recommend materials that reduce the associated risk. Materials will be evaluated if (because of their physical, chemical, or biological characteristics; quantity; or concentrations) they cause or contribute to adverse effects in organisms or offspring or pose substantial present or future danger to the environment. The analysis shall include consideration of the generation of wastes and by-products.

207.2.1 A health hazard is a condition, inherent to the operation, maintenance, storage, transport, use of materiel, or disposal, that can cause death, injury, acute or chronic illness, disability, or reduced job performance of personnel by exposure to physiological stresses. Specific health hazards and impacts that shall be considered include:

a. Chemical hazards (e.g., materials that irritate or are hazardous because of physical properties such as flammability, toxicity, carcinogenicity, or propensity to deprive an organism of oxygen).

b. Physical hazards (e.g., acoustical energy, vibration, acceleration/deceleration, barostress, heat or cold stress, finished materials, and shrapnel).

c. Biological hazards (e.g., bacteria, viruses, fungi, and mold)

d. Ergonomic hazards (e.g., hazards that occur as a consequence of engaging in activities that impose excessive physical or cognitive demands, such as assuming non-neutral postures, sustaining harsh body contacts or load-bearing stress, performing taxing muscular exertions, sustaining long duration activity, etc.).

e. Other hazardous or potentially hazardous materials that may be formed by the test, maintenance, operation, or final disposal/recycling of the system.

f. Non-ionizing radiation hazards. Provide a listing of all non-ionizing (radio frequency (RF) and laser) transmitters contained in the system. List all parameters required to determine

Downloaded from http://www.everyspec.com

the non-ionizing radiation hazards of the system, including RF shock and burn hazards, RF hazard distances, laser eye and skin hazard distances, etc.

g. Ionizing radiation hazards. Provide a listing of all system ionizing radiation sources (including isotopes), quantities, activities, and hazards.

207.2.2 The HHA shall provide the following categories of information:

a. Hazard identification. Identify the hazardous agents by name(s), Chemical Abstract Service (CAS) number if available, and the affected system components and processes. Hazard identification also includes:

(1) Exposure pathway description. Describe the conditions and mode by which a hazardous agent can come in contact with a living organism. Include a description of the mode by which the agent is transmitted to the organism (e.g., ingestion, inhalation, absorption, or other mode of contact), as well as evidence of environmental fate and transport. Consider components of the system which may come into contact with users.

(2) Exposure characterization. Characterize exposures by providing measurements or estimates of energy intensities or substance quantities and concentrations. Provide either a description of the assessment process or the name of the assessment tool or model used. For material hazards, estimate the expected use rate of each hazardous material for each process or component for the subsystem, total system, and program-wide impact. Consider bio-availability and biological uptake if applicable.

b. Severity and probability. Estimate severity, probability, and Risk Assessment Code (RAC) using the process described in Section 4 of this Standard. The definitions in Tables I and II, and the RACs in Table III shall be used, unless tailored alternative definitions and/or a tailored matrix are formally approved in accordance with Department of Defense (DoD) Component policy. As appropriate for each hazard, describe the potential acute and chronic health risks (e.g., carcinogenicity, flammability, and reactivity).

c. Mitigation Strategy. Recommend a mitigation strategy for each hazard. Assign a target risk assessment code for each hazard based on the degree of risk reduction achievable by the mitigation.

207.2.3 In addition to the information required in 207.2.2 above, the following sections describe the HHA or part of the HHA that provides Hazardous Material (HAZMAT) evaluation, ergonomics evaluation, or describes the operational environment.

207.2.3.1 The HHA or part of the HHA providing HAZMAT evaluation, in addition to the information required in 207.2.2 above, shall:

a. Identify the HAZMAT by quantity, characteristics, and concentrations of the materials in the system. Identify source documents, such as Material Safety Data Sheets (MSDSs), and information from vendors and subvendors for components of systems and subsystems. At a

Downloaded from http://www.everyspec.com

minimum, if available, material identification includes material identity, common or trade names, chemical name, CAS number, national stock number (NSN), local stock number, physical state, and manufacturer and supplier names and contact information (including information from the Department of Defense HAZMAT information resource system).

b. Characterize material hazards, including hazardous waste, and determine associated risks. Examine acute health, chronic health, carcinogenic, contact, flammability, reactivity, and environmental hazards.

c. Describe how the HAZMAT is used for each process or component for the subsystem and total system.

d. Estimate the usage rate of each HAZMAT for each process or component for the subsystem, total system, and program-wide impact.

e. Recommend the disposition for each HAZMAT (to include hazardous waste) identified. Material substitution or altered processes shall be considered to reduce risks associated with the material hazards while evaluating the impact on program costs.

207.2.3.2 In addition to the information required in 207.2.2 above, the HHA or part of the HHA providing ergonomics evaluation shall:

a. Describe the purpose of the system and the mission scenarios in which the system will be used. This description should include all performance criteria established by the customer. If known, include manpower estimates that the customer anticipates will be allocated toward operating and maintaining the system. Also describe:

(1) Physical properties of all system components that personnel will manually handle or wear, and that will support personnel body weight (such as seating and bedding).

(2) A task analysis that lists the physical and cognitive actions that operators will perform during typical operations and routine maintenance.

(3) Exposures to mechanical stress encountered while performing work tasks.

b. Identify characteristics in the design of the system or work processes that could degrade performance or increase the likelihood of erroneous actions that may result in mishaps.

c. Determine manpower requirements to operate and maintain the system from the sum of the physical and cognitive demands imposed on personnel. Recommend a strategy to reduce these demands through equipment or job redesign if the determined requirements exceed the projected manpower allocation. Such recommendations may also be considered where they provide significant manpower or cost savings. Recommend methodologies to further optimize system design and control exposures to mechanical stress from load bearing, manual handling, and other physical activities through appropriate engineering and administrative controls that may include reducing load and force requirements, adding material handling aids or tools,

Downloaded from http://www.everyspec.com

reducing non-neutral postures, reducing frequency of repeated motion, increasing the manpower allocation, or redistributing tasks among personnel manning the system.

207.2.3.3 The HHA or part of the HHA providing the information required in 207.2.1 shall describe the operational environment, including how the equipment or system(s) will be used and maintained and the location in which it will be operated and maintained. Identify acoustic noise, vibration, acceleration, shock, blast, and impact force levels and related human exposures associated with comparable legacy systems, including personnel operating and maintaining these systems and exposures/levels in the surrounding (external) environment, particularly where exposures exceeding regulatory or recommended exposure standards have been documented or can reasonably be anticipated.

a. Assess and describe anticipated whole body movement, including whole body vibration, vehicle shock, and motions that are likely to result in musculoskeletal disorders, disorientation, or motion sickness. This information may be provided through a description of operating parameters, such as speed and vehicle loading; environment of operation and external influences, such as waves for marine vehicles; terrain conditions for land vehicles; and the position and seating characteristics of occupants.

b. Describe and quantify the potential for blast overpressure and other sudden barotrauma and the estimated pressure changes, time and rate of onset, and frequency of occurrence.

c. Identify and categorize main noise and vibration sources in the new or modified system(s). Include:

(1) The type of equipment and exposures associated with its operation in related systems. Where available or readily computed, the sound power level of relevant equipment shall be determined

(2) Octave band analysis and identification of predominant frequencies of operation.

(3) Impulse, impact, and steady-state noise sources, including anticipated intensity (dB) scale, periodicity/frequency of occurrence, and design and operational factors that may influence personnel and weapon system exposures.

d. Calculate estimated noise, blast, and vibration levels prior to final design and measurement of noise, blast, and vibration levels after construction of prototypes or initial demonstration models. If the calculated levels exceed exposure limits per Military Standard (MIL-STD)-1474 or Department of Defense (DoD) Component-specific standards, perform evaluations to include frequency analysis and estimated noise exposures to steady state and impulse noise. Describe, via calculation, the estimated resonant frequencies for occupants in seating and the effect of whole body vibration. These frequencies should be compared to known guidelines (e.g., MIL-STD-1472, International Organization for Standardization (ISO) 2631-1, ISO 2631-2, and ISO 2631-5) for whole body vibration with reference to degree of movement, frequency, and anticipated duration of exposures. Where feasible, anticipated target organ

Downloaded from http://www.everyspec.com

systems (e.g., back, kidneys, hands, arms, and head) should be identified and the likelihood of discordant motions should be described. Identify potential alternative processes and equipment that could reduce the adverse impacts.

e. Describe the anticipated effect of protective equipment and engineering changes, if required, for mitigating personnel exposures to noise and vibration, as well as the projected total number of individuals per platform and the total population exposed during the anticipated life of the system. Describe advanced hearing protective devices using active noise cancellation with regard to frequency and scale of noise attenuation and any frequency "trade-offs" in attenuation achieved. Use of protective equipment shall describe the optimal (design) and anticipated effective noise reduction and vibration reduction of the protective equipment. Document the methodology and assumptions made in calculations.

f. Describe the limitations of protective equipment and the burden imposed with regard to weight, comfort, visibility, and ranges of population accommodated, and quantify these parameters where feasible. Describe conformance to relevant design and performance standards for protective equipment.

207.2.3.4. The HHA or part of the HHA providing non-ionizing radiation evaluation, in addition to the information required in 207.2 above, shall refer to MIL-STD-464, MIL-STD-1425, and Military Handbook (MIL-HDBK)-454 for further guidance and clarification on associated tasks. Ionizing and non-ionizing radiation should be evaluated in accordance with DoD Military Standards consistent with Department of Defense Instruction (DoDI) 6055.11, Protection of DoD Personnel from Electromagnetic Fields and DoDI 6055.15, DoD Laser Protection Program.

207.2.4 Include a list of source materials used in conducting the analysis. It may include Government and contractor reports, standards, criteria, technical manuals, and specifications.

207.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 207 and identification of related tasks in the SOW or other contract requirements. (R)

b. Selected hazards, hazardous areas, hazardous materials, or other specific items to be examined or excluded.

c. Desired analysis methodologies and technique(s) and any special data elements, format, or data reporting requirements (consider Task 106, Hazard Tracking System).

d. Sources of information that will be made available and should be utilized. For example, DoD Service-specific HAZMAT policies may apply for in-Service maintenance, testing, and disposal.

e. Standards and criteria for acceptable exposures and controls.

Downloaded from http://www.everyspec.com

f. A list of mandatory references, including specific issue dates. The following list of references represents a starting point for information to support this task, but is not intended to be comprehensive.

(1) 29 Code of Federal Regulations (CFR) 1910, U.S. Department of Labor, Occupational Safety and Health Administration (OSHA), General Industry Regulations.

(2) 29 CFR 1910.1200, OSHA Hazard Communication.

(3) DODI 6055.12, DoD Hearing Conservation Program.

(4) DoD Handbook 743, Anthropometry of U.S. Military Personnel (Metric).

(5) MIL-STD-464, Electromagnetic Environmental Effects Requirements for Systems.

(6) MIL-STD-1425, Safety Design Requirements for Military Lasers and Associated Support Equipment.

(7) MIL-STD-1472, DoD Design Criteria Standard for Human Engineering.

(8) MIL-STD-1474, DoD Design Criteria Limit Noise Limits.

(9) MIL-HDBK-454, General Guidelines for Electronic Equipment.

(10) MIL-HDBK-1908, Definitions of Human Factors Terms.

(11) MIL-STD-46855, Human Engineering Requirements for Military Systems, Equipment, and Facilities.

(12) U.S. Army Health Hazard Assessors Guide, U.S. Army Center for Health Promotion and Preventive Medicine.

(13) U.S. Army Manpower and Personnel Integration (MANPRINT) Program.

(14) U.S. Army Regulation 40-10, Health Hazard Assessment Program in Support of the Army Acquisition Process.

(15) Department of the Army Pamphlet 40-501, Hearing Conservation Program.

(16) Navy and Marine Corps (NAVMC) Directive 5100.8, Marine Corps Occupational Safety and Health (OSH) Program Manual

(17) NAVMC Public Health Center Technical Manual 6260.51.99-2.

Downloaded from http://www.everyspec.com

(18) Navy Bureau of Medicine and Surgery Instruction 6270.8A, Obtaining Health Hazard Assessments.

(19) Marine Corps Order 6260.1E, Marine Corps Hearing Conservation Program.

(20) U.S. Air Force Manual 48-153, Health Risk Assessment.

(21) Air Force Occupational Safety and Health (AFOSH) STD 48-9, Radio Frequency Radiation (RFR) Safety Program.

(22) AFOSH STD 91-501, Air Force Consolidated Occupational Safety Standard.

(23) General Services Administration Federal Standard 313, Material Safety Data, Transportation Data, and Disposal Data for Hazardous Materials Furnished to Government Activities.

(24) ISO 2631-1:1997, Mechanical Vibration and Shock – Evaluation of Human Exposure to Whole Body Vibration and Shock. Part 1: General Requirements.

(25) ISO 2631-2, Mechanical Vibration and Shock – Evaluation of Human Exposure to Whole Body Vibration. Part 2: Vibration in Buildings (1 Hz to 80 Hz).

(26) ISO 2631-5, Mechanical Vibration and Shock – Evaluation of Human Exposure to Whole Body Vibration and Shock. Part 5: Method for Evaluation of Vibration Containing Multiple Shocks.

(27) ISO 5349, Guide for the Measurement and the Assessment of Human Exposure to Hand Transmitted Vibration.

(28) American National Standards Institute (ANSI) S2.70, Guide for Measurement and Evaluation of Human Exposure to Vibration Transmitted to the Hand.

(29) Institute of Electrical and Electronics Engineers (IEEE) Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 KHz to 300 GHz, IEEE Standards Coordinating Committee on Non-Ionizing Radiation Hazards.

(30) Threshold Limit Values for Chemical Substances and Physical Agents and Biological Exposure Indices, American Conference of Governmental Industrial Hygienists.

(31) American Society for Testing and Materials (ASTM) E2552 - Standard Guide for Assessing the Environmental and Human Health Impacts of New Energetic Compounds.

g. Concept of operations.

Downloaded from http://www.everyspec.com

h. Projected manpower allocation in support of 207.2.3.2.

i. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.

Downloaded from http://www.everyspec.com

TASK 208
FUNCTIONAL HAZARD ANALYSIS

208.1 Purpose. Task 208 is to perform and document a Functional Hazard Analysis (FHA) of an individual system or subsystem(s). The FHA is primarily used to identify and classify the system functions and the safety consequences of functional failure or malfunction, i.e. hazards. These consequences will be classified in terms of severity for the purpose of identifying the safety-critical functions (SCFs), safety-critical item (SCIs), safety-related functions (SRFs), and safety-related items (SRIs) of the system. SCFs, SCIs, SRFs, and SRIs will be allocated or mapped to the system design architecture in terms of hardware, software, and human interfaces to the system. The FHA is also used to identify environmental and health related consequences of functional failure or malfunction. The initial FHA should be accomplished as early as possible in the Systems Engineering (SE) process to enable the engineer to quickly account for the physical and functional elements of the system for hazard analysis purposes; identify and document SCFs, SCIs, SRFs, and SRIs; allocate and partition SCFs and SRFs in the software design architecture; and identify requirements and constraints to the design team.

208.2 Task description. The contractor shall perform and document a FHA to analyze functions associated with the proposed design. The FHA should be based on the best available data, including mishap data (if obtainable) from similar systems and other lessons learned. This effort will include inputs, outputs, critical interfaces, and the consequence of functional failure.

208.2.1 At a minimum, the FHA shall consider the following to identify and evaluate functions within a system:

a. Decomposition of the system and its related subsystems to the major component level.

b. A functional description of each subsystem and component identified.

c. A functional description of interfaces between subsystems and components. Interfaces should be assessed in terms of connectivity and functional inputs and outputs.

d. Hazards associated with loss of function, degraded function or malfunction, or functioning out of time or out of sequence for the subsystems, components, and interfaces. The list of hazards should consider the next effect in a possible mishap sequence and the final mishap outcome.

e. An assessment of the risk associated with each identified failure of a function, subsystem, or component. Estimate severity, probability, and Risk Assessment Code (RAC) using the process described in Section 4 of this Standard. The definitions in Tables I and II, and the RACs in Table III shall be used, unless tailored alternative definitions and/or a tailored matrix are formally approved in accordance with Department of Defense (DoD) Component policy.

f. An assessment of whether the functions identified are to be implemented in the design hardware, software, or human control interfaces. This assessment should map the functions to

Downloaded from http://www.everyspec.com

their implementing hardware or software components. Functions allocated to software should be mapped to the lowest level of technical design or configuration item prior to coding (e.g., implementing modules or use cases).

g. An assessment of Software Control Category (SCC) for each Safety-significant Software Function (SSSF). Assign a Software Criticality Index (SwCI) for each SSSF mapped to the software design architecture.

h. A list of requirements and constraints (to be included in the specifications) that, when successfully implemented, will eliminate the hazard or reduce the risk. These requirements could be in the form of fault tolerance, detection, isolation, annunciation, or recovery.

208.2.2 The contractor shall update the FHA following system design or operational changes as necessary.

208.2.3 The contractor shall document results of the analysis to include the following:

a. System description. This summary describes the physical and functional characteristics of the system and its subsystems. Reference to more detailed system and subsystem descriptions, including specifications and detailed review documentation, shall be supplied when such documentation is available.

b. Hazard analysis methods and techniques. Provide a description of each method and technique used in conduct of the analysis. Include a description of assumptions made for each analysis and the qualitative or quantitative data used.

c. Hazard analysis results. Contents and formats may vary according to the individual requirements of the program and methods and techniques used. As applicable, analysis results should be captured in the Hazard Tracking System (HTS).

208.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 208. (R)

b. Identification of functional discipline(s) to be addressed by this task. (R)

c. Desired analysis methodologies and technique(s) and any special data elements, format, or data reporting requirements (consider Task 106, Hazard Tracking System).

d. Applicable requirements, specifications, and standards.

Downloaded from http://www.everyspec.com

e. Concept of operations.

f. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.

Downloaded from http://www.everyspec.com

TASK 209
SYSTEM-OF-SYSTEMS HAZARD ANALYSIS

209.1 Purpose. Task 209 is to perform and document an analysis of the System-of-Systems (SoS) to identify unique SoS hazards. This task will produce special requirements to eliminate or mitigate identified unique SoS hazards which otherwise would not exist.

209.2 Task description. The contractor shall perform and document an analysis of the SoS to identify unique SoS hazards and mitigation requirements. The human shall be considered an element of the SoS, receiving both inputs and initiating outputs within the analysis.

209.2.1 The contractor will provide traceability of all identified unique SoS hazards to architecture locations, interfaces, data, and the stakeholder(s) associated with each hazard.

209.2.2 The contractor will assess the risk of identified unique SoS hazard(s) and recommend mitigation measures to eliminate the hazards or reduce the associated risks when the hazards cannot be eliminated. The definitions in Tables I and II, and the Risk Assessment Codes (RACs) in Table III shall be used, unless tailored alternative definitions and/or a tailored matrix are formally approved in accordance with Department of Defense (DoD) Component policy.

209.2.3 The contractor will verify and validate the effectiveness of recommended mitigation measures.

209.2.4 The contractor shall document results of the analysis to include the following:

a. SoS description. This summary describes the physical and functional characteristics of the SoS. Reference to more detailed individual system descriptions, including specifications and detailed review documentation, shall be supplied when such documentation is available.

b. Hazard analysis methods and techniques. Provide a description of each method and technique used in conduct of the analysis. Include a description of assumptions made for each analysis and the qualitative or quantitative data used.

c. Hazard analysis results. Contents and formats may vary according to the individual requirements of the program and methods and techniques used. As applicable, analysis results should be captured in the Hazard Tracking System (HTS).

209.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 209. (R)

b. Identification of functional discipline(s) to be addressed by this task. (R)

c. Identify architectures and systems, which comprise the SoS. (R)

Downloaded from http://www.everyspec.com

d. Concept of operations.

e. Include probable location(s) and distance(s) of the systems within the SoS.

f. Desired analysis methodologies and technique(s) and any special data elements, format, or data reporting requirements (consider Task 106, Hazard Tracking System).

g. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.

Downloaded from http://www.everyspec.com

TASK 210
ENVIRONMENTAL HAZARD ANALYSIS

210.1 Purpose. Task 210 is to perform and document an Environmental Hazard Analysis (EHA) to support design development decisions. The EHA will identify hazards to the environment throughout all life-cycle phases and modes; document the hazards in the Hazard Tracking System (HTS); manage the hazards using the system safety process described in Section 4; and provide the system-specific data to support National Environmental Policy Act (NEPA) and Executive Order (EO) 12114 requirements.

210.2 Task description. The contractor shall perform and document an EHA in order to influence design decisions by integrating environmental considerations into the Systems Engineering (SE) process. The contractor should start the EHA process as early as possible consistent with initiation of the overall SE process. The contractor will continue to identify and manage environmental hazards using the system safety process described in Section 4 throughout the duration of the task.

210.2.1 Starting the EHA as part of the early SE processes is typically the most cost-effective means of minimizing environmental impacts from the operations and support of a new or modified system. Conversely, early design decisions made without consideration of environmental requirements may result in environmental impacts that cannot be easily designed out and will require mitigation later in the acquisition process. These issues could potentially result in mission and operational constraints and compliance burdens for receiving installations, test, launch, and training ranges, depot maintenance installations, and operational training units.

a. The elimination of hazards or reduction of associated risks with an informed and structured risk assessment and acceptance process is essential. Early identification and introduction of environmental hazards into the SE process provides decision makers with a more complete and relevant picture of the potential risks during all life-cycle phases and modes, and will help mitigate the risk.

b. The definitions in Tables I and II, and the Risk Assessment Codes (RACs) in Table III shall be used, unless tailored alternative definitions and/or a tailored matrix are formally approved in accordance with Department of Defense (DoD) Component policy.

210.2.2 The system safety process, through the SE process, shall be used to identify and assess hazards and make recommendations for hazard elimination and risk reduction. When assessing hazards that may impact the environment, the eight-element system safety process in Section 4 of this Standard shall be followed.

a. The scope of the EHA should consider the entire system life-cycle and address hazards associated with, but not limited to:

(1) Hazardous materials use and generation.

(2) Demilitarization and disposal requirements.

Downloaded from http://www.everyspec.com

(3) Exposure to chemical, biological, and other hazards impacting public health.

(4) Noise generation resulting from operation of the system.

(5) Pollutant emissions generation (e.g., air, water, and solid waste).

(6) Release of hazardous substances incidental to the routine maintenance and operation of the system.

(7) Inadvertent hazardous releases.

(8) Environmental impacts on sea, air, space, and land resources and ecosystems.

b. Programs shall begin the process of identifying environmental requirements and hazards using sources such as:

(1) Environmental hazard analysis data and information, risk assessments, mishaps, and lessons learned from legacy and similar systems.

(2) Early acquisition activities (e.g., Analysis of Alternatives and Technology Development Strategy).

(3) User requirements documents (e.g., Joint Capabilities Integration and Development System, Concept of Operations, etc.).

(4) System design data and information (e.g., design specifications).

(5) Demilitarization and disposal of legacy and similar systems.

(6) Environmental issues at legacy and similar system locations and potential locations throughout the life-cycle.

(7) Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE) and NEPA documents from legacy and similar systems.

(8) Preliminary Hazard List (PHL)/Preliminary Hazard Analysis (PHA) for the system under development.

(9) Life-cycle Sustainment Plan(s) for legacy or similar systems.

c. When determining environmental mitigation measures, the analysis should consider the impact of mitigations on safety and health, as well as other applicable SE design considerations.

210.2.3 The contractor shall document results of the analysis to include the following:

Downloaded from http://www.everyspec.com

a. System description. This summary describes the physical and functional characteristics of the system and its subsystems. Reference to more detailed system and subsystem descriptions, including specifications and detailed review documentation, shall be supplied when such documentation is available.

b. Hazard analysis methods and techniques. Provide a description of each method and technique used in conduct of the analysis. Include a description of assumptions made for each analysis and the qualitative or quantitative data used.

c. Hazard analysis results. Contents and formats may vary according to the individual requirements of the program and methods and techniques used. As applicable, analysis results should be captured in the HTS.

210.2.4 If hazards are associated with Hazardous Materials (HAZMAT), the following minimum data elements will be tracked and reported:

a. HAZMAT item or substance name.

b. HAZMAT Category (prohibited, restricted, or tracked).

c. Special Material Content Code (SMCC) as designated in DoD 4100.39-M, Volume 10.

d. Location of HAZMAT within the system.

e. Quantity of HAZMAT within the system with traceability to version specific hardware designs.

f. Application, process, or activity whereby quantities of HAZMAT are embedded in the system, or used during operations, and support of the system.

g. Reasonably anticipated HAZMAT (whether categorized or not categorized) generated during the system's life-cycle (e.g., installation, Government test and evaluation, normal use, and maintenance or repair of the system).

h. Reasonably anticipated HAZMAT (whether categorized or not categorized) generated during mishaps.

i. Special HAZMAT control, training, handling measures, and Personal Protective Equipment (PPE) needed, including provision of required Material Safety Data Sheets (MSDSs).

210.2.5 If hazards are associated with pollutant (including noise) generation, the following additional data elements should be included in the HTS:

a. Identification of the specific pollutants associated with system operations and maintenance activities.

Downloaded from http://www.everyspec.com

b. Sources of emission for each pollutant.

c. Quantity and magnitude or rate of pollution generated during normal operation and maintenance as specified by the program office.

d. Special emission control, training, handling measures, and personal protective equipment needed.

210.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 210. (R)

b. Minimum reporting requirements. (R)

c. Desired analysis methodologies and technique(s) and any special data elements, format, or data reporting requirements (consider Task 106, Hazard Tracking System).

d. Legacy and related systems and equipment to be reviewed.

e. Geographic locations to consider when assessing environmental mishap severity and regulatory compliance considerations.

f. Concept of operations.

g. Any specialized NEPA/EO 12114 proponent support tasks.

h. The current planned system life-cycle for projecting HAZMAT usage or generation if applicable.

i. HAZMAT management limitations, exceptions, exemptions, or thresholds if applicable.

j. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.

Downloaded from http://www.everyspec.com

TASK SECTION 300 - EVALUATION

Downloaded from http://www.everyspec.com

TASK 301
SAFETY ASSESSMENT REPORT

301.1 Purpose. Task 301 is to perform and document a Safety Assessment Report (SAR) to provide a comprehensive evaluation of the status of safety hazards and their associated risks prior to test or operation of a system, before the next contract phase, or at contract completion.

301.2 Task description. The contractor shall perform and document an assessment to identify the status, at the time of the report, of safety hazards, associated risks, mitigation measures, and formal risk acceptance decisions. This documentation shall include hazards that were identified and eliminated, and specific procedural controls and precautions to be followed to mitigate the risks of hazards that could not be eliminated. The contractor shall prepare a report that contains the following information:

a. The specific risk matrix used to classify hazards. The definitions in Tables I and II, and the Risk Assessment Codes (RACs) in Table III shall be used, unless tailored alternative definitions and/or a tailored matrix are formally approved in accordance with Department of Defense (DoD) Component policy.

b. The results of analyses and tests performed to identify hazards, assess risks, and verify/validate effectiveness of mitigation measures.

c. Hazard Tracking System (HTS) data.

d. A summary of risks for each identified hazard.

e. Any Hazardous Material (HAZMAT) contained within the system or required for the operations and support of the system.

f. Test or other event-unique mitigation measures necessary to reduce risks.

g. Recommendations applicable to hazards located at the interface of the system with other systems.

h. Based on the scope of the report, a summary statement addressing the system's readiness to test, operate, or proceed to the next acquisition phase.

i. List all pertinent references, including (but not limited to) test and analysis reports, standards and regulations, specifications and requirements documents, operating manuals, and maintenance manuals.

301.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 301. (R)

Downloaded from http://www.everyspec.com

b. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.

c. Procedures for communicating formal Governmental risk acceptance to the contractor.

d. Desired analysis methodologies and technique(s) and any special data elements, format, or data reporting requirements (consider Task 106, Hazard Tracking System).

e. The specific scope of the requested assessment report (e.g., test or operation of a system, life-cycle phase, or contract completion).

Downloaded from http://www.everyspec.com

TASK 302
HAZARD MANAGEMENT ASSESSMENT REPORT

302.1 Purpose. Task 302 is to perform and document a Hazard Management Assessment Report (HMAR) to provide a comprehensive evaluation of the status of hazards and their associated risks prior to test or operation of a system, before the next contract phase, or at contract completion.

302.2 Task description. The contractor shall perform and document an assessment to identify the status, at the time of the report, of hazards, associated risks, mitigation measures, and formal risk acceptance decisions. This documentation shall include hazards that were identified and eliminated and specific procedural controls and precautions to be followed to mitigate the risks of hazards that could not be eliminated. The contractor shall prepare a report that contains the following information:

a. The specific risk matrix used to classify hazards. The definitions in Tables I and II, and the Risk Assessment Codes (RACs) in Table III shall be used, unless tailored alternative definitions and/or a tailored matrix are formally approved in accordance with Department of Defense (DoD) Component policy.

b. The results of analyses and tests performed to identify hazards, assess risks, and verify/validate effectiveness of mitigation measures.

c. Hazard Tracking System (HTS) data.

d. A summary of risks for each identified hazard.

e. Any Hazardous Material (HAZMAT) contained within the system or required for the operations and support of the system, including:

(1) Identification of material type, quantity, and hazards.

(2) Precautions and procedures necessary during use, packaging, handling, storage, transportation, and disposal. Include all explosives hazard classifications and Explosive Ordnance Disposal (EOD) requirements.

(3) Assessments of why less hazardous materials could not be used.

f. Test or other event-unique mitigation measures necessary to reduce risks.

g. Recommendations applicable to hazards located at the interface of the system with other systems.

h. Based on the scope of the report, a summary statement addressing the system’s readiness to test, operate, or proceed to the next acquisition phase.

Downloaded from http://www.everyspec.com

i. List all pertinent references, including (but not limited to) test and analysis reports, standards and regulations, specifications and requirements documents, operating manuals, and maintenance manuals.

302.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 302. (R)

b. Identification of functional discipline(s) to be addressed by this task. (R)

c. Procedures for communicating formal Governmental risk acceptance to the contractor.

d. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.

e. Desired analysis methodologies and technique(s) and any special data elements, format, or data reporting requirements (consider Task 106, Hazard Tracking System).

f. The specific scope of the requested assessment report (e.g., test or operation of a system, life-cycle phase, or contract completion).

Downloaded from http://www.everyspec.com

TASK 303
TEST AND EVALUATION PARTICIPATION

303.1 Purpose. Task 303 is to participate in the Test and Evaluation (T&E) process to evaluate the system, verify and validate risk mitigation measures, and to manage risks for test events.

303.2 Task description. The contractor shall participate in T&E planning, support the preparation of test event Safety Releases, conduct post-test event actions, and maintain a repository of reports. The objective is to eliminate the hazards or reduce the associated risks when the hazards cannot be eliminated for both the system and the test events.

303.2.1 T&E planning shall include, at a minimum, the following:

a. Participation in the preparation and updating of the T&E Strategy (TES) and the T&E Master Plan (TEMP) to include hazard considerations and identification of when hazard analyses, risk assessments, and risk acceptances shall be completed in order to support T&E schedules.

b. Participation in the development of test plans and procedures to include hazard considerations that support:

(1) Identification of mitigation measures to be verified and validated during a given test event with recommended evaluation criteria.

(2) Identification of known system hazards present in a given test event, recommended test-unique mitigations, and test event risks.

(3) Preparation of the Safety Release.

(4) Analysis of hazards associated with test equipment and procedures.

(5) Government completion of applicable environmental analysis and documentation pursuant to DoD Service-specific National Environmental Policy Act (NEPA) and Executive Order (EO) 12114 requirements in test and evaluation planning schedules.

(6) Documentation of procedures for advising operators, maintainers and testers involved in the test event of known hazards, their associated risks, test-unique mitigation measures, and risk acceptance status.

303.2.2 Conduct the following post-test event actions.

a. Analyze test results to assess effectiveness of mitigation measures as tested.

b. Analyze test results to identify and assess new system hazards and to potentially update risk assessments for known hazards.

Downloaded from http://www.everyspec.com

c. Analyze incident, discrepancy, and mishap reports generated during test events for information on hazards and mitigation measures. Ensure mitigation measures are incorporated in future test plans as appropriate.

d. Document new or updated system related hazard information in the Hazard Tracking System (HTS) as appropriate.

303.2.3 Maintain a repository of T&E results. Provide Government access to the repository. Provide the Government with this repository at the end of the contract. The repository shall include the following:

a. Hazards identified during test events.

b. Verification and validation of mitigation measures.

c. Incident, discrepancy, and mishap reports generated during test events with information on corrective actions.

303.3. Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 303. (R)

b. Identification of functional discipline(s) to be addressed by this task. (R)

c. Procedures for communicating formal Governmental risk acceptance to the contractor.

d. Any special data elements, format, or data reporting requirements (consider Task 106, Hazard Tracking System).

e. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.

Downloaded from http://www.everyspec.com

TASK 304
REVIEW OF ENGINEERING CHANGE PROPOSALS, CHANGE NOTICES, DEFICIENCY REPORTS, MISHAPS, AND REQUESTS FOR DEVIATION/WAIVER

304.1 Purpose. Task 304 is to perform and document the application of the system safety process described in Section 4 of this Standard to Engineering Change Proposals (ECPs); change notices; deficiency reports; mishaps; and requests for deviations, waivers and related change documentation.

304.2 Task description. The contractor shall perform and document the application of the system safety process described in Section 4 of this Standard to:

a. Each ECP and change notice (temporary or permanent) to identify new hazards or hazards potentially modified by the ECP or change notice (temporary or permanent), assess the associated risk(s), and determine if new or existing hazards could be eliminated or when the hazards cannot be eliminated, the associated risks reduced through the ECP or change notice (temporary or permanent) under review.

b. Each hardware or software deficiency report to identify potential new hazards or modifications to existing risk levels.

c. System-related mishaps (as specified in 304.3.c) to provide analysis of hazards that contributed to the mishap and recommendations for materiel risk mitigation measures, especially those that minimize human errors.

d. Review mishaps from similar systems to refine risk assessments and identify hazards.

e. Each request for deviation or waiver to identify and assess hazards that may result.

f. Document the results of the task in the Hazard Tracking System (HTS) as appropriate.

304.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 304. (R)

b. Identification of functional discipline(s) to be addressed by this task. (R)

c. Guidance for contractor participation and access to mishap investigations, including procedures for obtaining investigation data and any requirements for protection of privileged safety data from unauthorized disclosure. (R)

d. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.

Downloaded from http://www.everyspec.com

TASK SECTION 400 - VERIFICATION

Downloaded from http://www.everyspec.com

TASK 401
SAFETY VERIFICATION

401.1 Purpose. Task 401 is to define and perform tests and demonstrations or use other verification methods on safety-significant hardware, software, and procedures to verify compliance with safety requirements.

401.2 Task description. The contractor shall define and perform analyses, tests, and demonstrations; develop models; and otherwise verify the compliance of the system with safety requirements on safety-significant hardware, software, and procedures (e.g., safety verification of iterative software builds, prototype systems, subsystems, and components). Induced or simulated failures shall be considered to demonstrate the acceptable safety performance of the equipment and software.

401.2.1 When analysis or inspection cannot determine the adequacy of risk mitigation measures, tests shall be specified and conducted to evaluate the overall effectiveness of the mitigation measures. Specific safety tests shall be integrated into appropriate system Test and Evaluation (T&E) plans, including verification and validation plans.

401.2.2 Where safety tests are not feasible, the contractor shall recommend verification of compliance using engineering analyses, analogies, laboratory tests, functional mockups, or models and simulations.

401.2.3 Review plans, procedures, and the results of tests and inspections to verify compliance with safety requirements.

401.2.4 The contractor shall document safety verification results and submit a report that includes the following:

a. Test procedures conducted to verify or demonstrate compliance with the safety requirements on safety-significant hardware, software, and procedures.

b. Results from engineering analyses, analogies, laboratory tests, functional mockups, or models and simulations used.

c. T&E reports that contain the results of the safety evaluations, with a summary of the results provided.

401.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 401 (R)

b. Identification of functional discipline(s) to be addressed by this task. (R)

Downloaded from http://www.everyspec.com

c. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.

d. Any special data elements, format, or data reporting requirements (consider Task 106, Hazard Tracking System).

Downloaded from http://www.everyspec.com

TASK 402
EXPLOSIVES HAZARD CLASSIFICATION DATA

402.1 Purpose. Task 402 is to perform tests and analyses, develop data necessary to comply with hazard classification regulations, and prepare hazard classification approval documentation associated with the development or acquisition of new or modified explosives and packages or commodities containing explosives (including all energetics).

402.2 Task description. The contractor shall provide hazard classification data to support program compliance with the Department of Defense (DoD) Ammunition and Explosives Hazard Classification Procedures (DAEHCP) (Army Technical Bulletin 700-2, Naval Sea Systems Command Instruction 8020.8, Air Force Technical Order 11A-1-47, and Defense Logistics Agency Regulation 8220.1). Such pertinent data may include:

a. Narrative information to include functional descriptions, safety features, and similarities and differences to existing analogous explosive commodities, including packaging.

b. Technical data to include Department of Defense Identification Codes (DODICs) and National Stock Numbers (NSNs); part numbers; nomenclatures; lists of explosive compositions and their weights, whereabouts, and purposes; lists of other hazardous materials and their weights, volumes, and pressures; technical names; performance or product specifications; engineering drawings; and existing relevant Department of Transportation (DOT) classification of explosives approvals.

c. Storage and shipping configuration data to include packaging details.

d. Test plans.

e. Test reports.

f. Analyses.

402.3. Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 402. (R)

b. Hazard classification data requirements to support the Integrated Master Schedule. (R)

c. Hazard classification data from similar legacy systems.

d. Any special data elements or formatting requirements.

Downloaded from http://www.everyspec.com

TASK 403
EXPLOSIVE ORDNANCE DISPOSAL DATA

403.1 Purpose. Task 403 is to provide Explosive Ordnance Disposal (EOD) source data, recommended render-safe procedures, and disposal considerations. Task 403 also includes the provision of test items for use in new or modified weapons systems, explosive ordnance evaluations, aircraft systems, and unmanned systems.

403.2 Task description. The contractor shall:

a. Provide detailed source data on explosive ordnance design functioning and safety so that proper EOD tools, equipment, and procedures can be validated and verified.

b. Recommend courses of action that EOD personnel can take to render safe and dispose of explosive ordnance.

c. Provide test ordnance for conducting EOD validation and verification testing. The Naval Explosive Ordnance Disposal Technology Division will assist in establishing quantities and types of assets required.

d. Provide training aids for conducting EOD training. The Naval Explosive Ordnance Disposal Technology Division will assist in establishing quantities and types of training aids required.

403.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include, as applicable:

a. Imposition of Task 403. (R)

b. The number and types of test items for EOD validation and verification testing. The Naval Explosive Ordnance Disposal Technology Division will assist in establishing quantities and types of assets required.

c. The number and types of training aids for EOD training. The Naval Explosive Ordnance Disposal Technology Division will assist in establishing quantities and types of training aids required.

Downloaded from http://www.everyspec.com

GUIDANCE FOR THE SYSTEM SAFETY EFFORT

A.1 Scope. This Appendix is not a mandatory part of the standard. The information contained herein is intended for guidance only. This Appendix provides guidance on the selection of the optional tasks and use of quantitative probability levels.

A.2. Task Application. The system safety effort described in Section 4 of this Standard can be augmented by identifying specific tasks that may be necessary to ensure that the contractor adequately addresses areas that the Program needs to emphasize. Consideration should be given to the complexity and dollar value of the program and the expected levels of risks involved. Table A-I provides a list of the optional tasks and their applicability to program phases. Once recommendations for task applications have been determined, tasks can be prioritized and a "rough order of magnitude" estimate should be created for the time and effort required to complete each task. This information will be of considerable value in selecting the tasks that can be accomplished within schedule and funding constraints.

TABLE A-I. Task application matrix

			PROGRAM PHASE				
Task	**Title**	**Task Type**	**MSA**	**TD**	**EMD**	**P&D**	**O&S**
101	Hazard Identification and Mitigation Effort Using The System Safety Methodology	MGT	G	G	G	G	G
102	System Safety Program Plan	MGT	G	G	G	G	G
103	Hazard Management Plan	MGT	G	G	G	G	G
104	Support of Government Reviews/Audits	MGT	G	G	G	G	G
105	Integrated Product Team/Working Group Support	MGT	G	G	G	G	G
106	Hazard Tracking System	MGT	S	G	G	G	G
107	Hazard Management Progress Report	MGT	G	G	G	G	G
108	Hazardous Materials Management Plan	MGT	S	G	G	G	G
201	Preliminary Hazard List	ENG	G	S	S	GC	GC
202	Preliminary Hazard Analysis	ENG	S	G	S	GC	GC
203	System Requirements Hazard Analysis	ENG	G	G	G	GC	GC
204	Subsystem Hazard Analysis	ENG	N/A	G	G	GC	GC
205	System Hazard Analysis	ENG	N/A	G	G	GC	GC
206	Operating and Support Hazard Analysis	ENG	S	G	G	G	S
207	Health Hazard Analysis	ENG	S	G	G	GC	GC
208	Functional Hazard Analysis	ENG	S	G	G	GC	GC
209	System-Of-Systems Hazard Analysis	ENG	N/A	G	G	GC	GC
210	Environmental Hazard Analysis	ENG	S	G	G	G	GC
301	Safety Assessment Report	ENG	S	G	G	G	S
302	Hazard Management Assessment Report	ENG	S	G	G	G	S
303	Test and Evaluation Participation	ENG	G	G	G	G	S
304	Review of Engineering Change Proposals, Change Notices, Deficiency Reports, Mishaps, and Requests for Deviation/Waiver	ENG	N/A	S	G	G	G
401	Safety Verification	ENG	N/A	S	G	G	S
402	Explosives Hazard Classification Data	ENG	N/A	S	G	G	GC
403	Explosive Ordnance Disposal Data	ENG	N/A	S	G	G	S

Task Type
ENG – Engineering
MGT – Management

Program Phase
MSA – Materiel Solution Analysis
TD – Technology Development
EMD – Engineering and Manufacturing Development
P&D – Production and Deployment
O&S – Operations and Support

Applicability Codes
G – Generally Applicable
S – Selectively Applicable
GC – Generally Applicable to Design Change
N/A – Not Applicable

Downloaded from http://www.everyspec.com

A.3. Quantitative Probability Example. For quantitative descriptions, the frequency is the actual or expected number of mishaps (numerator) during a specified exposure (denominator). The denominator can be based on such things as the life of one item; number of missile firings, flight hours, systems fielded, or miles driven; years of service, etc.

TABLE A-II. Example probability levels

Probability Levels				
Description	**Level**	**Individual Item**	**Fleet/Inventory***	**Quantitative**
Frequent	**A**	Likely to occur often in the life of an item	Continuously experienced.	Probability of occurrence greater than or equal to 10^{-1}.
Probable	**B**	Will occur several times in the life of an item	Will occur frequently.	Probability of occurrence less than 10^{-1} but greater than or equal to 10^{-2}.
Occasional	**C**	Likely to occur sometime in the life of an item	Will occur several times.	Probability of occurrence less than 10^{-2} but greater than or equal to 10^{-3}.
Remote	**D**	Unlikely, but possible to occur in the life of an item	Unlikely but can reasonably be expected to occur.	Probability of occurrence less than 10^{-3} but greater than or equal to 10^{-6}.
Improbable	**E**	So unlikely, it can be assumed occurrence may not be experienced in the life of an item	Unlikely to occur, but possible.	Probability of occurrence less than 10^{-6}.
Eliminated	**F**	Incapable of occurrence within the life of an item. This category is used when potential hazards are identified and later eliminated.		

* The size of the fleet or inventory should be defined.

Downloaded from http://www.everyspec.com

SOFTWARE SYSTEM SAFETY ENGINEERING AND ANALYSIS

B.1 Scope. This Appendix is not a mandatory part of the standard. The information contained herein is intended for guidance only. This Appendix provides additional guidance on the software system safety engineering and analysis requirements in 4.4. For more detailed guidance, refer to the Joint Software Systems Safety Engineering Handbook and Allied Ordnance Publication (AOP) 52, Guidance on Software Safety Design and Assessment of Munition-Related Computing Systems.

B.2. Software system safety. A successful software system safety engineering activity is based on a hazard analysis process, a safety-significant software development process, and Level of Rigor (LOR) tasks. The safety-significant software development process and LOR tasks comprise the software system safety integrity process. Emphasis is placed on the context of the "system" and how software contributes to or mitigates failures, hazards, and mishaps. From the perspective of the system safety engineer and the hazard analysis process, software is considered as a subsystem. In most instances, the system safety engineers will perform the hazard analysis process in conjunction with the software development, software test, and Independent Verification and Validation (IV&V) team(s). These teams will implement the safety-significant software development and LOR tasks as a part of the overall Software Development Plan (SDP). The hazard analysis process identifies and mitigates the exact software contributors to hazards. The software system safety integrity process increases the confidence that the software will perform as specified to software system safety and performance requirements while reducing the number of contributors to hazards that may exist in the system. Both processes are essential in reducing the likelihood of software initiating a propagation pathway to a hazardous condition or mishap.

B.2.1 Software system safety hazard analysis. System safety engineers performing the hazard analysis for the system (Preliminary Hazard Analysis (PHA), Subsystem Hazard Analysis (SSHA), System Hazard Analysis (SHA), System-of-Systems (SoS) Hazard Analysis, Functional Hazard Analysis (FHA), Operating and Support Hazard Analysis (O&SHA), and Health Hazard Analysis (HHA)) will ensure that the software system safety engineering analysis tasks are performed. These tasks ensure that software is considered in its contribution to mishap occurrence for the system under analysis, as well as interfacing systems within an SoS architecture. In general, software functionality that directly or indirectly contributes to mishaps, such as the processing of safety-significant data or the transitioning of the system to a state that could lead directly to a mishap, should be thoroughly analyzed. Software sources and specific software errors that cause or contribute to hazards should be identified at the software module and functional level (functions out-of-time or out-of-sequence malfunctions, degrades in function, or does not respond appropriately to system stimuli). In software-intensive, safety-significant systems, mishap occurrence will likely be caused by a combination of hardware, software, and human errors. These complex initiation pathways should be analyzed and thoroughly tested to identify existing and/or derived mitigation requirements and constraints to the hardware and software design. As a part of the FHA (Task 208), identify software functionality which can cause, contribute to, or influence a safety-significant hazard. Software

Downloaded from http://www.everyspec.com

requirements that implement Safety-Significant Functions (SSFs) are also identified as safety-significant.

B.2.2 Software system safety integrity. Software developers and testers play a major role in producing safe software. Their contribution can be enhanced by incorporating software system safety processes and requirements within the SDP and task activities. The software system safety processes and requirements are based on the identification and establishment of specific software development and test tasks for each acquisition phase of the software development life-cycle (requirements, preliminary design, detailed design, code, unit test, unit integration test, system integration test, and formal qualification testing). All software system safety tasks will be performed at the required LOR, based on the safety criticality of the software functions within each software configuration item or software module of code. The software system safety tasks are derived by performing an FHA to identify SSFs, assigning a Software Control Category (SCC) to each of the safety-significant software functions, assigning an Software Criticality Index (SwCI) based on severity and SCC, and implementing LOR tasks for safety-significant software based on the SwCI. These software system safety tasks are further explained in subsequent paragraphs.

B.2.2.1 Perform a functional hazard analysis. The SSFs of the system should be identified. Once identified, each SSF is assessed and categorized against the SCCs to determine the level of control of the software over safety-significant functionality. Each SSF is mapped to its implementing computer software configuration item or module of code for traceability purposes.

B.2.2.2 Perform a software criticality assessment for each SSF. The software criticality assessment should not be confused with risk. Risk is a measure of the severity and probability of occurrence of a mishap from a particular hazard, whereas software criticality is used to determine how critical a specified software function is with respect to the safety of the system. The software criticality is determined by analyzing the SSF in relation to the system and determining the level of control the software exercises over functionality and contribution to mishaps and hazards. The software criticality assessment combines the severity category with the SCC to derive a SwCI as defined in Table V in 4.4.2 of this Standard. The SwCI is then used as part of the software system safety analysis process to define the LOR tasks which specify the amount of analysis and testing required to assess the software contributions to the system-level risk.

B.2.2.3 Software Safety Criticality Matrix (SSCM) tailoring. Tables IV through VI should be used, unless tailored alternative matrices are formally approved in accordance with Department of Defense (DoD) Component policy. However, tailoring should result in a SSCM that meets or exceeds the LOR tasks defined in Table V in 4.4.2 of this Standard. A SwCI 1 from the SSCM implies that the assessed software function or requirement is highly critical to the safety of the system and requires more design, analysis, and test rigor than software that is less critical prior to being assessed in the context of risk reduction. Software with SwCI 2 through SwCI 4 typically requires progressively less design, analysis, and test rigor than high-criticality software. Unlike the hardware-related risk index, a low index number does not imply that a design is unacceptable. Rather, it indicates a requirement to apply greater resources to the

Downloaded from http://www.everyspec.com

analysis and testing rigor of the software and its interaction with the system. The SSCM does not consider the likelihood of a software-caused mishap occurring in its initial assessment. However, through the successful implementation of a system and software system safety process and LOR tasks, the likelihood of software contributing to a mishap may be reduced.

B.2.2.4 Software system safety and requirements within software development processes. Once safety-significant software functions are identified, assessed against the SCC, and assigned a SwCI, the implementing software should be designed, coded, and tested against the approved SDP containing the software system safety requirements and LOR tasks. These criteria should be defined, negotiated, and documented in the SDP and the Software Test Plan (STP) early in the development life-cycle.

a. SwCI assignment. A SwCI should be assigned to each safety-significant software function and the associated safety-significant software requirements. Assigning the SwCI value of Not Safety to non-safety-significant software requirements provides a record that functionality has been assessed by software system safety engineering and deemed Not Safety. Individual safety-significant software requirements that track to the hazard reports will be assigned a SwCI. The intent of SwCI 4 is to ensure that requirements corresponding to this level are identified and tracked through the system. These “low” safety-significant requirements need only the defined safety-specific testing.

b. Task guidance. Guidance regarding tasks that can be placed in the SDP, STP, and safety program plans can be found in multiple references, including the Joint Software Systems Safety Engineering Handbook by the Joint Software Systems Safety Engineering Workgroup and AOP 52, Guidance on Software Safety Design and Assessment of Munition-Related Computing Systems. These tasks and others that may be identified should be based on each individual system or SoS and its complexity and safety criticality, as well as available resources, value added, and level of acceptable risk.

B.2.2.5. Software system safety requirements and tasks. Suggested software system safety requirements and tasks that can be applied to a program are listed in the following paragraphs for consideration and applicability:

a. Design requirements. Design requirements to consider include fault tolerant design, fault detection, fault isolation, fault annunciation, fault recovery, warnings, cautions, advisories, redundancy, independence, N-version design, functional partitioning (modules), physical partitioning (processors), design safety guidelines, generic software safety requirements, design safety standards, and best and common practices.

b. Process tasks. Process tasks to consider include design review, safety review, design walkthrough, code walkthrough, independent design review, independent code review, independent safety review, traceability of SSFs, SSFs code review, SSFs, Safety-Critical Function (SCF) code review, SCF design review, test case review, test procedure review, safety test result review, independent test results review, safety quality audit inspection, software quality assurance audit, and safety sign-off of reviews and documents.

Downloaded from http://www.everyspec.com

c. Test tasks. Test task considerations include SSF testing, functional thread testing, limited regression testing, 100 percent regression testing, failure modes and effects testing, out-of-bounds testing, safety-significant interface testing, Commercial-Off-the-Shelf (COTS), Government-Off-the-Shelf (GOTS), and Non-Developmental Item (NDI) input/output testing and verification, independent testing of prioritized SSFs, functional qualification testing, IV&V, and nuclear safety cross-check analysis.

d. Software system safety risk assessment. After completion of all specified software system safety engineering analysis, software development, and LOR tasks, results will be used as evidence (or input) to assign software's contribution to the risk associated with a mishap. System safety and software system safety engineering, along with the software development team (and possibly the independent verification team), will evaluate the results of all safety verification activities and will perform an assessment of confidence for each safety-significant requirement and function. This information will be integrated into the program hazard analysis documentation and formal risk assessments. Insufficient evidence or evidence of inadequate software system safety program application should be assessed as risk.

(1) Figure B-1 illustrates the relationship between the software system safety activities (hazard analyses, software development, and LOR tasks), system hazards, and risk. Table B-I provides example criteria for determining risk levels associated with software.

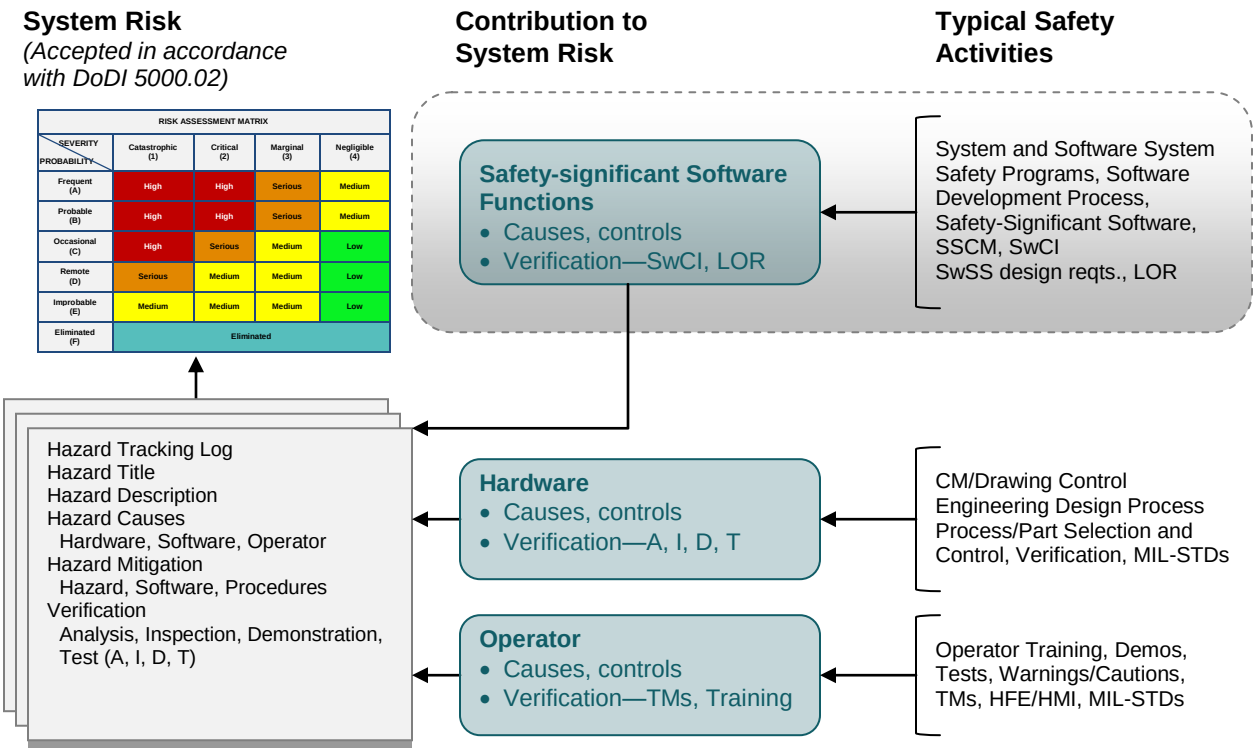


FIGURE B-1. Assessing software's contribution to risk

Downloaded from http://www.everyspec.com

(2) The risks associated with system hazards that have software causes and controls may be acceptable based on evidence that hazards, causes, and mitigations have been identified, implemented, and verified in accordance with DoD customer requirements. The evidence supports the conclusion that hazard controls provide the required level of mitigation and the resultant risks can be accepted by the appropriate risk acceptance authority. In this regard, software is no different from hardware and operators. If the software design does not meet safety requirements, then there is a contribution to risk associated with inadequately verified software hazard causes and controls. Generally, risk assessment is based on quantitative and qualitative judgment and evidence. Table B-I shows how these principles can be applied to provide an assessment of risk associated with software causal factors.

TABLE B-I. Software hazard causal factor risk assessment criteria

Risk Levels	Description of Risk Criteria
	A software implementation or software design defect that upon occurring during normal or credible off-nominal operations or tests:
High	• Can lead directly to a catastrophic or critical mishap, or • Places the system in a condition where no independent functioning interlocks preclude the potential occurrence of a catastrophic or critical mishap.
Serious	• Can lead directly to a marginal or negligible mishap, or • Places the system in a condition where only one independent functioning interlock or human action remains to preclude the potential occurrence of a catastrophic or critical hazard.
Medium	• Influences a marginal or negligible mishap, reducing the system to a single point of failure, or • Places the system in a condition where two independent functioning interlocks or human actions remain to preclude the potential occurrence of a catastrophic or critical hazard.
Low	• Influences a catastrophic or critical mishap, but where three independent functioning interlocks or human actions remain, or • Would be a causal factor for a marginal or negligible mishap, but two independent functioning interlocks or human actions remain. • A software degradation of a safety critical function that is not categorized as high, serious, or medium safety risk. • A requirement that, if implemented, would negatively impact safety; however code is implemented safely.

e. Defining and following a process for assessing risk associated with hazards is critical to the success of a program, particularly as systems are combined into more complex SoS. These SoS often involve systems developed under disparate development and safety programs and may require interfaces with other Service (Army, Navy/Marines, and Air Force) or DoD agency systems. These other SoS stakeholders likely have their own safety processes for determining the acceptability of systems to interface with theirs. Ownership of the overarching system in

Downloaded from http://www.everyspec.com

these complex SoS can become difficult to determine. The process for assessing software's contribution to risk, described in this Appendix, applies the same principals of risk mitigation used for other risk contributors (e.g., hardware and human). Therefore, this process may serve as a mechanism to achieve a "common ground" between SoS stakeholders on what constitutes an acceptable level of risk, the levels of mitigation required to achieve that acceptable level, and how each constituent system in the SoS contributes to, or supports mitigation of, the SoS hazards.

Downloaded from http://www.everyspec.com

CONCLUDING MATERIAL

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

Preparing activity:
Air Force – 40

Review activities:
OSD – OH
Army – AR, AT, CE, CR, MI, TE
Navy/USMC – AS, CG, EC, MC, OS, SA, SH, YD
Air Force – 05, 10, 11, 13, 19, 22, 70, 71, 84, 99

SD-4 project:
SAFT -2006-002

NOTE: The activities listed above were interested in this document as of the date of this document. Since organizations and responsibilities can change, you should verify the currency of the information above using the Acquisition Streamlining and Standardization Information System (ASSIST) Online database at https://assist.dla.mil.