NOT MEASUREMENT SENSITIVE

MIL-STD-882D
w/CHANGE 1
Draft Dated 29 March 2010

SUPERSEDING
MIL-STD-882D
10 February 2000

DEPARTMENT OF DEFENSE STANDARD PRACTICE

SYSTEM SAFETY

Environment, Safety, and Occupational Health Risk Management Methodology for Systems Engineering

AMSC N/A **AREA SAFT**

FOREWORD

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

2. While executing its mission, DoD is committed to protecting private and public personnel from accidental death, injury, or occupational illness and safeguarding defense systems, infrastructure, and public property from accidental destruction, damage, or environmental impacts. DoD is committed to using a structured risk assessment and acceptance framework that manages and minimizes environment, safety, and occupational health (ESOH) risks throughout the lifecycle of the system. Using the system safety approach is essential in managing ESOH risk associated with DoD systems. The Department of Defense recognizes that system safety processes and methodologies are applicable to a broader scope of technical disciplines, such as environment and occupational safety and health. A key DoD objective is to expand the use of system safety methodologies to integrate the ESOH risk management into the overall Systems Engineering (SE) process, rather than addressing ESOH risks as operational considerations afterward.

3. This system safety standard practice identifies DoD's approach for identifying and assessing ESOH hazards and mitigating ESOH risks encountered in the development, test, production, use, and disposal of defense systems. The approach described herein conforms to Department of Defense Instruction 5000.02. ESOH hazards shall be identified and assessed, and ESOH risks shall be mitigated and accepted in accordance with DoD policy. When Military Standard 882 is specified in a solicitation or contract, but no specific task is identified, only sections 3 and 4 are mandatory.

4. This revision incorporates changes to meet Government and industry desire to reinstate task descriptions. These tasks may be specified in contract documents. 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 system safety practices. This standard strengthens integration across ESOH and SE during the acquisition process to ultimately improve consistency of environment, safety, and occupational health practices across programs. Specific changes include:

a. Added the subtitle "ESOH Risk Management Methodology for Systems Engineering" to emphasize ESOH integration into SE.

b. Rewrote task descriptions to clarify and dissociate from each other.

c. 100-series tasks – program management and control.

d. 200-series tasks – design and integration.

e. 300-series tasks – design evaluation.

f. 400-series tasks – compliance and verification.

g. Emphasized the identification and derivation of applicable ESOH technical requirements.

h. Added Hazardous Materials Management Process, Health Hazard Analysis, Systems-of-Systems Integration and Interoperability Hazard Analysis, and Environmental Hazard Analysis tasks.

i. For severity, applied increased dollar value on losses.

j. Added “Eliminated” level for probability.

k. Reintroduced software system safety techniques and principles.

l. Placed more emphasis on establishing a collaborative ESOH effort, providing coordinated ESOH input to SE to maximize performance by minimizing the environmental “footprint” of the system and improving safety of personnel and the system itself.

m. Updated Appendix A – Guidance for Implementation of an ESOH Effort, which includes additional detail on hazard definitions and prescribes a process for rolling up risks for individual hazards into mishaps.

5. All comments (recommendations, additions, and deletions) and any pertinent, beneficial document information may be addressed to Headquarters Air Force Materiel Command, 4375 Chidlaw Road, Wright-Patterson Air Force Base, OH 45433-5006, or may be e-mailed to chuck.dorney@wpafb.af.mil. Because contact information can change, verify the currency of this address information using the Acquisition Streamlining and Standardization Information System online database at *http://assist.daps.dla.mil/*.

CONTENTS

FIGURE PAGE

TABLE PAGE

1. SCOPE

1.1. Scope. This system safety standard practice identifies the Department of Defense (DoD) Systems Engineering (SE) approach to eliminating environment, safety, and occupational health (ESOH) hazards, where possible, and minimizing ESOH risks where those hazards cannot be eliminated. This standard covers ESOH hazards encountered in the development, test, production, use, and disposal of defense systems and infrastructure. The approach conforms to Department of Defense Instruction (DODI) 5000.02. ESOH hazards shall be identified and assessed, and ESOH risks shall be accepted in accordance with DoD policy. When Military Standard (MIL-STD) 882D w/CHANGE 1 is specified in a solicitation or contract but no specific task is identified, only Sections 3 and 4 are mandatory.

2. APPLICABLE DOCUMENTS

2.1. General. Sections 3, 4, and 5 of this standard contain no applicable documents. This section does not include documents cited in other sections of this standard or recommended for additional information or as examples.

3. DEFINITIONS

3.1. Acronyms used in this standard. The acronyms used in this standard are defined as follows:

ASSIST	Acquisition Streamlining and Standardization Information System
CDR	Critical Design Review
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
DOT	Department of Transportation
ECP	Engineering Change Proposal
EMD	Engineering and Manufacturing Development
EO	Executive Order
EOD	Explosive Ordnance Disposal
ESOH	Environment, Safety, and Occupational Health
FHA	Functional Hazard Analysis
FMEA	Failure Modes and Effects Analysis
FSCAP	Flight Safety-Critical Aircraft Parts
GFE	Government Furnished Equipment
GOTS	Government Off-the-Shelf
HHA	Health Hazard Assessment
HM	Hazardous Materials
HMMP	Hazardous Materials Management Plan
HTS	Hazard Tracking System

IIHA	Integration and Interoperability Hazard Analysis
IPT	Integrated Product Team
ISO	International Organization for Standardization
IV&V	Independent Verification and Validation
LOR	Level of Rigor
MFOQA	Military Flight Operations Quality Assurance
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
MSDS	Material Safety Data Sheet
NDI	Non-Developmental Item
NEPA	National Environmental Policy Act
NSN	National Stock Number
O&SHA	Operating and Support Hazard Analysis
ODS	Ozone Depleting Substance(s)
OSHA	Occupational Safety and Health Administration
PDR	Preliminary Design Review
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PM	Program Manager
PPE	Personal Protective Equipment
RAC	Risk Assessment Code
RF	Radio Frequency
RFP	Request for Proposal
SAR	Safety Assessment Report
SCC	Software Control Category
SCF	Safety-Critical Function
SCI	Safety-Critical Item
SCN	Specification Change Notice
SDP	Software Development Plan
SE	Systems Engineering
SHA	System Hazard Analysis
SoS	System-of-Systems
SOW	Statement of Work
SPR	Software Problem Report
SRA	Safety Requirements Analysis
SRR	System Requirements Review
SSF	Safety-Significant Function
SSCM	Software Safety Criticality Matrix
SSHA	Subsystem Hazard Analysis
SSEP	System Safety Engineering Plan
SSI	Safety-Significant Item
STANAG	Standardization Agreement (North Atlantic Treaty Organization)
STR	Software Trouble Report
SwCI	Software Criticality Index
WG	Working Group

3.2. Definitions. To ensure consistency across all DoD programs, the following mandatory definitions apply.

3.2.1. 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.

3.2.2. Causal factor. One or several mechanisms that trigger the hazard that may result in a mishap; failures, conditions, or events which contribute either directly or indirectly to the existence of a hazard.

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

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

3.2.5. ESOH technology requirement. Hazard mitigation technology designed to eliminate or reduce risk of systems or equipment failure and associated personnel and environmental hazards, which may occur with or without failure of the system. These technologies are not inherent parts of the design of the system, but rather are additions that mitigate a specific safety, personnel, or environmental hazard. For example, aircraft landing gear would not be an ESOH technology for this purpose because it is an essential part of the basic design of an aircraft. Military Flight Operations Quality Assurance (MFOQA) technology would be an example of an ESOH technology.

3.2.6. Event risk. The assessment of risk as it applies to the specified hardware/software configuration and event(s) of limited duration prior to fielding. Examples of events include testing, field user evaluation, and demonstrations.

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

3.2.8. Flight safety-critical aircraft part (FSCAP). Any aircraft part, assembly, or installation containing a critical characteristic whose failure, malfunction, or absence may cause a catastrophic failure resulting in loss or serious damage to the aircraft, or may cause an uncommanded engine shutdown resulting in an unsafe condition.

3.2.9. Hazard. A condition that if triggered by one or more causal factor(s) can contribute to or result in a mishap.

3.2.10. Hazardous material. Any substance that, due to its chemical, physical, toxicological, or biological nature, causes safety, public health, or environmental concerns.

3.2.11. Human systems integration. Includes 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.

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

3.2.13. 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-significant software function will perform as required.

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

3.2.15. Loss. For the purposes of this document, the term "loss" refers to the summation of the estimated costs for equipment repair or replacement, facility repair or replacement, environmental cleanup, personal injury or illness, environmental liabilities, and any fines or penalties resulting from the projected mishap.

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

3.2.17. Mitigation measure. The recommended action required to eliminate the hazard or reduce the risk of one or more hazards by lowering the probability or severity of mishap.

3.2.18. Probability. The likelihood of the causal factor triggering a hazard; an expression of the likelihood of occurrence of a mishap. Probability is expressed as a value between zero and one. Probability is a component of risk.

3.2.19. Program Manager (PM). The designated individual with responsibility for and authority to accomplish program objectives for development, production, and sustainment to meet the user's operational needs. The PM shall be accountable for credible cost, schedule, and performance reporting to the Milestone Decision Authority.

3.2.20. Residual risk. The risk level that remains after all mitigation measures have been implemented, verified, validated, and formally accepted prior to fielding.

3.2.21. Risk. A measure of the potential loss from a given hazard. Risk is a combined expression of the severity of the mishap and the probability of the causal factor(s).

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

3.2.23. Safety-critical. A term applied to a condition, event, operation, process, or item of whose mishap or hazard severity consequence is deemed to be either Catastrophic or Critical

by definition (e.g., safety-critical function (SCF), safety-critical path, and safety-critical component).

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

3.2.25. Safety-critical item. A hardware or software item that has been determined through system safety analysis to potentially contribute to a Catastrophic or Critical hazard, or that may be implemented to mitigate a Catastrophic or Critical hazard. Note: The term critical safety item (CSI) refers to items covered by Public law 108-136, sec 802 for aviation CSIs and Public Law 109-364, sec 130 for ship CSIs. The definition and use of this term should be confined to that mandated process. The term is not used in this Standard. A safety-critical item may or may not be labeled as a critical safety item.

3.2.26. Safety related. A term applied to anything that is safety-critical or safety-significant.

3.2.27. Safety-related software. Those software components and units whose errors can result in a potential hazard or loss of predictability or control of a system. In the context of this standard, all software that affects the safety of the system is safety related. Safety-related software can be further broken down based on its contribution level to a hazard and the severity of the hazard.

3.2.27.1. Safety-critical software function. A function that has been determined through system safety analysis to potentially contribute to a Catastrophic or Critical system safety hazard if not performed correctly, or that may be implemented to mitigate a Catastrophic or Critical hazard.

3.2.27.2. Safety-significant software function. A function that has been determined through system safety analysis to perform a function related to safety, but is not safety critical. Software functions whose failures result in a hazard of Marginal or Negligible mishap severity.

3.2.28. Safety-significant function (SSF). A function whose failure to operate or incorrect operation will directly result in a mishap of a severity less than Catastrophic or Critical.

3.2.29. Safety-significant item. A hardware or software item which contributes to an SSF.

3.2.30. Safety technology. Hazard mitigation technology, material selection, and associated management processes designed to eliminate or reduce risk of systems or equipment failure and associated personnel hazards which may occur with or without failure of the system.

3.2.31. Severity. An assessment of the potential degree of loss from the mishap. Severity is one component of risk.

3.2.32. 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), nondevelopmental item (NDI), commercial-off-the-shelf (COTS), re-used, Government-furnished equipment (GFE), and Government-developed software used in the system.

a. Firmware. The combination of a hardware device, computer instructions, and computer data that reside as read-only software on the hardware device.

b. Non-developmental item. 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, Government-off-the-shelf (GOTS), Government Furnished Equipment (GFE), re-use items, or previously developed items provided to the program "as is."

c. Commercial-off-the-shelf. Available commercial software purchased for use in a specific system other than the application or system the software was originally designed for. COTS software can include operating systems, libraries, development tools, or complete applications.

d. Government-off-the-shelf. Government-created software, usually from another project. The software was not created by the current developers (see reused software). Source code and all available documentation are usually included, along with test and analysis results.

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

f. Government furnished information. 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.

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

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

3.2.33. 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.

3.2.34. Software system safety. The application of system safety principles to software to ensure that software executes within the system context and operational environment with an acceptable level of safety risk.

3.2.35. 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, such as the gathering of specified data, data processing, and delivery to users.

3.2.36. System-of-systems. A set or arrangement of interdependent systems that are related or connected to provide a given capability.

3.2.37. 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 lifecycle.

3.2.38. System safety engineering. An engineering discipline that employs specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards to reduce associated risk.

3.2.39. System safety management. All plans and actions taken to identify, assess, mitigate, track, control, accept, and document risks encountered in the development, test, acquisition, use, and disposal of systems, subsystems, equipment, and facilities.

3.2.40. 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.

3.2.41. 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 lifecycle (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 lifecycle.

3.2.42. Target risk. The projected residual risk level that the Program Manager plans to achieve by implementing mitigation measures consistent with the design order of precedence.

3.2.43. User. An operational Command or agency that receives or will receive benefit from the acquired system. Combatant commanders and their Component Commands are the users. There may be more than one user for a system. Because the DoD Component Commands are required to organize, equip, and train forces for the combatant commanders, they are users for systems. The Chiefs of the Services and heads of other DoD Components are validation and approval authorities and are not viewed as users.

3.2.44. User representative. A Command or agency that has been formally designated to represent single or multiple users in the capabilities and acquisition process. The DoD Services and the Components of the combatant commanders are normally the user representatives. There should only be one user representative for a system.

4. GENERAL REQUIREMENTS

4.1. General requirements. Program Managers shall include MIL-STD-882D w/CHANGE 1 in all developmental and sustaining engineering solicitations and identify any specific tasks to be performed. System specifications shall include specific ESOH requirements, including any unique classifications and certifications or any risk reduction needs unique to the program. Sections 3 and 4 delineate the minimum mandatory requirements for an acceptable system safety program for any DoD system. When MIL-STD-882D w/CHANGE 1 is required in a solicitation or contract but no specific tasks are included, only the requirements in Sections 3 and 4 apply.

4.2. System safety requirements. This section defines the system safety requirements throughout the lifecycle for any system, new development, upgrade, modification, resolution of deficiencies, or technology development. When properly applied, these requirements should ensure the identification and understanding of ESOH hazards and their associated risks. The requirements should also eliminate hazards or reduce risks through a systematic approach of hazard analysis and risk assessment and management. ESOH refers to all individual, interrelated disciplines that encompass environment, safety, and occupational health. The system safety process shall be used across the ESOH disciplines to identify hazards and mitigate risks through the SE process. Mitigation measures optimized for only one of the disciplines can create hazards in other disciplines. Therefore, hazard assessments should include all three ESOH disciplines, as well as other applicable SE disciplines.

4.3. System safety process. The eight-step system safety process consists of:

4.3.1. Document the system safety approach. The PM and contractor shall document the approved systems engineering and management approach and other actions needed to establish a fully functional ESOH effort in accordance with current DoD acquisition policy. The efforts shall be proactive and integrated with the systems engineering process to influence the design. The minimum requirements for the approach will include:

a. Designating individual(s) responsible to the PM for executing the ESOH effort, including clearly defined roles and responsibilities.

b. Identifying the ESOH effort and how the program is integrating ESOH considerations into the SE process, Integrated Product and Process Development process, and the overall program management structure.

c. Identifying the prescribed and derived ESOH requirements applicable to the system. Examples include pollution prevention mandates, ESOH design requirements, safety technology considerations, and occupational and community noise standards. Once the ESOH requirements are identified, ensure the flow-down of all requirements to subcontractors, vendors, and suppliers, as well as the verification of the change in the design as a result of implementing those requirements.

d. Defining how hazards and associated risks are tracked and formally accepted by the appropriate risk acceptance authority. The steps below shall be documented in a closed-loop hazard tracking system.

4.3.2. Identify hazards. Identify hazards through a systematic hazard analysis process that includes system hardware and software, system interfaces, the environment, and the intended use or application. 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 lifecycle and potential impacts to personnel, infrastructure, defense systems, the public, and the environment. As hazards are identified, they are entered into the hazard tracking system.

4.3.3. Assess risk. Assess the severity and probability of the potential effect(s) for each hazard. This assessment establishes the initial risk for each hazard. Tables I through III shall be used, unless a DoD Component develops and approves alternate risk assessment matrices. These alternate risk matrices shall be derived from Tables I through III. ESOH risks shall be accepted in accordance with DoD policy.

TABLE I. Severity categories

SEVERITY CATEGORIES		
Severity Category	Severity Level	Environment, Safety, and Occupational Health Mishap Result Criteria
Catastrophic	1	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or loss 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 loss exceeding $1M but less than $10M.
Marginal	3	Could result in one or more of the following: injury or occupational illness resulting in 10 or more lost work days, reversible moderate environmental impact, or loss exceeding $100K but less than $1M.
Negligible	4	Could result in one or more of the following: injury or illness resulting in less than 10 lost work days, minimal environmental impact, or loss less than $100K.

TABLE II. Probability levels

PROBABILITY LEVELS			
Description	**Level**	**Specific Individual Item[1,2]**	**Fleet or Inventory[2]**
Frequent	A	Likely to occur often in the life of an item; with a probability of occurrence greater than 10^{-1} in that life.	Continuously experienced.
Probable	B	Will occur several times in the life of an item; with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.	Will occur frequently.
Occasional	C	Likely to occur sometime in the life of an item; with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.	Will occur several times.
Remote	D	Unlikely, but possible to occur in the life of an item; with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life.	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; with a probability of occurrence of less than 10^{-6} in that life.	Unlikely to occur, but possible.
Eliminated[3]	F	Incapable of occurrence in the life of an item. This category is used when potential hazards are identified and later eliminated.	Incapable of occurrence within the life of an item. This category is used when potential hazards are identified and later eliminated.

DoD_MIL-STD-882_002

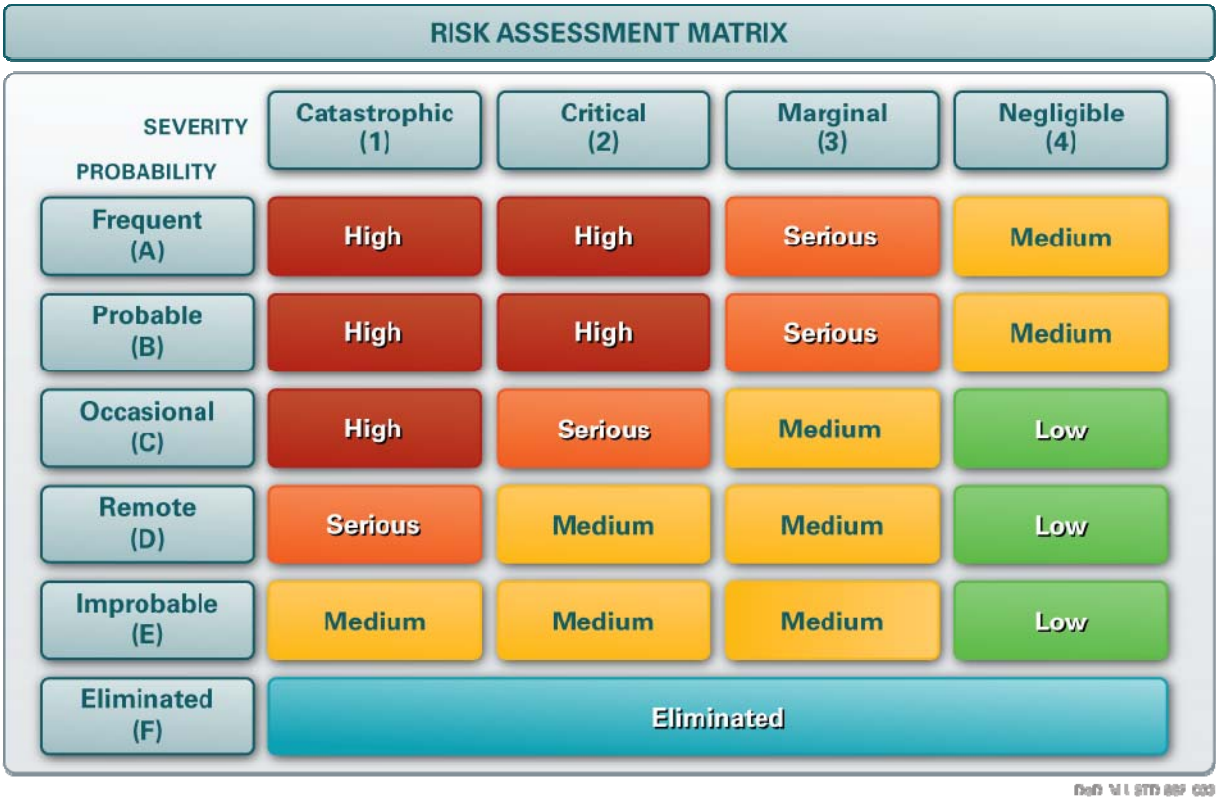
NOTES:

(1) Use either the quantitative or qualitative descriptions of probability, as appropriate, for a given analysis.

(2) Use either the individual item or fleet inventory description, depending on which description produces the more frequent probability level for a given analysis.

(3) Probability level F is reserved for cases where the causal factor is either no longer present or it is impossible to lead to the mishap. No amount of doctrine, training, warning, caution, personal protective equipment (PPE), or other change can move a mishap probability to level F.

TABLE III. Risk assessment matrix



NOTE: A risk assessment code (RAC) is a combination of one severity and one probability that correlates to a specific cell (e.g., a RAC of 1A is the combination of a Catastrophic severity and a Frequent probability).

4.3.4. 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.

4.3.4.1. For software assessments, Tables IV through VI shall be used, unless tailored and formally approved in accordance with DoD Component policy. The degree of software control is defined using the software control categories in Table IV (or approved tailored alternative), and severity level is defined using Table I (or approved tailored severity categories). A Software Safety Criticality Matrix (SSCM) based on the approved severity categories and software control categories shall be developed and shall define a Software Criticality Index (SwCI). Table V provides the SSCM based on Table I severity categories and Table IV software

control categories. The SwCI is used to define the required LOR for activities. Table VI provides the relationship between the SwCI, the Table III Risk Assessment Matrix, the LOR, and how the LOR affects software's contribution to risk.

4.3.4.2. 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 activities 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.

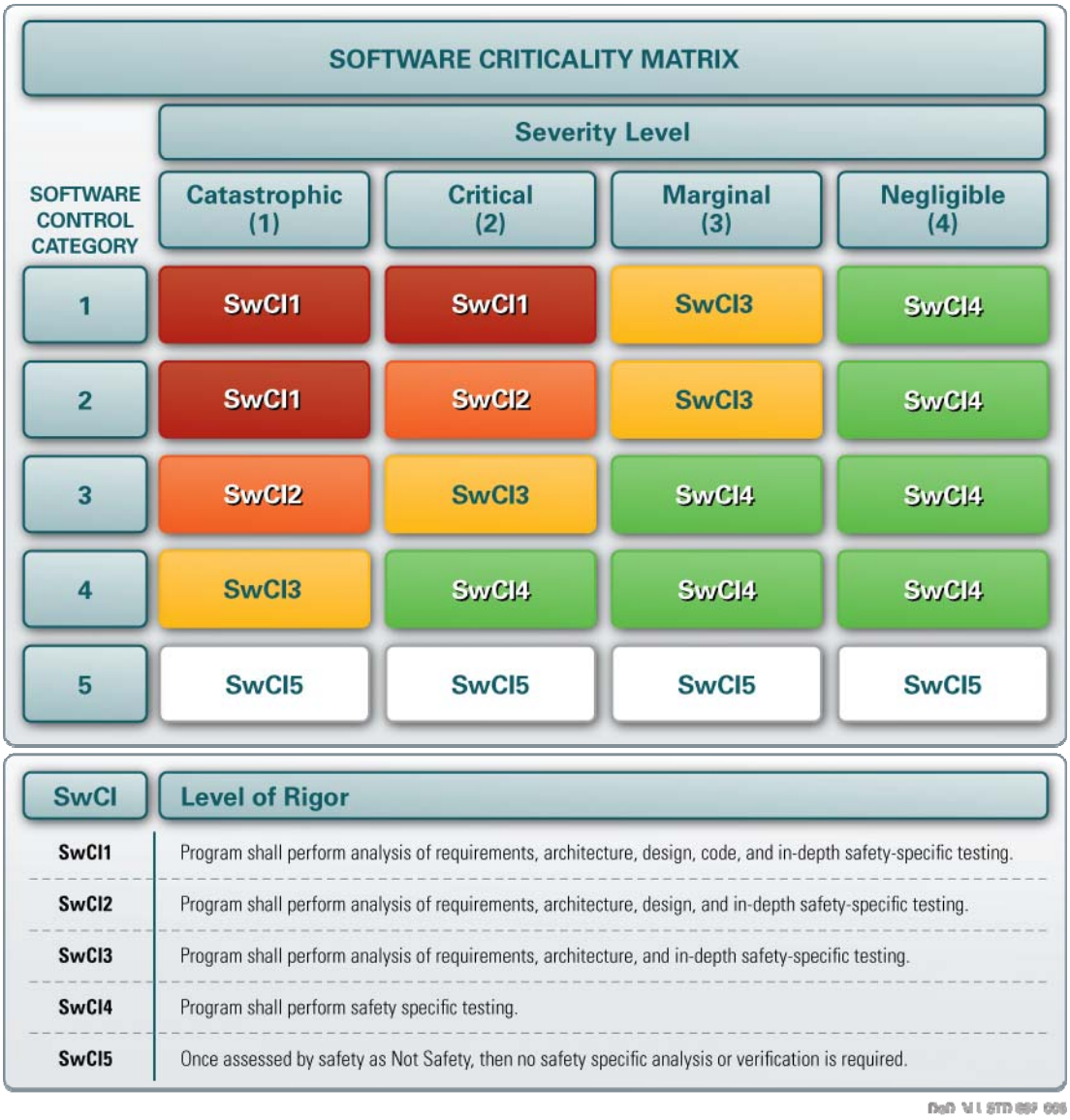
4.3.4.3. Appendix A.4 provides guidance for developing acceptable LOR for each software criticality category.

TABLE IV. Software control categories

SOFTWARE CONTROL CATEGORIES (SCC)		
Level	**Name**	**Description**
1	Autonomous	• A software function that exercises control/authority over hazardous hardware systems, sub-systems, or components without the possibility or need of intervention/ control by another system or operator to preclude the occurrence of a hazard.
2	Semi-Autonomous	• A software function that exercises control/authority over hazardous hardware systems, subsystems, or components which allows time for or requires intervention by independent safety controls or an operator action to preclude the occurrence of the hazard. • The software item supplies information requiring immediate operator action to execute an action for mitigation or control over a hazard. Software exception, failure, fault or delay will allow or fail to prevent the mishap occurrence.
3	Redundant Fault Tolerant	• A software function that exercises control/authority over hazardous hardware systems, subsystems, or components that requires at least two independent activities (either human action or system function) to complete the operation or check the integrity of the functional output. • Software generates data and or information used to make critical decisions. The system includes several, redundant independent fault tolerant mechanisms for each hazardous condition, detection, and display.
4	Influential	• A software function that generates information of a safety related nature used to make decisions by the operator but does not require operator action to avoid a hazard (there are two or more redundant, independent correlated displays to allow the operator to avoid hazards).
5	Not Safety	• Software functionality does not possess command and/or control authority over safety-related hardware systems, sub-systems or components and does not provide safety-related information. Software does not provide safety-related or time sensitive data or information that requires control entity interaction. Software does not transport or resolve communication of safety-related or time-sensitive data.

4.3.5. Software Safety Criticality Matrix. The SSCM (Table V) uses the 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 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 associated with each SwCI is the minimum set of verification activities required to be performed on the identified software.

TABLE V. Software safety criticality matrix



SOFTWARE CRITICALITY MATRIX				
	Severity Level			
SOFTWARE CONTROL CATEGORY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
1	SwCI1	SwCI1	SwCI3	SwCI4
2	SwCI1	SwCI2	SwCI3	SwCI4
3	SwCI2	SwCI3	SwCI4	SwCI4
4	SwCI3	SwCI4	SwCI4	SwCI4
5	SwCI5	SwCI5	SwCI5	SwCI5

SwCI	Level of Rigor
SwCI1	Program shall perform analysis of requirements, architecture, design, code, and in-depth safety-specific testing.
SwCI2	Program shall perform analysis of requirements, architecture, design, and in-depth safety-specific testing.
SwCI3	Program shall perform analysis of requirements, architecture, and in-depth safety-specific testing.
SwCI4	Program shall perform safety specific testing.
SwCI5	Once assessed by safety as Not Safety, then no safety specific analysis or verification is required.

NOTE: Consult the Joint Services Software System Safety Handbook for additional guidance on how to conduct required software analyses.

4.3.5.1. Upon completion of all specified software system safety engineering and LOR tasks, the results will be used as evidence that the software contribution to the identified system-level mishap can be considered mitigated. If the software design does not provide sufficient evidence that it meets safety requirements, then an assessment must be made to determine the residual risk associated with inadequately verified software hazard causes and controls (i.e., open in the hazard record). Once all of the hazard's causes have been mitigated and verified, appropriate management authorities accept the residual risks for the associated system mishap. Risk acceptance is performed in accordance with DoD policy.

4.3.6. Assessment of software contribution to risk. Risk acceptance authorities are defined by DoD policy. The minimum PM-specified LOR activities must be successfully performed in order to assess that software contributions to the system-level risk have been mitigated. If the required LOR activities are not successfully performed, then the system risk(s) contributions associated with unspecified, incomplete, or unsuccessful LOR shall be documented according to Table VI or the approved tailored alternative. Table VI depicts the relationship between SwCI, risk categories, completion of LOR, and residual risk. Once documented, the risk shall be provided to the PM for a decision on whether to expend the resources required to reduce the risk or to process a formal system safety risk assessment for acceptance by the appropriate decision authority.

4.3.6.1. For software, the SwCI and LOR define the requirements of mitigation efforts. An SwCI1 from the SSCM does not imply that a software-related risk may be unacceptable. Rather, the SwCI1 LOR is required to be successfully performed prior to SwCI1 software contribution to High system risk being considered as reduced. Likewise, SwCI2 and risk category Serious requires SwCI2 LOR be successfully performed, SwCI3 and risk category Medium requires SwCI3 LOR, and SwCI4 and Risk Category Low requires SwCI4 LOR to be successfully performed to reduce the software's contribution to system-level risk. SwCI5 is considered Not Safety and does not require safety-specific testing or analysis.

4.3.6.2. If all required LOR activities are performed successfully, the software's contribution to risk can be considered as mitigated down. Appendix A provides guidance on evaluating software's contribution to system risk. Once all risk has been mitigated, appropriate management authorities accept the residual risks (or event risk) in accordance with DoD policy.

TABLE VI. Relationship between SwCI, risk categories, LOR, and residual risk

RELATIONSHIP BETWEEN SwCI, RISK CATEGORIES, LOR AND RESIDUAL RISK		
Software Criticality Index (SwCI)	**Risk Category (Table III)**	**Software LOR and Risk Assessment/Acceptance**
SwCI1	High	If SwCI1 LOR is unspecified, incomplete and/or unsuccessful, 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 a SwCI1 LOR or prepare a formal risk assessment with a HIGH residual risk.
SwCI2	Serious	If SwCI2 LOR is unspecified, incomplete and/or unsuccessful, 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 a SwCI2 LOR or prepare a formal risk assessment with a SERIOUS residual risk.
SwCI3	Medium	If SwCI3 LOR is unspecified, incomplete and/or unsuccessful, 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 a SwCI3 LOR or prepare a formal risk assessment with a MEDIUM residual risk.
SwCI4	Low	SwCI4 LOR in accordance with Table V or approved DoD policy. If SwCI4 LOR is unspecified, incomplete and/or unsuccessful, 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 a SwCI4 LOR or accept the LOW residual risk.
SwCI5	Not Safety	No safety-specific analyses or testing is required.

4.4. Identify risk mitigation measures. Potential risk mitigation alternatives shall be identified, and the expected effectiveness of each alternative or method shall be measured. Risk mitigation is an iterative process for eliminating or reducing risk to the lowest acceptable level within the constraints of operational effectiveness and suitability, time, and cost. The system safety design order of precedence is explained below. In general, design changes can either eliminate or reduce the severity and probability of a mishap. The remaining types of mitigation measures can only reduce the probability of the mishap.

4.4.1. Eliminate hazards through design selection. Ideally, the risk of a hazard should be eliminated. This elimination is often accomplished by selecting a design alternative that removes the hazard altogether.

4.4.2. Reduce risk through design alteration. If the risk of a hazard cannot be eliminated by adopting an alternative design or alternative material, consider design changes that reduce the severity and/or the probability of a hazard.

4.4.3. Incorporate engineered features or devices. If the risk of a hazard is unable to be eliminated or adequately mitigated through a design alteration, reduce the risk using an engineered feature or device. In general, engineered features actively interrupt the mishap sequence and devices reduce the risk of a mishap.

4.4.4. Provide warning devices. If engineered features and devices do not adequately lower the risk of the hazard, include a detection and warning system to alert personnel to the presence of a hazardous condition or occurrence of a hazardous event.

4.4.5. Develop procedures and training. Where other risk reduction methods cannot adequately mitigate the risk from a hazard, incorporate special procedures and training. Procedures may prescribe the use of PPE or the collection of hazardous waste and materials for reuse, recycling, or disposal. Warnings, cautions, and other written advisories shall not be used as the only risk reduction method for High and Serious initial risk levels.

4.5. Reduce risk. Select and implement the mitigation measures that achieve the acceptable risk level. In reducing risk, 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 risks and status of risk reduction efforts at technical reviews.

4.6. Verify risk reduction. Verify the implementation and validate the effectiveness of all selected risk mitigation measures through appropriate analysis, testing, or inspection.

4.7. Accept risk. Before exposing people, equipment, or the environment to known system-related hazards, the associated risk levels shall be accepted by the appropriate authority as defined in current DoD policy. The formal risk acceptance decision documentation shall include the associated system configuration and shall be retained for the life of the system. Tables I through III (Tables IV and VI for software) shall be used to define the risk levels at the time of the acceptance decision. The user representative shall be part of this process throughout the lifecycle of the system and shall provide formal concurrence before all Serious and High risk acceptance decisions. After fielding, data from mishap reports, user feedback, and experience with similar systems or other sources may expose new hazards or demonstrate that the risk for a known hazard is higher than previously recognized. In these cases, the new or elevated risk shall be accepted in accordance with DoD policy.

4.8. Manage life-cycle risk. After the system is fielded, the PM shall ensure that the system safety process continues to identify hazards and maintain the hazard tracking system throughout its lifecycle. This life-cycle effort shall consider any changes to the interfaces, users, hardware and software, mishap data, mission(s) or profile, system health data, and similar concerns. The program office and user community shall maintain effective communications to collaborate, identify, and manage new hazards and modified risks. If new risks are discovered or

known hazards are determined to have a higher risk category than previously assessed, the risk will need to be formally accepted in accordance with DoD policy.

5. DETAILED REQUIREMENTS

5.1. Optional information. Appendix A and individual series tasks 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 sequence of task and subtask accomplishment should be tailored to the individual program to which they are being applied. The 100-series tasks apply to program management and control. The 200-series tasks apply to design and integration. The 300-series tasks apply to design evaluation. The 400-series tasks apply to compliance and verification.

5.2.1. 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 explains the actual subtasks that compose the PM-specified task a contractor shall perform. The PM shall tailor task descriptions as required by governing regulations and as appropriate to particular systems or equipment, program type, magnitude, and funding. In tailoring the tasks, the PM defines the detail and depth of the effort, and the results are incorporated into the appropriate contractual documents. When preparing proposals, the contractor may include additional tasks or task modifications with supporting rationale for each addition or modification.

c. The details to be specified in each task description lists specific details, additions, modifications, deletions, or options to the requirements of the task that the PM should consider when tailoring the task description to fit program needs. This information is then included in the stated task document. The list provided with each task is not necessarily complete and may be supplemented by the PM. 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 PM provides these details to the contractor for proper implementation of the task.

6. NOTES

6.1. Notes section. This section contains information of a general or explanatory nature that may be helpful but is not mandatory.

6.1.1. Intended use. This standard establishes a common basis for a properly executed ESOH effort within the DoD Defense Acquisition System requirements.

6.1.2. Acquisition requirements. Acquisition documents should specify the title, number, and date of the standard and any requested tasks.

6.1.3. Associated data item descriptions (DIDs). This standard has been assigned an Acquisition Management Systems Control number authorizing it as the source document for the following DIDs. When it is necessary to obtain data, the applicable DIDs must be listed on the Contract Data Requirements List (DD Form 1423).

a. DIDs associated with this standard include:

DID Number	DID Title
DI-SAFT-80101B	System Safety Hazard Analysis Report
DI-SAFT-80102B	Safety Assessment Report (SAR)
DI-SAFT-80103B	Engineering Change Proposal System Safety Report
DI-SAFT-80104B	Waiver or Deviation System Safety Report (WDSSR)
DI-SAFT-80105B	System Safety Program Progress Report
DI-SAFT-80106B	Health Hazard Assessment Report
DI-SAFT-80913B	Explosive Ordnance Disposal Data
DI-SAFT-81299B	Explosive Hazard Classification Data
DI-SAFT-81300A	Mishap Risk Assessment Report
DI-SAFT-81626	System Safety Program Plan

b. DIDs which may be applicable to the system safety program but are not directly linked to this standard include:

DID Number	DID Title
DI-ADMIN-81250	Conference Minutes
DI-MISC-80043B	Ammunition Data Card
DI-MISC-80370	Safety Engineering Analysis Report
DI-ILSS-81495	Failure Mode and Effects Criticality Analysis Report
DI-SAFT-80184	Radiation Hazard Control Procedures
DI-SAFT-81065	Safety Studies report
DI-SAFT-81066	Safety Studies Plan

c. The above DIDs are current as of the date of this standard. The ASSIST database should be researched at *http://assist.daps.dla.mil/quicksearch* to ensure that only current and approved DIDs are cited on the DD Form 1423.

6.1.4. Subject term (key word) listing

a. Environment.

b. Environmental impact.

c. Hazard.

d. Hazardous material (HM).

e. Lifecycle.

f. Mishap.

g. Occupational health.

h. Probability.

i. Risk.

j. Safety.

k. Severity.

l. System safety.

m. System safety engineering.

n. Systems Engineering.

6.1.5. Identification of changes. Because of the extent of the changes, marginal notations are not used in this revision to identify changes with respect to the previous issue.

TASK 101
ESTABLISH AN ESOH EFFORT

101.1. Purpose. The purpose of Task 101 is to establish the foundation for integrating ESOH considerations and requirements into the SE process.

101.2. Task description.

101.2.1. Establish and execute an ESOH effort within SE that meets the requirements of Section 4, General Requirements, and all other tasks and requirements designated by the Program Manager.

101.2.2. Plan for the ESOH effort, including the identification and allocation of adequate manpower and funding resources, to ensure the ESOH effort is completed.

101.2.3. Define ESOH roles and responsibilities, as well as lines of communication within the program organization and with associated organizations, including Government, subcontractors, and program offices of related systems and components. Within SE, define the interrelationship among ESOH efforts and establish interfaces with other functional elements of the program, including human systems integration, test and evaluation, logistics, financial, and contracting.

a. Ensure the flow down of all identified ESOH requirements to subcontractors, associate contractors, vendors, and suppliers. This includes 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.

b. Report ESOH risks 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.

101.2.4. Develop and maintain a closed-loop hazard tracking system that includes subcontractor, vendor, and supplier hazard tracking data. The minimum data elements for the tracking system are hazard, causal factor, mishap, initial risk, event risk, target risk, residual risk, mitigation measures, and status.

101.2.4.1. If using hazard probability levels and severity categories other than those specified in Section 4, define the probability and severity criteria, identify the risk assessment matrix, and submit for formal approval in accordance with DoD Component policy.

101.2.4.2. Reporting of the following—

a. Hazards and associated risks.

b. Safety-related functions, safety-critical functions, safety-significant functions, safety-related items, safety-critical items, safety-significant items, and flight safety-critical aircraft parts.

c. Operation, maintenance, sustainment, and disposal ESOH requirements.

d. Measures used to mitigate ESOH hazards.

e. Assessment for HM elimination/minimization and trade studies to support recommended material use.

f. Identification of HM in and associated with the system, including materials required for operations, maintenance, and disposal.

g. Safety analyses and assessments required to support safety releases prior to developmental or operational testing.

101.2.5. Identify the event-driven ESOH activities, such as reviews, approvals, certifications, analyses, safety releases, and National Environmental Policy Act (NEPA) and Executive Order (EO) 12114 analyses and documentation, and include them in the Integrated Master Schedule.

101.2.6. Evaluate compliance with EOs such as EO 12114 and EO 13423; applicable national, state, and local ESOH laws, regulations, and statutes, including NEPA; international agreements; and Department of Defense and applicable DoD Component acquisition ESOH policy.

101.3. Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 101. (R)

b. PM requirements for incident processing.

c. PM requirements and methodology of reporting on this task.

d. Qualifications for key ESOH personnel.

e. Other specific ESOH effort requirements.

TASK 102
SYSTEM SAFETY ENGINEERING PLAN

102.1. Purpose. The purpose of Task 102 is to develop a System Safety Engineering Plan (SSEP). The SSEP can have two scopes. One scope shall detail the tasks and activities of system safety management and engineering activities for a program that are required to identify, evaluate, and eliminate or mitigate ESOH hazards or reduce the associated risk through a systematic approach of hazard analysis, risk assessment, and management. The second scope shall provide the system integrating contractor or Program Manager with appropriate management oversight of system safety engineering and management efforts and the capability to establish and maintain uniform integrated system safety requirements across all elements of a portfolio of programs. The approved plan shall provide a formal basis of understanding between the contractor and PM on how ESOH efforts will be established and executed to meet contractual requirements, including general and specific provisions.

102.2. Task description. The contractor shall develop an SSEP to provide a basis of understanding between the contractor and the PM on how the system safety engineering and management processes will be accomplished to meet contractual ESOH requirements included in the general and special provisions of the contract. The approved plan shall, item-by-item, account for all contractually required tasks and responsibilities. The SSEP shall include the following:

102.2.1. Plan scope and objectives. Each SSEP shall describe, at a minimum: (1) a planned system safety approach for accomplishing the general requirements in Section 4 and other contractually required tasks as they relate to the ESOH disciplines, (2) qualified people to accomplish tasks, (3) authority to implement the plan through all levels of Systems Engineering and management (such as the Systems Engineering Plan, Test and Evaluation Strategy, etc), and (4) appropriate commitment of resources (both staffing and funding) to ensure that SSEP tasks are completed. The SSEP shall define a process to satisfy the system safety requirements imposed by the contract. This section shall:

a. Describe the scope of the overall SSEP, SE effort, and the related ESOH effort.

b. Describe the interface between the core personnel and all other applicable ESOH disciplines (e.g., system safety, range safety, explosive and ordnance safety, chemical and biological safety, directed energy, laser and radio-frequency safety, software system safety, industrial hygiene, and NEPA), SE and all other support disciplines (e.g., maintainability, quality control, reliability, software development, and human systems integration), and all system integration and test disciplines.

c. List the tasks and activities of system safety management and engineering. Describe the interrelationships between the various technical disciplines and other functional elements of the program. List the other program requirements and tasks applicable to the system safety engineering effort and identify where these are specified or described.

d. Account for all contractually required ESOH efforts and system safety engineering and management tasks and responsibilities. A matrix shall be provided to correlate the requirements of the contract to the location in the SSEP where the requirement is addressed.

e. Describe the interfaces between the contractor, including communication methods; the system safety engineering and management efforts required from each contractor, subcontractor, or supplier; and how those efforts will be integrated into the system safety engineering and management efforts for the total system as they relate to ESOH. Include a discussion of how the risks will be integrated into the overall system or system-of-systems to provide the Government with an overall picture of the hazards and risks.

f. Describe the processes for system safety analysis for the use of COTS and NDI.

102.2.2. Organization. The SSEP shall describe, at a minimum:

a. The organization or function of the system safety engineering and management efforts as related to ESOH within the organization of the total program. Use charts to show the organizational and functional relationships and lines of communication. Show the organizational relationship between other functional elements having responsibility for tasks with system safety process impacts and the ESOH management and engineering organization. Review and approval authority of applicable tasks by appropriate personnel shall be described.

b. The responsibility and authority of ESOH personnel, other contractor organizational elements involved in the system safety engineering efforts, and subcontractors. Describe the methods by which personnel may raise issues of concern directly to the contractor's Program Manager or supervisor. Identify the organizational unit responsible for executing each task. Identify the authority for resolution of all identified hazards.

c. The staffing of the system safety efforts related to all ESOH disciplines for the duration of the contract. The SSEP should include manpower loading and schedule, control of resources, and a summary of the qualifications of key ESOH roles. Those who have coordination and approval authority for contractor-prepared documentation should be included in the SSEP. Specific contract language is usually required to have key personnel identified and that the acquirer be formally notified of any replacement(s).

d. The method, authority, and coordination the contractor will use to integrate system-level and system-of-systems level system safety efforts as related to ESOH. This includes assigning requirements to action organizations and subcontractors, coordinating subcontractor system safety engineering programs, integrating hazard analyses, facilitating program and design reviews, reporting on program status and metrics, and establishing ESOH IPTs and WGs.

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

f. If integration of various systems is required, define the role of the integrator and the effort required from each contractor and subcontractor to integrate system safety requirements for the total system. Define where the control, authority, and responsibility transition from one contractor to another.

102.2.3. Milestones. The SSEP shall, at a minimum:

a. Define system safety milestones as they relate to all ESOH disciplines. Relate these milestones to major program milestones, technical reviews, program element responsibility, and required inputs and outputs.

b. Provide a program schedule of system safety engineering tasks as they relate to all ESOH disciplines, including start and completion dates, reports, and reviews.

c. Identify subsystem, component, and software system safety activities, as well as integrated system-level activities (e.g., design analyses, tests, and demonstrations) applicable to the system safety process but specified in other engineering studies and development efforts to preclude duplication.

d. Provide the estimated manpower loading required to complete each task.

e. Include a schedule of technical meetings between all associate contractors to discuss, review, and integrate the safety effort. When issues cannot be resolved within the technical meeting structure, the integrating contractor will elevate issues to the PM.

102.2.4. General ESOH requirements and criteria. The SSEP shall:

a. Describe general engineering requirements and ESOH design criteria. Describe system safety requirements for support equipment and operational safety requirements for all appropriate phases of the lifecycle up to and including disposal. List the standards and system specifications containing ESOH requirements that the contractor shall use in the execution of the contract. Include titles, dates, and where applicable, paragraph numbers.

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

c. Describe closed-loop procedures for taking action to resolve identified risk, including those involving COTS and NDI.

102.2.5. Hazard analysis. At a minimum, the SSEP shall describe:

a. The hazard analysis techniques and formats to be used in qualitative or quantitative analyses to identify hazards, their causes and effects, hazard elimination, and risk reduction requirements and how those requirements will be verified. When conducting system-

of-systems risk assessments, 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 shall be used in the conduct of this effort.

b. The depth within the system that each technique is used, including hazard identification associated with the system, subsystem, components, software, hazardous material, personnel, human systems integration, ground support equipment, COTS, NDI, facilities, and their interrelationship in the logistic support, training, maintenance, operational, and disposal (including render-safe and emergency disposal) environments.

c. The method for ensuring flow-down of safety-critical/significant functions, safety-critical items (SCI), and FSCAPs, as well as associated requirements to the supplier and integration of subcontractor/supplier hazard analyses with overall system hazard analyses.

d. Efforts to identify and control hazards associated with materials used during the system's lifecycle. When performing a safety assessment of a system-of-systems, summarize the risk presented by the operation of the integrated system. Data or analyses provided by associate contractors or subcontractors shall be used in the conduct of this effort.

e. A systematic software system safety approach to:

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

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

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

(7) Identify and assign the SwCI for each safety-related software function (SRSF) and its associated requirements.

f. Perform a final system risk assessment that incorporates software hazard causal factors and risk mitigations. Resolve differences between associate contractors in areas related to safety, especially during development of safety inputs to system and item specifications. Where problems cannot be resolved by the integrator, notify the PM for resolution and action.

102.2.6. Supporting data. At a minimum, the SSEP shall:

a. Describe the approach for collecting and processing pertinent historical hazard, mishap, and lessons learned data.

b. Identify deliverable data by title, number, and means of delivery (e.g., hard copy and electronic).

c. Identify non-deliverable ESOH data, describe the procedures for PM accessibility, and retain data of historical value.

d. When the plan describes a system-of-systems, the SSEP shall include:

(1) Requirements for any special integrated safety analyses.

(2) A description of specific integration roles outside of the contract.

(3) Identification of interfacing hardware and software that are not part of the specific contract (e.g., GFE and Government-furnished information).

(4) Contractual language to ensure that associate contractors are responsive to the requirements of the SSEP.

102.2.7. Safety verification. At a minimum, the SSEP shall document how the safety program will:

a. Verify (e.g., test, analysis, inspection, etc.) requirements and methods for providing concrete evidence in artifacts and test results that safety is adequately demonstrated. Identify any certification requirements for software, safety devices, or other special safety test or safety mitigation testing (e.g., Failure Modes Effects Analysis (FMEA), insensitive munitions tests, and render-safe and emergency disposal procedures).

b. Ensure that procedures for safety-related verification information are transmitted to the PM for review and analysis.

c. Ensure, in accordance with DoD policy requirements, that ESOH risks associated with testing are identified and transmitted to the PM for formal acceptance prior to the test event.

102.2.8. Audit program. The SSEP shall describe the techniques and procedures to be employed by the contractor to make sure the objectives and requirements of the system safety engineering process are being accomplished.

102.2.9. Training. The SSEP shall describe the training for engineering, technician, operations, and maintenance personnel involved in system safety engineering activities associated with acquisition, sustainment, and disposal of the item(s) under contract.

102.2.10. Incident reporting. The contractor shall describe in the SSEP the mishap, incident alerting, notification, investigation, and reporting processes, including notification of the PM.

102.3. Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 102. (R)

b. Additional information to be provided.

c. Qualifications for key ESOH personnel.

TASK 103
SUPPORT TO GOVERNMENT REVIEWS/AUDITS

103.1. Purpose. The purpose of Task 103 is to establish a requirement for the contractor to support reviews and audits performed by or for the Program Manager. This task is also used to acquire support for special requirements, such as certifications and test/flight readiness reviews.

103.2. Task description.

103.2.1. The contractor shall support reviews and audits performed by representatives of the PM to the extent specified in the contract.

103.2.2. To the extent the PM specifies in the contract, the contractor shall support presentations to Government-certifying activities such as, but not limited to, program and technical reviews, munitions safety boards, nuclear safety boards, mission readiness reviews, flight readiness reviews, launch readiness reviews, and flight safety review boards. These presentations also may include special reviews such as flight/article readiness reviews or preconstruction briefings.

103.3. Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 103. (R)

b. Reviews and audits, their content, any guidance instructions, and probable location(s). (R)

c. Method of documenting the results of reviews and audits.

TASK 104
ESOH IPT/WORKING GROUP SUPPORT

104.1. Purpose. The purpose of Task 104 is to require contractors to support the ESOH Integrated Product Team or WG, as defined by the Program Manager.

104.2. Task description. The contractor shall participate as an active member of ESOH WGs. Relationships with the SE IPTs and other related teams shall be established. Such participation shall include, but is not limited to, the following activities:

a. Present the status of contractor ESOH efforts.

b. Summarize hazard analyses and the status of all risks. Identify issues or problems associated with risk mitigations. Work toward agreement on the effectiveness of implemented mitigation measures and associated reduction of risks.

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

d. Respond to action items assigned by the chair of the ESOH Working Group.

e. Review and validate ESOH requirements, criteria, and constraints applicable to the program.

f. Plan and coordinate support for required reviews and certification processes.

g. Review and validate the NEPA/ EO 12114 Compliance Schedule.

104.2.1. Subcontractors. The contractor shall require that all major subcontractors participate in the ESOH IPT/WG.

104.2.2. Associate Contractor. The integrating contractor shall require that all associate contractors participate in the ESOH IPT/WG.

104.3. Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 104. (R)

b. Contractor membership requirements and role assignments. (R)

c. Frequency or total number of ESOH IPT/WG meetings and probable locations. (R)

d. Requirement for the contractor to prepare and distribute the agenda and minutes of the ESOH IPT/WG. (R)

TASK 105
HAZARD TRACKING SYSTEM

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

105.2. Task description. The contractor shall develop and maintain a centralized hazard tracking system that shall contain, at a minimum:

a. Hazard.

b. Life-cycle phases affected by the hazard.

c. Causal factor (e.g., hardware, software, or human).

d. Effects.

e. Mishap,

f. Initial RAC and associated risk category.

g. Target RAC and associated risk category.

h. Event RAC and associated risk category.

i. Residual RAC and associated risk category.

j. Mitigation measures.

k. Hazard status (e.g., open or closed).

l. Hazard traceability (running history of actions taken or planned with rationale to mitigate risks).

m. Verification and validation method.

n. Action person(s) and organizational element.

o. 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).

p. If hazards are associated with hazardous materials, the following additional data fields should be included in the hazard tracking system:

(1) Location of HM within the system during its entire lifecycle.

(2) Quantity of HM within the system during its entire lifecycle.

(3) Process or activity whereby quantities of HM are used or generated during operations, support, or disposal of the system.

(4) Reasonably anticipated hazardous materials that are used or generated during the lifecycle of the system (e.g. installation, test and evaluation, normal use, maintenance or repair, and disposal of the system).

(5) Reasonably anticipated hazardous materials to be used or generated in emergency situations (e.g., exhaust, fibers from composite materials released during accidents, combustion byproducts, etc.).

(6) Special HM controls, training, handling measures, and personal protective equipment needed, including provision of required material safety data sheets (MSDSs).

105.2.1. NOTE: Task 204 (Subsystem Hazard Analysis), Task 205 (System Hazard Analysis), Task 206 (Operating and Support Hazard Analysis), and Task 210 (Environmental Hazard Analysis) may include additional requirements for the hazard tracking system.

105.3. Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 105. (R)

b. Government access and data rights to the hazard tracking system. (R)

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

TASK 106
ESOH PROGRESS SUMMARY

106.1. Purpose. The purpose of Task 106 is to prepare a periodic progress report summarizing the pertinent ESOH management and engineering activities that occurred during the reporting period.

106.2. Task description.

106.2.1. The contractor shall prepare a periodic ESOH progress report that summarizes general progress made relative to the ESOH effort during the specified reporting period and forecasts projected work for the next reporting period.

106.2.2. Report Requirements. The contractor shall prepare a report that contains, at a minimum, the following information:

a. A brief summary of the activities, progress, and status of the ESOH effort relative to the scheduled program milestones. The summary shall highlight significant achievements and issues. The summary shall also include progress toward completion of ESOH activities and documentation of data.

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

c. Individual hazard resolution status and the status of all recommended corrective actions that have not been implemented.

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

e. Discussion of contractor documentation reviewed by the ESOH effort staff during the reporting period. The discussion shall indicate whether the documents were acceptable for content and whether inputs to improve the safety posture were made.

f. Proposed agenda items for the next ESOH IPT/WG meeting, if such groups are established.

106.3. Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 106. (R)

b. Progress reporting period. (R)

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

TASK 107
HAZARDOUS MATERIALS MANAGEMENT PLAN

107.1. Purpose. The purpose of Task 107 is to develop a Hazardous Materials Management Plan. Hazardous materials management is an integral part of the ESOH hazard management effort that occurs within the program's SE process using the MIL-STD-882D w/CHANGE 1 methodology. The HMMP shall describe how the Government and contractor will coordinate activities required to eliminate or reduce HM (often through pollution prevention initiatives) in systems; system components; associated support items; required operations and support processes; and those which are generated during support, demilitarization, or disposal of the system. The HMMP, as described in this task, meets the requirements of National Aerospace Standard 411.

107.2. Task description. The HMMP will define Government and contractor roles, responsibilities, and procedures needed to accomplish HM management and tracking of contractual requirements included in the general and special provisions of the contract. The approved plan shall require item-by-item accounting for all contractually required tasks and responsibilities. At a minimum, the HMMP shall include HMs targeted for elimination and reduction; the process for approving HM usage where HM cannot be eliminated; the Government and contractor processes to properly identify, control, analyze, and track HM to protect human health, safety, and the environment and to support end user needs; and the list of HM contained within the system and required for the operation or support of the system.

107.2.1. HM identification. An HM is defined as any substance that, due to its chemical, physical, toxicological, or biological nature, causes safety, public health, or environmental concerns. The HMMP will describe the procedures and criteria that the Government and contractor will use, in an iterative process, to create an HM map for the system though identification of the HM contained within the system that are required for the operation or support of the system or are generated to support or dispose of the system. The HMMP will not include those HM used by the contractor for production or manufacturing processes unless mutually agreed upon by the Government and contractor. The HMMP will include a list of managed HMs for the system. Examples of criteria that the Government and contractor can use to identify HM to be included in this list and managed under the HMMP include, but are not limited to:

a. Materials covered pursuant to the Occupational Safety and Health Administration (OSHA) Hazard Communication Standard.

b. Materials covered pursuant to the Emergency Planning and Community Right-to-Know Act.

c. Materials covered pursuant to Section 112 of the Clean Air Act; Section 302.4 of the Comprehensive Environmental Response, Compensation, and Liability Act; Section 311(b)(2)(A) and Section 307(a) of the Federal Water Pollution Control Act; Section 3001 of the Resource, Conservation and Recovery Act; and Section 7 the Toxic Substances Control Act. These include materials that appear on a list of hazardous materials prepared by a Federal, state,

or local regulatory agency, or those that have characteristics defined as hazardous by such an agency.

d. Materials that must be routinely tracked or reported under Federal or state laws.

e. High profile materials (contract-specified).

f. Materials subject to statutory phase-outs or regulatory use restrictions because of operating in or with DoD deliverables (e.g., ozone depleting substances (ODS) and greenhouse gases).

g. Deliverable materials subject to special shipping requirements under Department of Transportation (DOT) regulations.

h. Radioactive materials.

i. Propulsion fuels, propellants, and explosives.

j. Materials identified as hazardous or toxic through other system safety analyses.

k. Materials that can become hazardous from combustion or breakdown during mishaps (e.g., fibers from composite materials).

l. Materials of evolving regulatory interest (e.g., emerging contaminants).

m. DoD Component-specified targeted toxic and hazardous materials and chemicals.

107.2.2. Categorization of identified HM. Working together, the Government and the contractor will categorize identified HM as prohibited, restricted, or tracked.

a. Prohibited HM are materials that require the contractor to obtain Government approval before those materials can be included in systems, subsystems, and support equipment or planned for system operations and support.

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

c. Tracked HM do not require specific contractor action other than inclusion in the hazard tracking system.

107.2.3. Modification of HM list or categorizations. Dialogue between the Government and the contractor will continue after the initial agreement to include HM in the hazard tracking system (HTS). Because of the shifting regulatory environment, materials may be added to the HTS or the categorization (prohibited, restricted, and tracked) of included materials may change, requiring additional contractor action. The HMMP will describe procedures for modifying the HM list and will provide procedures for requesting contract modifications, including price, if HM list modifications add to the cost of the program.

107.2.4. HM data tracking. The HMMP will describe how the contractor will integrate data required to manage HM with the data included in the hazard tracking system. At a minimum, the contractor will be required to track all identified HM in the hazard tracking system. The minimum additional data elements required for HM management and the hazard tracking system include:

a. Location of HM within the system during its entire lifecycle.

b. Quantity of HM within the system during its entire lifecycle.

c. Process or activity whereby quantities of HM are used or generated during operations, support, or disposal of the system.

d. Reasonably anticipated hazardous materials that are used or generated during the lifecycle of the system (e.g., installation, test and evaluation, normal use, maintenance or repair, and disposal of the system).

e. Reasonably anticipated hazardous materials to be used or generated in emergency situations (e.g., exhaust, fibers from composite materials released during accidents, combustion byproducts, etc.).

f. Special HM control, training, handling measures, and personal protective equipment needed, including provision of required MSDSs.

107.3. Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 107 to establish contractual HM management requirements as early in the program lifecycle as possible. (R)

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

c. Period of time for estimating quantities of HM use or generation.

TASK 201
PRELIMINARY HAZARD LIST

201.1. Purpose. The purpose of Task 201 is to compile a list of potential hazards considering all ESOH disciplines early in the system development.

201.2. Task description

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

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

a. Mishap and incident reports.

b. Hazard tracking databases.

c. ESOH lessons learned.

d. Demilitarization and disposal.

e. ESOH regulatory issues at potential locations for system testing, training, fielding/basing, and depot maintenance.

f. NEPA and Executive Order 12114 documentation.

201.2.3. The contractor shall document the identified hazards. Contents and formats will be as agreed upon between the contractor and the Program Manager. The following content requirements must be included, unless otherwise modified:

a. A brief description of the hazard.

b. The basis/causal factor for each identified hazard.

c. Any recommended actions to eliminate or mitigate the hazard.

201.3. Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 201. (R)

b. Guidance on how to obtain access to Government documentation.

c. Content and format requirements for the hazard list.

d. Operational environment.

TASK 202
PRELIMINARY HAZARD ANALYSIS

202.1. Purpose. The purpose of Task 202 is to provide an initial risk assessment of identified ESOH hazards.

202.2. Task description. The contractor shall perform and document a Preliminary Hazard Analysis (PHA) to obtain an initial risk assessment of a concept or system. Based on the best available data, including mishap data (as accessible) from similar systems, legacy systems, and other lessons learned, hazards associated with the proposed design or function shall be evaluated for hazard severity and probability. ESOH provisions, alternatives, and mitigation measures needed to eliminate hazards or reduce associated risk shall be included. At a minimum, the PHA shall consider the following for identification and evaluation of hazards:

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

b. Interface considerations among various elements of the system (e.g., material compatibilities, electromagnetic interference, inadvertent activation, fire/explosive initiation and propagation, and hardware and software controls) and to other systems when in a network or system-of-systems architecture. Include consideration of the potential contribution by COTS, non-developmental items, and software (including software developed by other contractors or sources) to subsystem or system mishaps. Design criteria to control safety-critical 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.

c. Operating environment constraints (e.g., drop; shock; vibration; extreme temperatures; noise; exposure to toxic substances; health hazards; fire; electrostatic discharge; lightning; electromagnetic environmental effects; and ionizing and non-ionizing radiation, including laser and radio-frequency radiation).

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

e. Those test-unique hazards that will be a direct result of the test and evaluation of the article or vehicle.

f. Built infrastructure, real property installed equipment, and support equipment (e.g., provisions for storage, assembly, and checkout; proof testing of hazardous

systems/assemblies that may involve toxic, flammable, explosive, corrosive, or cryogenic materials or wastes; pollution, radiation, or noise emitters; and electrical power sources).

g. Natural infrastructure (e.g., land use, water resources, air quality, geology and soils, biological resources, cultural resources, hazardous materials, solid and hazardous waste, environmental noise, and aesthetic and visual resources).

h. Training and certification.

i. ESOH controls, safeguards, and possible alternate approaches (e.g., interlocks; system redundancy; fail safe design considerations using hardware or software controls; subsystem protection; fire detection and suppression systems; personal protective equipment; heating, ventilation, and air-conditioning; noise or radiation barriers; and pollution control equipment).

j. Malfunctions of the system-of-systems, system, subsystems, or software. Each malfunction shall be specified, the cause-and-result sequence of events determined, the hazard assessed, and appropriate specification or design changes developed.

202.2.1. The contractor shall document the results of the PHA in a tracking system that shall be made available to the Government.

202.3. Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 202. (R)

b. Special data elements, format, or data reporting requirements (consider Task 105 (Hazard Tracking System)).

c. Identify any selected hazards, hazardous areas, or other specific items to be examined or excluded.

d. Select technical data on GFE to enable the contractor to accomplish the defined task.

e. Operational environment.

TASK 203
SAFETY REQUIREMENTS ANALYSIS

203.1. Purpose. The purpose of Task 203 is to develop and document the ESOH design requirements and criteria for a system or facility under development or design, and verify compliance with the appropriate design and operational requirements.

203.2. Task description. The Safety Requirements Analysis (SRA) relates the hazards identified to the system design and identifies or develops design requirements to eliminate or reduce the risk of the identified hazards. The SRA also is used to incorporate design requirements that are ESOH-related but are not tied to a specific hazard. The SRA uses the PHL (Task 201) or the PHA (Task 202) as a basis, if available. In addition, as part of the compliance verification efforts and as appropriate or available, the SRA uses the PHA, Functional Hazard Analysis (FHA), Subsystem Hazard Analysis (SSHA), System Hazard Analysis (SHA), and Operating and Support Hazard Analysis (O&SHA). At a minimum, the analysis includes the following efforts:

203.2.1. The contractor shall determine applicable ESOH design requirements and guidelines for facilities; hardware and software based on a review of Federal, military, national, state, and local regulations; military and industry standards and specifications; EOs and applicable international agreements; historical ESOH documentation on similar and legacy systems; DoD requirements (e.g., insensitive munitions and Class I ODS) and recommended ESOH technology considerations (e.g., MFOQA); system performance specifications; and other system design requirements and documents. The contractor shall incorporate these ESOH design requirements and guidelines into high-level system specifications and design documents, as appropriate. The SRA includes an assessment of the system throughout its lifecycle and includes testing, training, installation, fielding, and routine and emergency operations and maintenance activities at all respective locations. The contractor shall document compliance of the design and any training, operations, and support processes or procedures with the identified ESOH requirements.

203.2.2. The contractor shall analyze the system design requirements, system and subsystem specifications, preliminary hardware configuration item development specification, software requirements specifications, interface requirements specifications, and equivalent documents, as appropriate, including the following subtasks:

a. The contractor shall ensure that the ESOH design requirements and guidelines are developed, refined, correctly and completely specified, properly translated into system hardware and software requirements and guidelines where appropriate, and implemented into the design and development of the system hardware and associated software.

b. The contractor shall identify ESOH hazards, including hazardous materials, and relate them to the specifications or documents listed above. The contractor shall develop design requirements to reduce the risk of those hazards.

c. The contractor shall identify the safety requirements associated with interfaces at a gross level that may cause or contribute to potential hazards. At a minimum, interfaces identified shall include control functions, monitoring functions, and safety systems and functions that may have a direct or indirect impact on safety. These interfaces and associated software shall be designated as safety-related.

d. The contractor shall perform a preliminary risk assessment on the identified safety-related software functional requirements in accordance with Section 4 of this standard.

e. The contractor shall ensure that ESOH design requirements are incorporated into the operator, maintenance, user, training, logistics, diagnostic, and demilitarization and disposal manuals and plans.

203.2.3. The contractor shall develop ESOH-related design change recommendations and testing requirements and shall incorporate them into the design documents, hardware, software, and system test plans. The following subtasks shall be accomplished:

a. The contractor shall develop ESOH-related change recommendations for the design and specification documents listed above and shall include a means of verification for each design requirement.

b. The contractor shall develop ESOH-related test requirements to incorporate into the test planning and documentation.

203.2.4. The contractor shall address ESOH requirements at all contractually required technical reviews, including design reviews (such as PDR and CDR) and the Software Specification Review. The contractor shall address the ESOH effort, analyses performed and to be performed, significant hazards identified, hazard resolutions or proposed mitigations, means of verification, and recommendations for hazards ready for closure.

203.2.5. As the program matures, the contractor shall also document compliance of the design, training, operations, and support processes and procedures with the identified ESOH requirements. This effort includes verification of required specialized devices, training, procedures, facilities, support requirements, and PPE.

203.3. Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 203. (R)

b. Level of contractor support required for design and other program and technical reviews. (R)

c. Operational environment.

TASK 204
SUBSYSTEM HAZARD ANALYSIS

204.1. Purpose. The purpose of Task 204 is to perform and document a Subsystem Hazard Analysis to verify subsystem compliance with safety requirements contained in subsystem specifications and other applicable documents; identify previously unidentified hazards associated with the design of subsystems, including component failure modes, critical human error inputs, and hazards resulting from functional relationships between components and equipment comprising each subsystem; and recommend actions necessary to eliminate identified hazards or mitigate their associated risk.

204.2. Task description. The contractor shall perform and document an SSHA to identify all components and equipment that could result in a hazard or whose design does not satisfy contractual system safety requirements relating to all safety areas, including ESOH. This element shall include GFE, 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 determine:

a. Modes of failure, including reasonable human errors, single point and common mode failures, and the ESOH effects when failures occur in subsystem components.

b. Potential contribution of hardware and software events (including those developed by other contractors/sources, GFE, or COTS hardware or software), faults, and occurrences (such as improper timing) on the ESOH aspects of the subsystem.

c. ESOH design criteria in the hardware, software, and facilities/installation specifications have been satisfied.

d. The method of implementing hardware, software, and facilities/installation design requirements and corrective actions has not impaired or decreased the safety of the subsystem, nor introduced any new hazards or risks.

e. Implementation of ESOH design requirements from top-level specifications to detailed design specifications for the subsystem. Analyze ESOH design requirements, such as those developed as part of the PHA and SRA, to ensure they satisfy the intent of the requirements.

f. Test plan and procedure recommendations to integrate testing of the hardware and software components.

g. System-level hazards attributed to the subsystem are analyzed and adequate mitigation of the potential hazard is implemented in the design.

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, 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 other software development documents, the contractor performing the SSHA shall monitor, obtain, and use the output of each phase of the formal software development process in evaluating the software contribution to the SSHA. Problems identified that require the reaction of the software developer shall be reported to the PM in time to support the ongoing phase of the software development process.

204.2.4. The contractor shall update the SSHA following any system design changes, including software design changes that affect ESOH aspects.

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

204.2.5.1. System description. This summary describes the physical and functional characteristics of the system and its components. Reference to more detailed system and component descriptions, including specifications and detailed review documentation, shall be supplied when such documentation is available. The capabilities, limitations, and interdependence of these components shall be expressed in terms relevant to system safety, including ESOH. The system and components shall be addressed with respect to the mission and the operational environment. System block diagrams or functional flow diagrams may be used to clarify system descriptions. Software, its role(s), the scope and physical boundaries, and assumptions shall be included in this description.

204.2.5.2. Hazard Analysis Results. The results will include a summary and a total listing of the hazard analysis. Contents and formats may vary according to the individual requirements of the program. The content and format requirements for hazard analysis results include:

a. A summary of the results.

b. A listing of identified hazards, including:

(1) Hazard.

(2) Life-cycle phases affected by the hazard.

(3) Causal factor (e.g., hardware, software, and human).

(4) Effects.

(5) Mishap.

(6) Initial RAC and associated risk category.

(7) Target RAC and associated risk category.

(8) Residual RAC and associated risk category.

(9) System.

(10) Subsystem.

(11) System component. The particular system element that concerns the analysis and includes defining the system/subsystem/component configuration the system is in when the hazard is encountered.

(12) Requirements references

(13) Mitigation measures.

(14) Hazard status (e.g., open or closed).

(15) Hazard traceability (running history of actions taken or planned with rationale to mitigate risks).

(16) Remarks. Summarizes the data used for the analysis and provides any information relating to the hazard not already addressed in the previous sections.

204.3. Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 204. (R)

b. Minimum RAC and risk category reporting requirements. (R)

c. Desired analysis technique(s) and any special data elements, format, or data reporting requirements.

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

e. Select GFE technical data to enable the contractor to accomplish the defined task.

f. Operational environment.

TASK 205
SYSTEM HAZARD ANALYSIS

205.1. Purpose. The purpose of Task 205 is to perform and document a System Hazard Analysis to verify system compliance with ESOH requirements contained in system specifications and other applicable documents; identify previously unidentified hazards associated with the subsystem interfaces and faults; assess the risk associated with the integrated system design, including software and subsystem interfaces; and recommend necessary actions to eliminate identified hazards or mitigate their associated risk.

205.2. Task description. The contractor shall perform and document a SHA to identify hazards and assess the risk of the integrated system design, including software and subsystem interfaces.

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

a. Compliance with specified ESOH design criteria.

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

c. Degradation of a subsystem or the total system affecting ESOH.

d. Design changes that affect subsystems.

e. Effects of reasonable human errors.

f. Determination:

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

(2) That ESOH design criteria in the hardware, software, and facilities/installation specifications have been satisfied.

(3) That the method of implementing the hardware, software, and facilities/installation design requirements and corrective actions have not introduced any new hazards or negatively impacted ESOH-related aspects of the system.

205.2.2. If no specific analysis techniques are directed or if the contractor recommends a different technique than the one specified by the PM, the contractor shall obtain PM approval of techniques to be used before performing the analysis. The SHA may be combined with or performed using similar techniques to those used for the FHA and Subsystem Hazard Analysis.

205.2.3. When software to be used within the system is being developed under other software development requirement documents, the contractor performing the SHA shall monitor, obtain, and use the output of each phase of the formal software development process in evaluating the software contribution to the SHA. Problems identified that require the reaction of the software developer shall immediately be reported to the PM.

205.2.4. The contractor shall update the SHA following any system design changes, including software design changes that affect system safety across all ESOH disciplines.

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

205.2.5.1. System description. The system description provides the physical and functional characteristics of the system and its components. Reference to more detailed system and component descriptions, including specifications and detailed review documentation, shall be supplied when such documentation is available. The capabilities, limitations, and interdependence of these components shall be expressed in terms relevant to ESOH. The system and components shall be addressed with respect to the mission and the operational environment. System block diagrams or functional flow diagrams may be used to clarify system descriptions. Software, its role(s), the scope and physical boundaries, and assumptions shall be included in this description.

205.2.5.2. Hazard analysis results. The results will consist of a summary and a total listing of the hazard analysis. Contents and formats may vary according to the individual requirements of the program. The content and format requirements for hazard analysis results include:

a. A summary of the results.

b. A listing of identified hazards, including:

(1) Hazard.

(2) Life-cycle phases affected by the hazard.

(3) Causal factor (e.g., hardware, software, and human).

(4) Effects.

(5) Mishap.

(6) Initial RAC and associated risk category.

(7) Target RAC and associated risk category.

(8) Event RAC and associated risk category.

(9) Residual RAC and associated risk category.

(10) Mitigation measures.

(11) Hazard status (e.g., open or closed).

(12) Hazard traceability (running history of actions taken or planned with rationale to mitigate risks).

(13) Remarks. Summarizes the data used for the analysis and provides any information relating to the hazard not already addressed in the previous sections.

205.3 Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 205. (R)

b. Minimum RAC and risk category reporting requirements. (R)

c. Desired analysis technique(s) and any special data elements, format, or data reporting requirements.

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

e. Select GFE technical data to enable the contractor to accomplish the defined task.

f. Operational environment.

TASK 206
OPERATING AND SUPPORT HAZARD ANALYSIS

206.1. Purpose. The purpose of Task 206 is to perform and document an Operating and Support Hazard Analysis, evaluate activities for hazards or risks introduced into the system by operational and support activities and procedures, and evaluate the adequacy of operational and support procedures, facilities, processes, and equipment used to eliminate or mitigate identified hazards.

206.2. Task description. The contractor shall perform and document an O&SHA to examine procedurally controlled activities. The O&SHA builds on the hazard analyses and typically begins during Engineering and Manufacturing Development (EMD). The O&SHA identifies and evaluates hazards resulting from implementing operations or tasks that individuals perform, and considers the planned system configuration/state at each phase of activity; the facility/installation interfaces; the planned operation and maintenance environments; the supporting tools or other equipment, including software-controlled automatic test equipment specified for use; operational/task sequence, concurrent task effects, and limitations; biotechnological, regulatory, or contractually specified personnel ESOH requirements; and the potential for unplanned events, including hazards introduced by human errors. The human shall be considered an element of the total system, receiving both inputs and initiating outputs within the analysis. The O&SHA shall identify the ESOH requirements (or alternatives) needed to eliminate or mitigate identified hazards and reduce the associated risk.

206.2.1. At a minimum, the analysis shall identify:

a. Activities that occur under hazardous conditions, time periods, approximate frequency and numbers of personnel involved, and the actions required to minimize risk during these activities/time periods.

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

c. Requirements for engineered features, devices, and equipment (e.g., pressure release valve, PPE, paint booth, scrubber, and automatic laser shut-off).

d. Warnings, cautions, and special emergency procedures (e.g., egress, rescue, escape, render safe, explosive ordnance disposal (EOD), spill cleanup, and back-out), including those necessitated by failure of a computer software-controlled operation to produce the expected and required safe result or indication.

e. Requirements for packaging, handling, storage, transportation, maintenance, and disposal of hazardous and toxic materials and hazardous wastes.

f. Requirements for ESOH training and personnel certification.

g. Effects of nondevelopmental and COTS hardware and software across the interface with other system components or subsystems.

h. Potentially hazardous system states under operator control.

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

206.2.2. The O&SHA shall document ESOH assessments of all procedures involved in the system, including production, deployment, installation, assembly, test, operation, maintenance, servicing, transportation, storage, modification, demilitarization, and disposal.

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, 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 any system design or operational changes.

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

206.2.5.1. System description. This summary describes the physical and functional characteristics of the system and its components. Reference to more detailed system and component descriptions, including specifications and detailed review documentation, shall be supplied when such documentation is available. The capabilities, limitations, and interdependence of these components shall be expressed in terms relevant to ESOH. The system and components shall be addressed with respect to the mission and the operational environment. System block diagrams or functional flow diagrams may be used to clarify system descriptions. Software, its role(s), the scope and physical boundaries, and assumptions shall be included in this description.

206.2.5.2. Hazard analysis results. The results will consist of a summary and a total listing of the hazard analysis. Contents and formats may vary according to the individual requirements of the program. The content and format requirements for the hazard analysis results follow:

a. A summary of the results. Data may include a summary of past evaluations of related legacy systems and their support operations, such as safety, industrial hygiene, environmental, ergonomic surveys, and reliability evaluations.

b. A listing of identified hazards, including:

(1) Hazard.

(2) Life-cycle phases affected by the hazard.

(3) Causal factor (e.g., hardware, software, and human).

(4) Mishap.

(5) Effects.

(6) Initial RAC and associated risk category.

(7) Target RAC and associated risk category.

(8) Event RAC and associated risk category.

(9) Residual RAC and associated risk category.

(10) Mitigation measures.

(11) Hazard status (e.g., open or closed).

(12) Hazard traceability (running history of actions taken or planned with rationale to mitigate risks).

(13) Verification and validation method.

(14) Action person(s) and organizational element.

(15) Record of risk acceptance(s), including 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).

(16) Remarks. Summarizes the data used for the analysis and provides any information relating to the hazard not already addressed in the previous sections.

(17) Caution and warning notes. A complete list of warnings, cautions, and procedures required in operating and maintenance manuals and for training courses.

206.3. Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 206. (R)

b. Minimum reporting requirements. (R)

c. Desired analysis technique(s) and identification of any special data elements, format, or data reporting requirements.

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

e. Select GFE technical data to enable the contractor to accomplish the defined task.

f. Legacy and related processes and equipment to be reviewed, including previous job hazards or other risk evaluations completed.

g. 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 (HHA)).

h. Operational environment.

TASK 207
HEALTH HAZARD ANALYSIS

207.1. Purpose. The purpose of Task 207 is to perform and document a Health Hazard Analysis to identify human health hazards, evaluate proposed hazardous materials and processes using such materials, and propose protective measures to reduce the associated risks to a level acceptable to the Program Manager.

207.2. Task description. HHAs are evaluations of the potential ESOH effects resulting from exposure to a hazard or hazards. HHAs incorporate the identification, assessment, characterization, control, and communication of potential 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, pose substantial present or future danger to the environment, or result in damage to or loss of equipment or property during the system lifecycle. The analysis shall include consideration of the generation of hazardous wastes.

207.2.1. A health hazard is an existing or likely condition, inherent to the operation, maintenance, prolonged storage, transport, or use of materiel, 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, and ionizing and non-ionizing radiation).

c. Biological hazards (e.g., bacteria, viri, 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 introduction of the system or by the manufacture, test, maintenance, operation, or final disposal/recycling of the system.

f. Non-ionizing radiation hazards. Provide a listing of all non-ionizing (radio frequency and laser) transmitters contained in the system. List all parameters required to determine 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 ionizing radiation sources, including isotope, quantity, activity, and potential hazards based on the incorporation of the radioactive source into the system design.

207.2.2. The HHA for a hazardous agent or process shall provide the following categories of information:

a. Hazard identification. Identify the hazardous agents by name(s) 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.

(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.

b. Severity and probability. Estimate hazard severity, probability, and Risk Assessment Code using the process described in Section 4. 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 residual RAC for each hazard based on the degree of hazard reduction achievable by the mitigation.

207.2.3. In addition to the information required in Section 207.2 above, the following sections describe the HHA or part of the HHA that provides HM evaluation, ergonomics evaluation, or describes the operational environment.

207.2.3.1. The HHA or part of the HHA providing HM evaluation, in addition to the information required in Section 207.2 above, shall:

a. Identify the HM by quantity, characteristics, and concentrations of the materials in the system. Identify source documents, such as MSDSs, and information from vendors and

subvendors for components of systems and subsystems. At a minimum, material identification includes material identity, common or trade names, chemical name, Chemical Abstract Service 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 HM information resource system).

b. Characterize material hazards, including hazardous waste, and determine reference quantities and hazard ratings. Examine acute health, chronic health, carcinogenic, contact, flammability, reactivity, and environmental hazards.

c. Estimate the expected use rate of each HM for each process or component for the subsystem, total system, and program-wide impact.

d. Recommend the disposition for each HM (to include hazardous waste) identified. If, for any scale of operation, the reference quantity is exceeded by the estimated usage rate, 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 Section 207.2 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, that personnel will 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 customer’s 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, reducing non-neutral postures, 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 Section 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. This information can be used to support the Preliminary Hazard Analysis.

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. Identify the potential for generation of external airborne and waterborne noise signatures, if these are anticipated, to allow detection, identification, and tracking by hostile forces. This information may be used to support the PHA.

c. 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.

d. 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) Potential alternative processes and equipment, where such are available.

(4) 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.

e. 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 MIL-STD-1474 or 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 systems (e.g., back, kidneys, hands, arms, and head) should be identified and the likelihood of discordant motions should be described. This information can be used to refine the PHL.

f. 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 must describe the optimal (design) and anticipated effective noise reduction and vibration reduction of the protective equipment. Document the methodology and assumptions made in calculations.

g. 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.

h. Identify the residual potential for generation of external airborne and waterborne noise signatures after mitigation of noise emissions and associated external signature, if these factors are anticipated, to allow detection, identification, and tracking by hostile forces. Use information to support the final hazard assessment and risk acceptance.

i. The HHA or part of the HHA providing nonionizing radiation evaluation, in addition to the information required in Section 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 DODI 6055.11, *Protection of DoD Personnel from Exposure to Radiofrequency Radiation and Military Exempt Lasers*.

207.2.4. References. A list of source materials used in preparing the report may include Government and contractor reports, standards, criteria, technical manuals, and specifications. If references are numerous, place them in a bibliography as an appendix. References that may be used include:

a. Military Standard 1472F, *Department of Defense Design Criteria Standard for Human Engineering*.

b. Military Standard 1474D, *Department of Defense Design Criteria Limit Noise Limits*.

c. DODI 6055.12, *Department of Defense Hearing Conservation Program*.

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

e. 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).

f. 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.

g. ISO 5349, *Guide for the Measurement and the Assessment of Human Exposure to Hand Transmitted Vibration*.

h. *Threshold Limit Values for Chemical Substances and Physical Agents and Biological Exposure Indices for 2008* (or the latest version), American Conference of Governmental Industrial Hygienists.

i. U.S. Air Force Manual 48-153, *Health Risk Assessment*.

j. *U.S. Army Health Hazard Assessors Guide*, U.S. Army Center for Health Promotion and Preventive Medicine.

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

l. Army Regulation 40-10, *Health Hazard Assessment Program in Support of the Army Acquisition Process*.

m. Department of the Army Pamphlet 40-501, *Army Hearing Conservation Program*.

n. Navy and Marine Corps Public Health Center Technical Manual 6260.51.99-2.

o. Marine Corps Order 6260.1E, *Marine Corps Hearing Conservation Program*.

p. Navy Bureau of Medicine and Surgery Instruction 6270.8A, *Obtaining Health Hazard Assessments*.

q. OSHA 29 Code of Federal Regulations 1910.1200, *Hazard Communication*.

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

s. MIL- HDBK-46855, *Human Engineering Program Process and Procedures*.

t. Department of Defense Handbook 743, *Anthropometry of U.S. Military Personnel (Metric)*.

u. MIL-HDBK-1908, *Definitions of Human Factors Terms*.

v. MIL-STD-464, *Electromagnetic Environmental Effects Requirements for Systems*.

w. MIL-STD-1425, *Safety Design Requirements for Military Lasers and Associated Support Equipment*.

x. MIL-HDBK-454, *General Guidelines for Electronic Equipment*.

207.3. Details to be specified. Details to be specified in the RFP and 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. Any selected hazards, hazardous areas, hazardous materials, or other specific items to be examined or excluded.

c. Any special analysis techniques, data elements, format, or data reporting requirements (see Table I).

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

e. Standards and criteria for acceptable exposures and controls.

f. Mandatory references, including specific issue dates.

g. Operational environment.

TASK 208
FUNCTIONAL HAZARD ANALYSIS

208.1. Purpose. The purpose of Task 208 is to perform and document a Functional Hazard Analysis 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. These consequences will be classified in terms of severity for the purpose of identifying the SCFs, SCIs, FSCAPs, SSFs, and safety-significant items (SSIs) of the system. SCFs, SCIs, FSCAPs, SSFs, and SSIs 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 other ESOH-related consequences of functional failure or malfunction (e.g., failure of a seal resulting in a spill of a hazardous material). The initial FHA should be accomplished as early as possible in the 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, FSCAPs, SSFs, and SSIs; allocate and partition SCFs and SSFs in the software design architecture; and identify ESOH requirements and constraints to the design team.

208.2. Task description. The contractor shall perform and document an FHA to obtain an initial ESOH assessment of a concept or system. Functions associated with the proposed functional or physical design shall be analyzed 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, consequence of functional failure, and the severity assessment for each consequence. The risk acceptance authority shall determine the ESOH requirements and constraints needed to mitigate the risk. At a minimum, the FHA shall consider the following to identify and evaluate functions within a system:

a. Hardware components (the physical decomposition of the system and its related subsystems to the major component level). Hardware decomposition identifies a majority of the system's functionality. However, once the hardware is accounted for, software "managers" (i.e., software dedicated to managing particular features of a system, such as weapons managers, device managers, display managers, bus managers, etc.) will need to be identified to account for the functionality missed in the hardware assessment.

b. A functional description of each physical subsystem and component identified. Each physical subsystem and component will possess one or more functional attributes.

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

d. A functional description of interfaces between subsystems and components.

e. The safety consequences of loss of function, degraded function or malfunction, or functioning out of time or out of sequence for the physical subsystems, components, and interfaces. In a manner similar to a Failure Modes and Effects Analysis (FMEA), the list of

safety ramifications should consider the next effect in a possible mishap sequence and the final mishap outcome.

f. An assessment of the severity of the outcome associated with each identified failure of a function, subsystem, or component in terms of the severity categories defined in the SSEP. During this stage of the FHA, the assessment should only consider severity.

g. Identification of functions with an assessed severity of either Catastrophic or Critical (which are, by definition, safety-critical functions). Physical items or system functions with assessed mishap severities of Marginal or Negligible are considered "safety significant." Hardware and software supporting SCFs are normally identified as safety critical. Using SCI and SSI terms is helpful for traceability purposes within the design architecture and for assisting in the identification of systems engineering requirements.

h. 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 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).

i. An assessment of Software Control Category (SCC) for each SRSF. Safety-related software functions encompass both safety-critical and safety-significant software functions. Assign an SwCI for each SRSF mapped to the software design architecture.

j. A list of safety requirements and safety constraints for the design team (to be included in the specifications) that, when successfully implemented, will reduce the likelihood of mishap occurrence for hazards later identified in the PHA, SSHA, SHA, O&SHA, and HHA. These requirements should be in the form of hazard mitigation, fault tolerance, detection, isolation, annunciation, or recovery.

208.2.1. Report requirements. The contractor shall prepare a report that contains the results from the task described in paragraph 208.2 and includes the following information:

208.2.1.1. Results. At a minimum, the FHA should produce:

a. A physical and functional decomposition of the system (or system-of-systems). A work breakdown structure (WBS) format works well to account for all critical subsystems and components. (R)

b. A list of system functions. (R)

c. A list of SCFs (having Catastrophic or Critical severity consequence), items, and parts. (R)

d. A mapping of SCFs to the hardware and software design architectures. The SCF list and subsequent mapping will also be used as inputs to reliability, integrity, assurance, and quality planning. (R)

e. An assessment of SCC and SwCI for SRSFs allocated to the software design. (R)

f. A list of ESOH requirements and constraints of the system based on the severity of loss of function or malfunction. (R)

g. A list of other ESOH-critical functions (having Catastrophic or Critical severity consequence) and items. (R)

h. The FHA can further produce:

(1) A list of preliminary hazards for the PHL/PHA.

(2) Inputs to the FMEA.

(3) Methods to verify compliance with specific failure conditions or scenarios. For aircraft-related programs, Society of Automotive Engineers Recommended Practice 4761 provides guidance for defining the necessary safety objective verification approach for the relevant failure conditions.

(4) Identification and design status of SCI/SSI interfaces of the system.

(5) Remarks.

208.2.2. Completion criteria. The FHA is a living document that requires updating as system functions are added, deleted, or modified within the acquisition lifecycle. The generation of the FHA with its subsequent SCF, SCI, FSCAP, and SSI lists is an iterative task that begins prior to PDR. The document and its subsequent lists are finalized at CDR, but will require updates as changes are introduced into the system through the configuration change control process.

208.3. Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 208. (R)

b. Special data elements, format, and data reporting requirements. (R)

c. SRSF, SCF, SCI, FSCAP, SSI, and other ESOH-critical functions. (R)

d. Applicable requirements, specifications, and standards.

e. Operational environment.

TASK 209
SYSTEM-OF-SYSTEMS INTEGRATION AND INTEROPERABILITY HAZARD ANALYSIS

209.1. Purpose. The purpose of Task 209 is to analyze the system within the context of its system-of-systems for emergent hazards not found in other hazard analyses. This task will produce special requirements and tests to identify, eliminate, transfer, or mitigate hazards which otherwise would not emerge in general use of the system by itself.

209.2. Task description.

209.2.1. The contractor shall assess the architectures and systems context for the system and systems interfacing with it, integrating into or around it, and those systems with which it is interoperating with or through.

209.2.2. To the extent specified in the contract, the contractor shall analyze and test against the architectures provided. The adjacent, integrating, or interoperating architectures shall be analyzed for causal factors inducing emergent hazards within or nearby the system under development. The contractor shall also assess adjacent, integrating, and interoperating architectures and systems for hazardous scenarios which the system under development may induce or cause to emerge in those systems or architectures.

209.3. Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 209. (R)

b. Complete architectures for software, physical hardware, and locations. (R)

c. For the system under development, identify architectures and systems which are adjacent and those systems which will integrate or interoperate with the system under development. Include probable location(s) and distance(s) of the system under development and other systems-of-systems. (R)

d. Traceability of all emergent hazards to architecture locations, interfaces, data, and the system's stakeholder associated with each hazard. (R)

e. Operational testing, models and simulations, and development tests shall incrementally demonstrate that the emergent hazard(s) present an acceptable risk(s).

f. Operational environment.

TASK 210
ENVIRONMENTAL HAZARD ANALYSIS

210.1. Purpose. The purpose of Task 210 (Environmental Hazard Analysis) is to support design development decisions by identifying potential hazards to the natural environment resulting from the development, testing, deployment, maintenance and disposal of a system; supporting risk acceptance decisions for environmental hazards; and providing the system-specific data to support NEPA and EO 12114 requirements.

210.2. Task description. Influencing design decisions is important to integrating environmental considerations into the system because it is typically the most cost-effective means of effecting change in an acquisition program. 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, training ranges, and operational training units.

210.2.1. The elimination or reduction of environmental risk with an informed and structured risk assessment and acceptance process is essential for positively contributing to a program's efforts in meeting the system's life-cycle cost, schedule, and performance requirements. Early identification and resolution of ESOH hazards into the systems engineering process provides decision makers with a more complete and relevant picture of the potential risks associated with the test, operation, sustainment, and disposal of a system and will help mitigate the risk of unplanned technical, schedule, and cost impacts. The ESOH risk management process uses risk analysis matrices based on the requirements in this standard. The risk matrices define probability and severity criteria to categorize environmental risks for identified environmental hazards.

210.2.2. Using the system safety process and risk matrices. The system safety process shall be used across the ESOH disciplines to identify hazards and eliminate or mitigate risks through the systems engineering process. When assessing environmental hazards, the 8-step system safety process in Section 4 of this standard shall be followed. The severity and probability of potential mishap(s) for each hazard shall be assessed using the matrices in Tables I, II, and III of this standard unless tailored matrices have been formally approved for use by the program. Severity shall consider how the system will be operated. In addition, the analysis shall identify and quantify hazardous materials used in or generated throughout the system lifecycle and shall outline potential environmental impacts associated with the system's operation. When determining hazard mitigations, the hazard assessments should consider the mitigation impact to all three ESOH disciplines, as well as other applicable systems engineering disciplines, to identify the optimal ESOH mitigation for hazard(s). This will prevent mitigation measures from being optimized for only one of the ESOH disciplines, which could create hazards in other ESOH disciplines.

210.2.3. Environmental risks. There are three basic types of environmental risks:

a. Potential environmental impacts and adverse effects from routine system development, testing, training, operation, sustainment, maintenance, and demilitarization and disposal.

b. Potential environmental and mission readiness impacts from system failures or mishaps.

c. System life-cycle costs, schedule, and performance impacts from environmental compliance requirements.

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

a. Environmental hazard analysis data and information, risk assessments, and lessons learned from legacy and similar systems.

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

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

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

e. Demilitarization and disposal of legacy and similar systems.

f. ESOH regulatory issue mitigations at legacy and similar system locations and potential locations for system testing, training, and fielding/basing.

g. Programmatic ESOH Evaluation (PESHE) and NEPA documents from legacy and similar systems.

h. PHL/PHA for the system under development.

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

210.2.3.2. Environmental analysis considerations. The scope of environmental analysis should consider the entire system lifecycle and address hazards, risks, and mitigations associated with, but not limited to:

a. Hazardous materials use and generation.

b. Demilitarization and disposal requirements.

c. Exposure to chemical, biological, and other hazards impacting public health.

d. Environmental effects on sea, air, and land resources and ecosystems relative to NEPA and E.O. 12114 compliance.

e. Airborne noise generation resulting from the normal operation of the system.

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

g. Release of hazardous substances incidental to the routine maintenance and operation of the system.

h. Inadvertent releases.

210.2.4. Environmental analysis reporting requirements. Data shall be provided to identify all features of the system with the potential to cause environmental risks associated with the system during future tests, training, non-combat activities, maintenance, and disposal, including all elements captured in the ESOH hazard tracking system:

a. Hazard.

b. Life-cycle phases affected by the hazard.

c. Causal factor (e.g. hardware, software, and human).

d. Mishap.

e. Initial RAC and associated risk category.

f. Target RAC and associated risk category.

g. Event RAC and associated risk category.

h. Residual RAC and associated risk category.

i. Mitigation measures.

j. Hazard status (e.g., open or closed).

k. Hazard traceability (running history of actions taken or planned with rationale to mitigate risks).

l. Verification and validation method.

m. Action person(s) and organizational element.

n. Record of risk acceptance(s), including 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).

210.2.4.1. If hazards are associated with HM, the following additional data fields should be included in the hazard tracking system:

a. Location of HM imbedded in the system.

b. Quantity of HM imbedded in the system.

c. Reasonably anticipated hazardous materials that are used or generated during the lifecycle of the system (e.g., installation, test and evaluation, normal use, maintenance or repair, and disposal of the system).

d. Process/activity whereby quantities of HM are used or generated during operations, support, or disposal of the system.

e. Reasonably anticipated HM to be used or generated in emergency situations (e.g., exhaust, nanomaterials, fibers from composite materials released during accidents, combustion byproducts, etc.).

f. Special HM control, training, handling measures, personal protective equipment, required MSDSs, etc.

210.2.4.2. If hazards are associated with pollutant (including noise) generation, the following additional data fields should be included in the hazard tracking system:

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

b. Sources of emission for each pollutant.

c. Quantity and 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. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 210. (R)

b. Minimum reporting requirements. (R)

c. Desired analysis technique(s) and any special data elements, format, or data reporting requirements.

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

e. Locations to consider when assessing severity and regulatory compliance considerations.

f. Concept of normal operation and maintenance of the system.

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

h. Operational environment.

TASK 301
SAFETY ASSESSMENT REPORT

301.1. Purpose. The purpose of Task 301 is to perform and document a comprehensive evaluation of the risk being assumed prior to test or operation of a system, before the next contract phase, or at contract completion.

301.2. Task description.

301.2.1. The contractor shall perform and document a safety assessment to identify all safety features of the hardware, software, and system design and identify procedural, hardware, and software-related hazards that may be present in the system being acquired. This documentation shall include specific procedural controls and precautions to be followed. The contractor shall identify HM that are used in the design, operation, or maintenance of the system or will be generated by the system, and assess why a less hazardous material could not be used.

301.2.2. Report requirements. The contractor shall prepare a SAR that contains the results from the task described in paragraph 301.2.1 and includes the following information:

a. The safety criteria and methodology used to classify and rank hazards, plus any assumptions on which the criteria or methodologies were based or derived.

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

(1) Determining those hazards that still have an associated risk and the actions that have been taken to reduce the risk to a level contractually specified as acceptable.

(2) Examining the results of tests conducted to validate safety criteria, requirements, and analyses.

(3) Examining results of the safety efforts. Include a list of all significant hazards, along with specific recommendations for mitigation measure(s) required to ensure the safety of personnel, property, and the environment. Categorize the list of hazards to determine whether they may be expected under normal or abnormal operating conditions.

c. Any HM contained within the system and required for the operations and support of the system, including:

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

(2) Safety precautions and procedures necessary during use, packaging, handling, storage, transportation, and disposal. Include all explosives hazard classifications and EOD requirements.

(3) After launch safety-related activity of expendable launch vehicles and their payloads, including deployment, operation, reentry, and recovery (if required) which do not attain orbit (either planned or unplanned).

(4) Orbital safety hazard awareness associated with space systems, such as explosions, electromagnetic interference, radioactive sources, ionizing radiation, chemicals, space debris, separation distances between space vehicles, and natural phenomena.

(5) A copy of the MSDS (OSHA form or equivalent manufacturer format).

d. A statement summarizing the residual risks in the system.

e. A statement addressing the system's readiness to test, operate, and proceed to the next acquisition phase. In addition, include recommendations applicable to hazards at the interface of the system with the other systems.

f. References. 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. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 301. (R)

b. The specific purpose of the requested assessment report.

TASK 302
ESOH IN TEST AND EVALUATION

302.1. Purpose. The purpose of Task 302 is to ensure ESOH considerations are included as part of test and evaluation; to provide existing analysis, data, and reports; and to respond to all ESOH requirements necessary for testing in-house, at other contractor facilities, and at Government ranges, centers, or laboratories.

302.2. Task description. The contractor shall ensure that test and evaluation safety activities recommend actions and assess actions taken to eliminate or mitigate Catastrophic and Critical hazards in the test and evaluation environment. Marginal or Negligible hazards shall be addressed, as required by the PM. This task also encompasses specific ESOH efforts germane to ground or airborne/flight systems and launch requirements.

302.2.1. Test and evaluation planning. Specific test and evaluation system safety activities, considering all ESOH disciplines, will be conducted through the system's life cycle/contract period and shall incorporate, at a minimum, the following:

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

b. A schedule for analysis, evaluation, and approval of test plans, procedures, and other documents to ensure ESOH considerations are addressed during all testing.

c. ESOH preparation/input for test and operating procedures.

d. Analysis of hazards associated with test equipment, installation of test equipment, and instrumentation prior to test start.

e. The mechanism to inform the Program Manager of any identified hazards that are unique to the test environment.

f. Coordination and status reviews with test site ESOH representatives to ensure test ESOH requirements are identified, monitored, and completed as scheduled.

g. Completion of environmental analysis and documentation pursuant to DoD Service-specific NEPA and EO 12114 requirements.

h. PM-designated specialized requirements.

302.2.2. Safety reviews. Provide assistance to the safety review teams to the extent necessary to support a system safety certification process and validate from a safety perspective that the system is ready to test. This effort includes formal acceptance, in accordance with DoD policy, of all ESOH event risks associated with the test event(s).

302.2.3. Follow-up actions.

a. Analyze and document ESOH-related test results.

b. Initiate follow-up action to ensure completion of the corrective efforts taken to eliminate or mitigate test and evaluation hazards.

302.2.4. Reports. Maintain a repository of test and evaluation hazard and action status reports.

302.3. Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 302. (R)

b. Applicable specialized ESOH requirements for testing or use of range facilities. (R)

c. Schedule for meeting requirements designated in paragraph 302.2. (R)

TASK 303
REVIEW OF ENGINEERING CHANGE PROPOSALS, SPECIFICATION CHANGE NOTICES, SOFTWARE PROBLEM REPORTS, MISHAP INVESTIGATIONS, AND REQUESTS FOR DEVIATION/WAIVER

303.1. Purpose. The purpose of Task 303 is to perform and document analyses of Engineering Change Proposals (ECPs), Specification Change Notices (SCNs), Software Problem Reports (SPRs), Software Trouble Reports (STRs), and Class A and B mishap investigations. Task 303 also includes requests for deviations, waivers, and related change documentation to determine the ESOH impacts on the system.

303.2. Task description.

303.2.1. Engineering change proposals. The contractor shall analyze each ECP (as specified by the PM) to determine the associated hazards, assess the associated risk, and predict the ESOH impact of the ECP on the existing system. The contractor shall notify the PM of any detrimental impacts.

303.2.2. Specification change notices. The contractor shall analyze each SCN to determine the potential impact on ESOH-critical components or subsystems and notify the PM of any detrimental impacts.

303.2.3. Software problem reports. The contractor shall review each SPR to determine potential ESOH implications. If negative ESOH impacts are identified, the contractor shall notify the PM.

303.2.4. Program or software trouble reports. The contractor shall review each STR to determine potential ESOH implications. If negative ESOH impacts are identified, the contractor shall notify the PM.

303.2.5. Class A and B mishaps. The contractor shall review appropriate Class A and B mishaps from similar systems to refine risk analysis and identify emerging hazards.

303.2.6. Requests for deviation/waiver. The contractor shall analyze each request for deviation or waiver to determine the hazards and assess the risk of the proposed deviation from a requirement or specified method or process. The change in the risk involved in accepting the deviation or waiver shall be identified. The contractor must notify the PM when a deviation or waiver, method, or process detrimentally affects the system.

303.2.7. Report requirements. The contractor shall prepare a report that explains the results of the task described in paragraph 303.2.

303.3. Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 303. (R)

b. Amount of change requiring PM notification and the method and timing of such notification.

c. Class of ECP or type of deviation or waiver to which this task applies.

d. The individual who shall execute review and sign-off authority for each class of ECP or type of deviation or waiver.

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

TASK 401
SAFETY VERIFICATION

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

401.2. Task description.

401.2.1. The contractor shall define and perform tests and demonstrations, develop models, and otherwise verify the compliance of the system with safety requirements on safety-critical 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. Where hazards are identified during the development efforts and analysis or inspection cannot determine the adequacy of actions taken to reduce the risk, safety tests shall be specified and conducted to evaluate the overall effectiveness of the actions taken. Test plans and procedure documents, as required, shall be revised to include these tests. Where costs for safety testing are prohibitive, the PM can approve safety characteristics or procedures verified by engineering analyses, analogies, laboratory tests, functional mockups, or models and simulations. Specific safety tests shall be integrated into appropriate system test and demonstration plans, including verification and validation plans, to the maximum extent possible. Test plans, test procedures, and the results of all tests—including design verification, technical operational evaluation, technical data and requirements validation and verification, production acceptance, and shelf-life validation (including verification methods)—shall be reviewed to ensure the following:

a. The safety of the design (including operating and maintenance procedures) is adequately demonstrated, including verification of safety devices, warning devices, etc., for all Catastrophic and Critical hazards. Marginal and Negligible hazards shall also be addressed as required by the PM.

b. Results of safety evaluations of the system are included in the test and evaluation reports on hardware or software.

401.2.2. Report requirements. The contractor shall prepare a report that contains the results from the task described in paragraph 401.2 above and includes the following information:

a. Identification of the test procedures conducted to verify or demonstrate compliance with the safety requirements on safety-related hardware, software, and procedures (e.g., EOD and emergency procedures). When costs for safety testing is prohibitive, the PM can approve the safety characteristics or procedures that were verified by engineering analyses, analogies, laboratory tests, functional mockups, or models. Simulations will be identified and a summary of the results will be provided.

b. Identification of the test and evaluation reports that contain the results of the safety evaluations, with a summary of the results provided.

401.3. Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 401 (R)

b. Safety-critical equipment and procedures.

c. Additional development of inputs to test plans, procedures, and reports to verify safety requirements.

TASK 402
EXPLOSIVES HAZARD CLASSIFICATION DATA

402.1. Purpose. The purpose of Task 402 is to require the performance of tests and analyses, develop data necessary to comply with hazard classification regulations, and obtain requisite 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.

402.2.1. Explosives hazard classification. Compliance with DoD Ammunition and Explosives Hazard Classification Procedures (DAEHCP) (Army Technical Bulletin 700-2, Naval Sea Systems Command Instruction 8020.8, and Air Force Technical Order 11A-1-47) is mandatory when explosives are present at a DoD installation or facility worldwide or when, transporting explosives made by or under the direction or supervision of a DoD Component. Compliance should result in the PM obtaining requisite hazard classification approval documentation.

402.2.2. Data. To comply with DAEHCP, the Program Manager shall ensure his or her program personnel and contractors provide timely, requisite hazard classification data to appropriate DoD authorities (e.g., the DoD Explosives Safety Board). Such pertinent data may include:

a. Narrative information (e.g., functional descriptions, safety features, and similarities and differences to existing analogous explosive commodities, including packaging).

b. Technical data (e.g., 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 DOT classification of explosives approvals).

c. Storage and shipping configuration data (e.g., packaging details).

d. Test plans.

e. Test reports.

f. Analyses.

402.3. Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 402. (R)

b. Specific hazard classification data required. (R)

TASK 403
EXPLOSIVE ORDNANCE DISPOSAL SOURCE DATA

403.1. Purpose. The purpose of Task 403 is to require the contractor to provide source data, explosive ordnance disposal procedures, recommended render-safe procedures, and test items for new or modified weapons systems, explosive ordnance items, aircraft systems, and all unmanned systems.

403.2. Task description.

403.2.1. Source data. The contractor shall provide detailed source data on explosive ordnance design functioning and safety so that proper EOD tools, equipment, and procedures can be validated and verified. The Naval Explosive Ordnance Disposal Technology Division, Indian Head, Maryland, will assist in establishing quantities and types of assets required.

403.2.2. Explosive ordnance disposal procedures. The contractor shall recommend courses of action that explosive ordnance disposal personnel can take to render safe and dispose of explosive ordnance.

403.2.3. Test items. The contractor shall provide test ordnance for conducting EOD validation and verification testing.

403.3. Details to be specified. Details to be specified in the RFP and SOW shall include the following, as applicable:

a. Imposition of Task 403. (R)

b. Hazard classification data for all explosive components.

APPENDIX A
GUIDANCE FOR IMPLEMENTATION OF A SYSTEM SAFETY ENGINEERING EFFORT ACROSS ESOH DISCIPLINES

A.1. Scope. This appendix provides rationale and guidance to fit the needs of most ESOH efforts. Appendix A elaborates on management of ESOH risks using the system safety process. This appendix also includes further explanation of the effort and activities available to meet the general requirements described in Section 4 of this standard.

A.2. Guidance.

A.2.1. General. System safety applies engineering and management principles, criteria, and techniques to achieve ESOH risks as low as practicable within the constraints of operational effectiveness, time, and cost throughout all phases of the system lifecycle. System safety draws on professional knowledge and specialized skills in the mathematical, physical, and scientific disciplines, together with the principles and methods of engineering design and analysis, to specify and evaluate the ESOH risks associated with a system. Experience indicates that the degree of safety achieved in a system depends on the emphasis given and the proper allocation of planning, requirements, analysis, testing, and verification.

A.2.2. System safety process consists of eight steps:

A.2.2.1. Step 1 – document the system safety approach. The system safety approach is the foundation of the ESOH effort. It is important to establish the key attributes and actions of the ESOH effort as part of this step. Task 101 (Establish an ESOH Effort) details the requirements for establishing a solid ESOH effort. Task 102 (System Safety Engineering Plan), Task 103 (Support to Government ESOH Reviews/Audits), Task 104 (ESOH Integrated Product Team/Working Group Support), Task 105 (Hazard Tracking System), Task 106 (ESOH Progress Summary), and Task 107 (Hazardous Materials Management Plan) may be developed. Before formally documenting the system safety approach in the SSEP and contract SOW, the Program Manager, in concert with SE and associated environment, safety, occupational health, and other appropriate professionals, must determine what specific tasks and activities are necessary to meet program and regulatory requirements. This effort requires the system boundaries and use context to be clearly defined within the plan, including assumptions that establish the depth and breadth of the analyses. This effort consists of developing a planned approach for ESOH task accomplishment, providing qualified personnel to accomplish the tasks, establishing the authority for implementing ESOH tasks through all levels of management, and allocating appropriate resources to ensure that ESOH tasks are completed. This ongoing process includes additional analysis based on findings from previous efforts. System safety process planning includes:

A.2.2.1.1. Selective tailoring of a system safety effort is necessary to effectively achieve integration of ESOH considerations into the SE and programmatic risk management processes. The tasks should be applied as needed for a particular program. A large, complex system will likely require more tasks than a smaller system. Those ESOH analyses necessary for a particular program should be specified. For example, a large safety-critical system may need

to perform Task 201 (Preliminary Hazard List), Task 202 (Preliminary Hazard Analysis), Task 203 (Safety Requirements Analysis), Task 204 (Subsystem Hazard Analyses), Task 205 (System Hazard Analysis), Task 206 (Operating and Support Hazard Analysis), and Task 207 (Health Hazard Assessment). A smaller, less safety-related system may only need to perform Task 201 (PHL) and Task 202 (PHA) for an effective system safety program. The preferred format of the safety and hazard analyses can also be tailored as part of the system safety program. Task 106 (ESOH Progress Summary) gives more details. Depending on the program size and level of risk, safety verification methods ranging from analysis, inspection, demonstration, and testing can be tailored.

A.2.2.1.2. Specific safety performance requirements must be established based on overall program requirements and system user inputs. These general safety requirements are needed to meet the core program objectives. The more closely these requirements relate to a given program, the more easily the designers can incorporate the requirements into the system. In the appropriate system specifications, the safety performance requirements that are applicable and the specific risk categories considered acceptable for the system will be incorporated. Acceptable risk categories can be defined in terms of risk categories developed through an ESOH risk assessment matrix, an overall system mishap rate, demonstration of controls required to preclude unacceptable conditions, satisfaction of specified standards and regulatory requirements, or other suitable risk assessment procedures. Examples of safety performance statements include.

a. Quantitative requirements may be expressed in terms of either risk or the probability or frequency of a given severity category. Risk measures are typically expressed as a loss rate, such as “the expected dollar loss per flight hour shall not exceed $XXXX” or “the expected fatalities per year shall not exceed 0.00X.” Examples of probability or frequency requirements include “the Catastrophic system mishap rate shall not exceed X.XXx10-y per operational hour,” “the probability of Catastrophic severity mishap in the life of the fleet shall be less than 0.X,” or “mean time between failures shall not be less than X.Xx10y operating hours.”

b. Risk requirements could be expressed as “no hazards assigned a Catastrophic severity are acceptable.” Risk requirements could also be expressed as a level defined by a hazard risk assessment, such as “no Serious or High risks are acceptable.”

c. Standardization requirements. Standardization requirements are expressed relative to a known standard that is relevant to the system being developed. Examples include, “the system will comply with the laws of the State of Xxxxxxxx and be operable on the highways of the State of Xxxxxxxx” or “the system will be designed to meet American National Standards Institute Standard XXXX.XX-XXXX as a minimum.”.

A.2.2.1.3. ESOH milestones must be established relative to major program milestones, program element responsibility, and required inputs and outputs. This effort should include establishing an incident notification, investigation, and reporting process that includes notifying the PM. An approach and methodology must be established for reporting to the PM the following minimum information:

a. Safety-related functions, characteristics, and features. "Safety-related" is a term applied to any condition, event, operation, process, or item whose proper recognition, control, performance, or tolerance is essential to safe system operation and support (e.g., SRF, safety-related path, or safety-related component). SRFs, characteristics, and features should be reported to the PM. Understanding the importance of these components and the overall relationship to reducing risks for the system is essential. In particular, if these features are changed, or if through additional analyses or testing do not meet their original requirements, an assessment should be performed to understand the impact to the related risks. The impact should be reported to the PM.

b. Mitigations. The PM should be made aware of the mitigations used to reduce hazards. Similar to safety-related features, if the mitigations are changed, an assessment should be performed to understand the impact to the related risks, and the impact should be reported to the PM.

c. Hazardous materials selection. The rationale used for HM selection and the process for ensuring proper management of hazardous materials should be reported to the PM. See Task 107 (Hazardous Materials Management Plan).

d. Hazard communication. The method for communicating hazards and associated risks to the system user should be established and documented. Examples include establishing a safety alert process; providing training that includes a summary of associated risks; and documenting risks and appropriate procedures, including warnings and cautions, in the system's technical manuals.

e. Specialized safety approvals. Requirements for other specialized safety approvals (e.g., nuclear, range, explosive, chemical, biological, electromagnetic radiation, and lasers) should be specified, as necessary.

f. Analyses boundaries. The typical boundaries and assumptions must be specified for the system safety analyses and the typical limits of the analyses.

g. Analyses resolution. Hazard analyses have limited resolution depending on the system and details of the hazards. Analyses should be updated as more information is acquired.

A.2.2.1.4. Where software controls or mitigates system hazards, specific details must be included for integrating system safety processes and products into the software development lifecycle. As a minimum, the following topics should be addressed:

a. Identify and describe software contributors to hazards.

b. Identify safety-related software functions and safety-related software requirements.

c. Identify the software hazard criticality assessment process, including establishment of the Software Criticality Index (see Section 4.3.2) for each safety-related software function and safety-related requirement, and determine how it will be used to assign LOR tasks necessary to verify and validate the SCFs and requirements.

d. Perform a final risk assessment for hazards that have software contributors.

A.2.2.1.5. Elements of ESOH need to be embedded in the prime contractor's SOW and, if necessary, supporting contracts. MIL-STD-882D w/CHANGE 1 should be incorporated into the list of contractual compliance documents and include the potential of a developer to execute Section 4 requirements and any applicable tasks as source selection evaluation criteria. Contractors should be required to submit a preliminary plan (e.g., SSEP) with their proposal that describes the system safety effort required for the requested program. When directed by the PM, contractors should attach this preliminary plan to the contract or reference it within the SOW so it becomes the basis for a contractual system safety effort.

A.2.2.1.6. Individual tasks should be applied as needed for the particular program. Some programs may require only one or two tasks (e.g., a single PHA or SAR), while more complex programs may require application of most or all of the tasks. The interrelationships between ESOH and other functional elements of the program should be described. Other program requirements and tasks applicable to ESOH should be listed and referenced where they are specified or described. Tasks should include the organizational relationships between other functional elements having responsibility for tasks with ESOH impacts and the system safety management and engineering organization, including the review and approval authority of those tasks. The documentation of the system safety approach should describe the planned tasks and activities of system safety management and SE required to identify, evaluate, and eliminate or mitigate hazards. The goal of this effort is to reduce risk to a level as low as practicable throughout the system lifecycle. The documentation should state, at a minimum, a planned approach for task accomplishment, qualified personnel to accomplish tasks, the authority to implement tasks through all levels of management, and the appropriate commitment of resources (both manning and funding) to ensure that ESOH tasks are completed.

A.2.2.1.7. Task selection. Select tasks to fit the program. In most cases, the need for the tasks is self-evident. While experience plays a key role in task selection, it should be supplemented by a more detailed study of the program. Consideration must be given to the size and dollar value of the program and the expected level of risk involved. The selection of tasks must be applicable not only to the program phase, but also to the perceived risks involved in the design and the funds available to perform the system safety effort. Table A-I provides a list of tasks that system safety programs typically use. Once recommendations for task applications have been determined and more detailed requirements have been identified, tasks and requirements 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

TASK APPLICATION MATRIX

Task	Title	Task Type	Program Phase				
			MSA	TD	EMD	P&D	O&S
101	Establish an ESOH Effort	MGT	G	G	G	G	G
102	System Safety Engineering Plan	MGT	G	G	G	G	G
103	Support to Government Review/Audits	MGT	S	S	S	S	S
104	ESOH IPT/Working Group Support	MGT	G	G	G	G	G
105	Hazard Tracking System	MGT	G	G	G	G	G
106	ESOH Progress Summary	MGT	S	G	G	G	G
107	Hazardous Materials Management Plan (HMMP)	MGT	G	G	G	G	G
201	Preliminary Hazard List	ENG	G	S	S	S	N/A
202	Preliminary Hazard Analysis	ENG	G	G	G	GC	GC
203	Safety Requirements Analysis	ENG	G	G	G	S	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	GC	GC
207	Health Hazard Analysis	ENG	G	G	G	GC	GC
208	Functional Hazard Analysis	ENG	G	G	G	GC	GC
209	Systems-of-Systems Integration and Interoperability Hazard Analysis	ENG	G	G	G	GC	GC
210	Environmental Hazard Analysis	ENG	G	G	G	GC	GC
301	Safety Assessment Report	ENG	S	S	S	S	S
302	ESOH in Test and Evaluation	ENG	G	G	G	G	G
303	Review of ECPs Engineering Change Proposals, Specification Change Notices, Software Problem Reports, Mishap Investigations, and Requests for Deviations and Waivers	ENG	N/A	G	G	G	GC
401	Safety Verification	ENG	S	G	G	S	S
402	Explosives Hazard Classification Data	MGT	S	S	S	S	S
403	Explosive Ordinance Disposal Source Data	MGT	S	S	S	S	S

Task Type
ENG – Engineering
MGT – Management

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

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

DoD MIL-STD-882 (D)

A.2.2.2. Step 2 – identify hazards. Hazards should be identified and tracked through a systematic hazard analysis process encompassing detailed analysis of system hardware and software, the environment (in which the system will exist), and the intended use or application. Historical hazard and mishap data, including lessons learned from other systems, should be considered and used. Identification of hazards is the responsibility of all program members. For example, for complex systems, design engineers are often the most knowledgeable and familiar with a particular aspect of the design and are good sources for identifying specific hazards associated with that part of the system. During hazard identification and tracking, consider

hazards that could occur over the system lifecycle. Products of this step may include a PHL, a functional hazard assessment, and an HTS.

A.2.2.2.1. Hazard identification can be achieved with a variety of mutually complementary methods, including the use of checklists, prior work with similar systems, and operating scenario walkthroughs. Approaches have been developed and used to identify system hazards. A key aspect of many of these approaches is empowering the design engineers with the authority to design systems whose risk is as low as practicable and sanctioning them with the responsibility to identify the hazards associated with the design to program management. Hazard identification approaches often include using system users in the effort.

A.2.2.2.2. Hazards should be described in terms that identify a potential causal factor, the hazard whereby the harm may be caused, and the mishap of the harm itself. An example of a hazard described in this manner is laceration (mishap) from unprotected skin exposure (causal factor) to a sharp edge (hazard). Another example is ship damage (mishap) from a collision with foreign object (causal factor) due to degraded vision (hazard). Keep in mind that one combination of hazard and causal factor may have the potential to cause harm to more than one asset. Assets include personnel, facilities, equipment, operations, data, the public, the environment, the system itself, or other items of value. For the "ship-damage" mishap example above, if the ship is an oil tanker, a separate mishap for the same hazard and causal factor could be "oil spill," which could be a Catastrophic environmental risk. An effective way to deal with these multiple mishaps from one hazard and causal factor is to treat each mishap separately. The importance of this point becomes obvious during the risk reduction effort when each potential mitigation measure is identified and its effectiveness in reducing the risk to each asset is weighed against the cost and feasibility of the mitigation. In some cases, mishaps may be tightly linked. For instance, "death or serious injury to personnel" is linked to "serious damage to or loss of aircraft" when a causal factor includes aircraft impact with the ground. In this case, these two mishaps might best be treated as a single mishap.

A.2.2.3. Step 3 – assess risk. The severity and probability of the potential loss for each hazard (e.g., establish the initial risk for each hazard) must be assessed in accordance with Section 4 of this standard. The products of this element may include a PHA, O&SHA, SSHA, and SHA. When applying the risk assessment and values matrix, it may be appropriate to consider whether the mishap results in a mission-critical impact that causes mission failure or degraded capability.

A.2.2.3.1. Several methods are available to assess the risk, including expert judgment, numerical analysis, computer models, FMEA, and fault tree analysis. Tables I through III in Section 4 or Table A-II below shall be used unless a DoD Component develops and approves alternate risk assessment matrices. For systems with safety-related software (e.g., software controls and safety-related functions), each safety-related software function and requirement should be assigned an SwCI.

TABLE A-II. Risk Assessment Matrix

Risk Assessment Matrix

Specific Individual Item	Fleet or Industry	SEVERITY / PROBABILITY	Catastrophic (1) — Could result in one or more of the following: injury or illness resulting in less than 10 lost work days, minimal environmental impact, loss less than $100K.	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 loss exceeding $1M but less than $10M.	Marginal (3) — Could result in one or more of the following: injury or occupational illness resulting in 10 or more lost work days, reversible moderate environmental impact, or loss exceeding $100k but less than $1M.	Negligible (4) — Could result in one or more of the following: injury or illness resulting in less than 10 lost work days, or minimal environmental impact, loss less than $100K.
Likely to occur often in the life of an item; with a probability of occurrence greater than 10^{-1} in that life.	Continuously experienced	Frequent (A)	High	High	Serious	Medium
Will occur several times in the life of an item; with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.	Will occur frequently	Probable (B)	High	High	Serious	Medium
Likely to occur sometime in the life of an item; with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.	Will occur several times	Occasional (C)	High	Serious	Medium	Low
Unlikely, but possible to occur in the life of an item; with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life.	Unlikely but can reasonably be expected to occur	Remote (D)	Serious	Medium	Medium	Low
So unlikely, it can be assumed occurrence may not be experienced during a defined interval in the life of an item; with a probability of occurrence of less than 10^{-6} in that life.	Unlikely to occur, but possible	Improbable (E)	Medium	Medium	Medium	Low
Incapable of occurrence in the life of an item. This category is used when potential hazards are identified and later eliminated.	Incapable of occurrence within the life of an item. This category is used when potential hazards are identified and later eliminated	Eliminated (F)	Eliminated			

DoD M -STD 882 000

Note: table A-2 is a variant of table I-3.

1. *Use either the quantitative or qualitative descriptions of probability as appropriate for a given analysis.*
2. *Use either the individual item or fleet/inventory description depending on which description produces the more frequent probability level for a given analysis.*
3. *Probability level F is reserved for cases where the causal factor is either no longer present or it is impossible to lead to the mishap. No amount of doctrine, training, warning, caution, Personal Protective Equipment (PPE), or other change can move a mishap probability level to F.*

A.2.2.3.2. Assessing risk with multiple causal factors and hazards. This section assists the practitioner in assessing hazards, particularly those with multiple causal factors or hazards, and assessing the overall risk assessment for the related mishaps.

A.2.2.3.2.1 The RAC is a combination of one severity category and one probability level that correlates to a specific cell in Table III, Risk assessment matrix.

A.2.2.3.2.2 Figure A-1 illustrates an example of one hazard theory to describe a complete hazard; others may be used. The three elements illustrated are:

a. Causal factor – One or several mechanisms that trigger the hazard that may result in a mishap; failures, conditions, or events which contribute either directly or indirectly to the existence of a hazard.

b. Hazard – A condition that if triggered by one or more causal factor(s) can contribute to or result in a mishap.

c. Mishap – An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. For the purposes of this document, the term “mishap” includes negative environmental impacts from planned and unplanned events and accidents.

A.2.2.3.2.3 In examining the hazards identified for a particular system, the system safety practitioner will generally find that the outcome, or mishap, can be caused by more than one hazard or by one of several causal factors triggering the single hazard that causes the mishap. To determine the composite RAC for the risk, first determine the RAC for each hazard that leads to the same mishap. If the mishap can be caused by more than one hazard, compare the RACs for each hazard. The mishap should be assigned the RAC with the greatest risk. If the risk category (High, Serious, Medium, or Low) is the same for the hazards being compared, the mishap should be assigned the RAC with the greatest severity. For example, if two hazards for a mishap are assessed as a 1E (Medium risk) and 2E (Medium risk), the mishap should be assigned a RAC of 1E.

A.2.2.3.2.4 Just as multiple hazards can lead to the same mishap, multiple causal factors can trigger the same hazard, which then causes a mishap. In these instances, a composite RAC could also be generated for the hazard, based on the evaluation of RACs for the various causal factors that contribute to a hazard. Multiple causal factors such as human error, a software fault, or a mechanical malfunction could each individually cause an explosive charge to inadvertently detonate (hazard), crashing an aircraft (mishap). Each of these causal factors are assigned severity and probability combinations, such as 1B, 1D, and 1E. The composite RAC for the related hazard would be assigned as a 1B, as would the mishap, because that is the highest risk category leading to the mishap.

A.2.2.3.2.5 Example 1 in Figure A-1 shows an assessment in which there is only one causal factor leading to one hazard resulting in one mishap. Thus, only one RAC is carried

throughout the identification and assessment of the hazard for risk assignment of the mishap. The RAC would remain at the same level for all three elements of the hazard description.

A.2.2.3.2.6 Example 2 in Figure A-1 shows a mishap that can result from two different hazards triggered by three different causal factors. The three causal factors are associated with varying levels of risks, which trigger two hazards with varying levels of risk. When assessing the risk of a hazard caused by more than one causal factor, the highest risk associated with a causal factor should be used for the hazard. In this example, Hazard 2 could be triggered by two causal factors, which results in hazard RACs of 2D and 2E. The higher RAC should be assigned to the hazard; therefore, the hazard risk becomes 2D. Similarly, Hazard 2 and Hazard 3 are assigned varying risks, but both contribute to the same mishap. The mishap should be assigned the RAC which is equal to the higher of its two contributing hazards (Hazard 2 and Hazard 3). A RAC of 2C should be used over 2D and assigned as the risk.

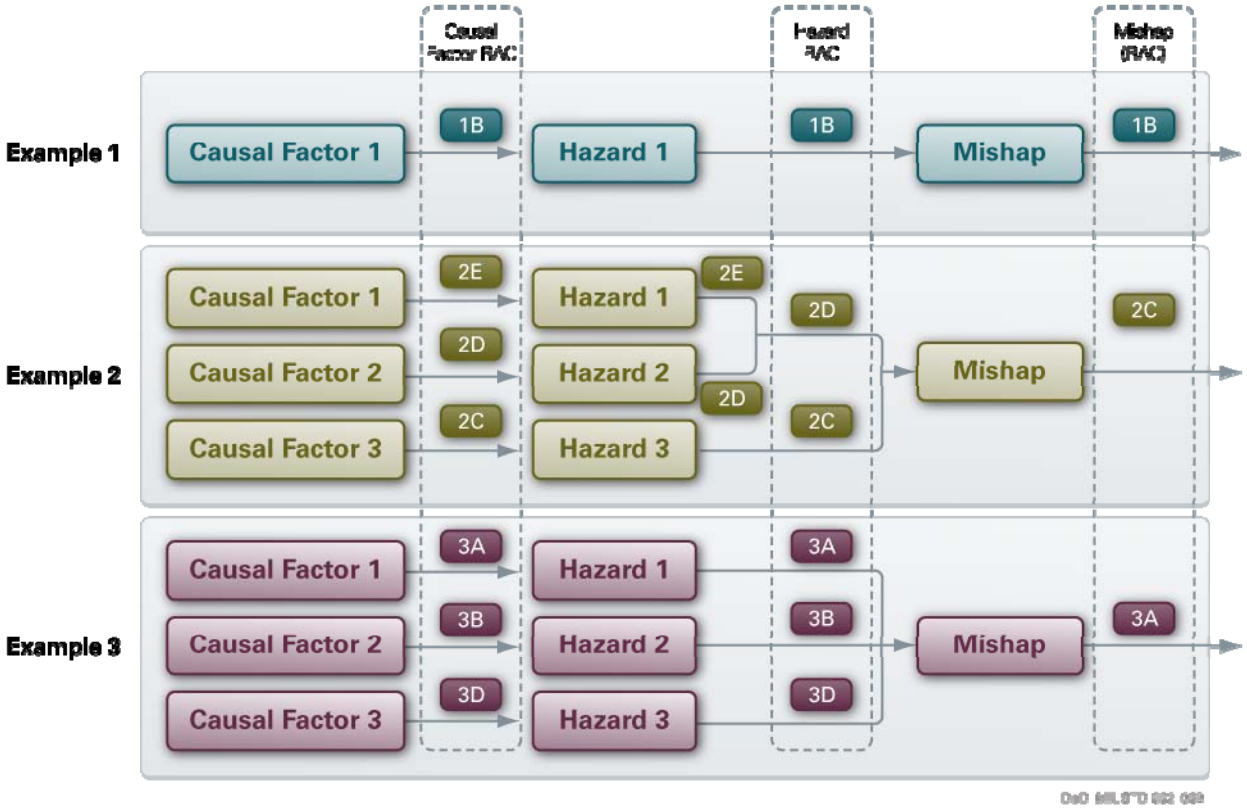


FIGURE A-1. Risk assessment examples of multiple causal factors and hazards

A.2.2.3.2.7 Example 3 in Figure A-1 shows a mishap from three independent hazards, which could be triggered by three causal factors. Using the methodology described in this section, Hazard 1 is assigned the RAC of Causal Factor 1, Hazard 2 is assigned the RAC of Causal Factor 2, and Hazard 3 is assigned the RAC of Causal Factor 3. Since each of the three

hazards leads to a common mishap, the highest RAC associated with the contributing hazards (Hazard 1, Hazard 2, and Hazard 3) should be assigned to the mishap. In this example, Hazard 1 is assessed as 3A, Hazard 2 is assessed as 3B, and Hazard 3 is assessed as 3D. The highest RAC among these three hazards is 3A; therefore, the mishap is assigned a RAC of 3A.

A.2.2.3.2.8 The practitioner needs to understand the various combinations of developing and describing causal factors, hazards, and mishaps and how to assign RACs when there are multiple inputs into the development and assessment of mishaps.

A.2.2.3.3. The risk impact is assessed, as necessary, using other factors to discriminate between hazards having the same risk index. One might discriminate between hazards with the same risk index in terms of mission capabilities or social, economic, and political factors. Program management will consult closely with the using organization on the decisions used to prioritize resulting actions.

A.2.2.4. Step 4 – identify risk mitigation measures. Risk reductions are achieved by understanding the risk drivers, reducing risk according to the system safety mitigation order of precedence, and then reassessing the risks. Mitigations may serve to eliminate the hazard or reduce the severity or probability of potential mishaps. The mitigations for each hazard should be selected based on effectiveness, cost, and feasibility. Feasibility includes consideration of both means and schedule for accomplishment. After mitigations have been selected, the risks should be reassessed to ensure that risks are as low as practicable. Potential risk mitigation alternatives and the expected effectiveness of each alternative or method must be identified. Hazards should be prioritized so that corrective action and redesign efforts can be focused to eliminate or mitigate serious hazards first.

A.2.2.5. Step 5 – reduce risk. The primary goal of the system safety process is to identify hazards and reduce the associated risks, ideally to completely eliminate those risks. Once all potential risk mitigations have been identified, the ESOH IPT/WG, in coordination with the PM and using organization, should evaluate the appropriate potential mitigations and make the appropriate selections. Mitigations should be selected based on cost, effectiveness, and feasibility.

A.2.2.6. Step 6 – verify risk reduction. Once the mitigations have been selected, the risk reduction needs to be verified to ensure the risk is actually reduced to the predicted level. Risk mitigation must be verified through appropriate analysis, inspection, demonstration, and testing. Mitigations must be evaluated to ensure implementation and confirm effectiveness. Through the system test effort, the PM must ensure that the selected mitigations will produce the expected reduction in risk. New hazards identified during testing must be incorporated into the HTS and addressed.

A.2.2.7. Step 7 – risk acceptance. The ESOH engineers, working groups, and the designated risk acceptance authority determine whether the risks have been reduced to as low as practicable within the constraints of operational effectiveness, suitability, time, and cost. The designated risk acceptance authority should be kept informed of identified hazards and risks, particularly if an event causes the hazard to be reopened or if the target risk is to be elevated.

The appropriate authority then accepts the risk in accordance with DoD policy and the documentation is retained.

A.2.2.8. Step 8 – life-cycle risk management. After the system is fielded, the risk management process should continue to maintain the HTS throughout its lifecycle. This life-cycle effort should consider any changes to the hardware and software, mishap data, mission, system health data, and similar concerns. The program office and user community must maintain effective communication channels to identify and manage new hazards and modified risks. The engineering authority for the system should have periodic reviews of the system ESOH effort to ensure residual risks are at the appropriate levels, review whether new hazards have been discovered, and ensure that no unresolved program actions remain that relate to ESOH. Updates to hazards should be documented in the HTS.

A.3. Software system safety engineering and analysis. A successful software system safety engineering activity is based on a hazard analysis process, a safety-related software development process, and a LOR process. The safety-related software development and LOR processes 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-related software development and LOR processes 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.

A.3.1. Software system safety engineering analysis. System safety engineers performing the hazard analysis for the system (PHA, SSHA, SHA, SoS Integration and Interoperability Hazard Analysis (IIHA), FHA, O&SHA, and 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 interfacing systems within an SoS architecture. In general, software functionality that directly or indirectly contributes to mishaps, such as the processing of safety-related 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-related 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 hazard 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-related hazard. Software requirements that implement safety-related functions are also identified as safety-related.

A.3.2. 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 lifecycle (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 defined by performing an FHA to identify safety-related functions, assigning an SCC to each of the software-related safety-critical and safety-significant software functions, assigning an SwCI based on severity and SCC, and implementing LOR tasks for safety-related software based on the SwCI. These software system safety tasks are further explained in subsequent paragraphs.

A.3.2.1. Perform a functional hazard analysis (see Task 208). The SRF of the system should be identified. Once identified, each SRF is assessed and categorized against the SCCs to determine the level of control of the software over safety-related functionality. Each SRF is mapped to its implementing computer software configuration item or module of code for traceability purposes.

A.3.2.2. Perform a software criticality assessment for each safety-related function. 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 safety-related function 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 an SwCI as defined in Table V. The SwCI is then used as part of the software system safety analysis process to determine the amount of analysis and testing (LOR) required for verification of the specific software requirement or function.

A.3.2.3. SSCM tailoring. The SSCM can and should be tailored for a given program. There are numerous software development and verification methods and tools. However, tailoring should result in an SSCM that meets or exceeds the LOR defined in Table V, unless approved by the appropriate DoD acquisition authority. An SwCI1 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 SwCI2 through SwCI4 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 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, the likelihood of software contributing to a mishap may be reduced.

A.3.2.4. Software system safety and requirements within software development processes. Once safety-related software functions are identified, assessed against the SCC, and assigned an SwCI, the implementing software should be designed, coded, and tested against the approved SDP containing the software system safety requirements and LOR. These criteria should be defined, negotiated, and documented in the SDP and the software test plan (STP) early in the development lifecycle.

A.3.2.4.1. SwCI assignment. An SwCI should be assigned to each safety-related software function and the associated safety-related software requirements. Assigning the SwCI value of Not Safety to nonsafety-related software requirements provides a record that functionality has been assessed by software system safety engineering and deemed Not Safety. Individual safety-related software requirements that track to the hazard reports will be assigned an 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-related requirements need only the defined safety-specific testing.

A.3.2.4.2. 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 System Safety Committee Software System Safety Handbook* and Allied Ordnance Publication 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.

A.3.2.5. 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.3.2.5.1. 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, design safety standards, and best and common practices.

A.3.2.5.2. 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 safety-related functions, safety-related functions code review, safety-related functions, 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.

A.3.2.5.3. Test tasks. Test task considerations include safety-related function testing, functional thread testing, limited regression testing, 100 percent regression testing, failure modes and effects testing, out-of-bounds testing, safety-related interface testing, COTS and GOTS input/output testing and verification, independent testing of prioritized safety-related functions, functional qualification testing, IV&V, and nuclear safety cross-check analysis.

A.3.2.6. Software system safety risk assessment. After completion of all specified software system safety engineering analysis, software development, and LOR activities, results will be used as evidence (or input) to assess software's contribution to the residual safety 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-critical requirement and function. This information will be integrated into the program hazard analysis documentation and formal risk assessments.

A.3.2.6.1. Figure A-2 illustrates the relationship between the software system safety activities (hazard analyses, software development, and LOR), system hazards, and mishap residual risk. Table A-3 provides amplifying criteria for determining mishap residual risk levels associated with software. Table A-3, as with all of risk assessment-based criteria in this standard, is to be tailored for each DoD customer application.

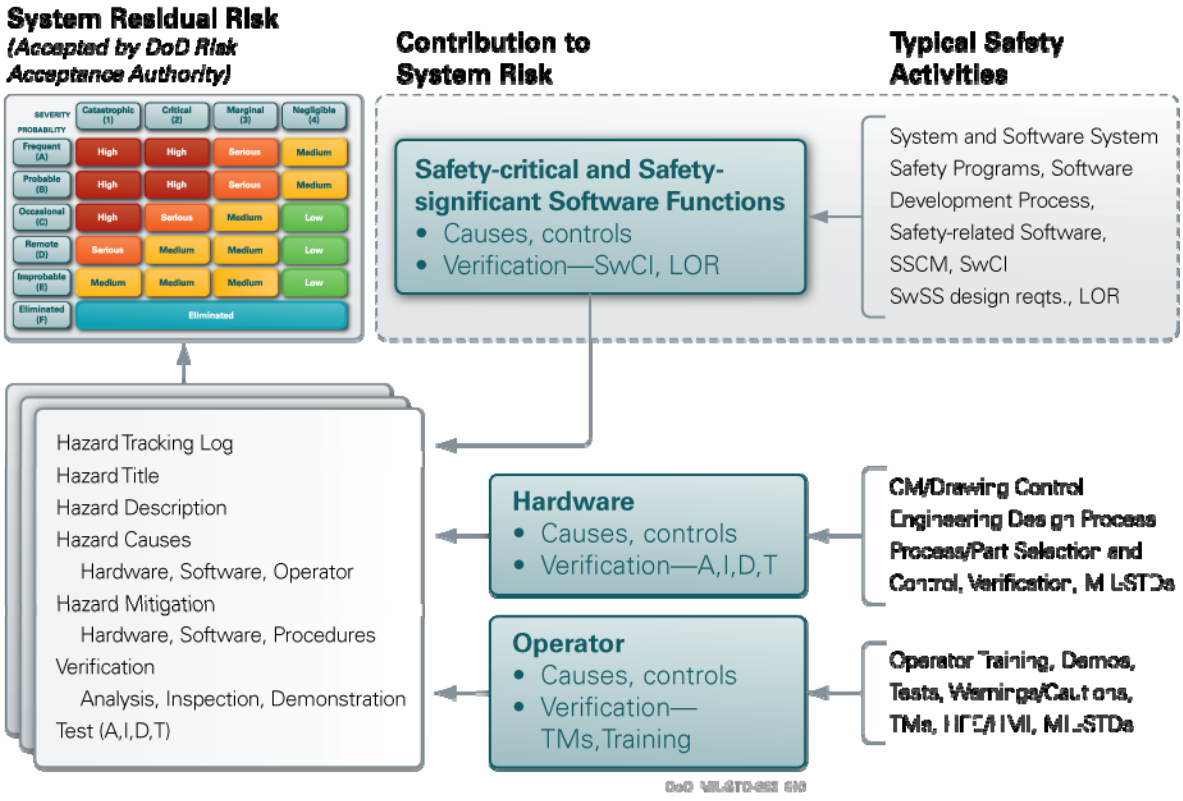


FIGURE A-2. Assessing Software's Contribution to Mishap Residual Risk

A.3.2.6.2. System hazards that have software causes and controls are closed based on evidence that hazards, causes, and mitigations have been identified, implemented, and verified in accordance with DoD customer requirements. The evidence supports the safety case that hazard controls provide the required level of mitigation and the resultant mishap residual risks can be accepted by the appropriate decision 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 residual risk associated with inadequately verified software hazard causes and controls. Generally, hazard closure and residual risk is based on quantitative and qualitative judgment and evidence. Hazards are closed and residual risks are mitigated to the lowest practical level based on analysis and evidence that sufficient numbers of independent safety controls have been implemented and verified. Table A-III shows how these principles can be applied to provide an assessment of residual risk for hazards with software causal factors.

TABLE A-III. Software Hazard Casual Factor Mishap Residual Risk Assessment Criteria

Residual Safety Risk	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	• Places the system in a condition where only one independent functioning interlocks or human actions remains to preclude the potential occurrence of a catastrophic or critical hazard, *or* • Can lead directly to a marginal or negligible mishap.
Medium	• Places the system in a condition where two independent functioning interlocks or human actions remains to preclude the potential occurrence of a catastrophic or critical hazard, *or* • Influences a marginal or negligible mishap, reducing the system to a single point (1) of failure.
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.

DoD_MIL-STD-882_D11

A.3.2.6.3. In order to accept a software control as implemented and verified, evidence that the software system safety requirements have been successfully verified to the DoD customer's specified LOR must be provided. Safety-related software that has undergone a rigorous software system safety program that meets the requirements defined in Chapter 4 may be acceptable as hazard mitigation, depending on the approved program risk acceptance process. A hazard can be mitigated to a relatively lower residual final RAC if sufficient evidence is provided. However, insufficient evidence or evidence of inadequate software system safety program application must be assessed as residual risk, as defined in 4.3.3.

A.3.2.6.4. Defining and following a process for assessing mishap residual risk for 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 these complex SoS can become difficult to determine. The process for assessing software's contribution to mishap residual 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 mishap residual 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.

APPENDIX B
CONTRACT TERMS AND CONDITIONS

B.1. Scope. This appendix provides guidance on general contract terms and conditions to fit the needs of most ESOH efforts.

B.2. Guidance. Some PMs include the following conditions in their solicitation, system specification, or contract as requirements for system design. These condition statements are optionally used as supplemental requirements based on specific program needs and include the following sections. These condition statements are worded as they would appear if used in this manner.

B.2.1. Unacceptable conditions. The following safety-critical conditions are considered unacceptable for development efforts. Positive action and verified implementation is required to reduce the risk associated with these situations to a level acceptable to the PM.

B.2.1.1. Single point failures. Single component or multi-component single-point failure, common mode failure, human error, or a design feature that could cause a mishap of Catastrophic or Critical severity categories.

B.2.1.2. Dual failures. Dual-independent component failures, dual-independent human errors, or a combination of a component failure and a human error involving safety-critical command and control functions which could cause a mishap of Catastrophic or Critical severity categories unless verification proves that the risk is Improbable or that this risk is accepted by the appropriate risk acceptance level.

B.2.1.3. Hazardous radiation. Generation of hazardous radiation or energy when no provisions have been made to protect personnel or sensitive subsystems from damage or adverse effects.

B.2.1.4. Packaging procedures. Packaging or handling procedures and characteristics that could cause a mishap for which no mitigations have been provided to protect personnel or sensitive equipment.

B.2.1.5. Unacceptable hazards. Hazard categories that are specified as unacceptable in the development agreement.

B.2.1.6. Human factors capabilities. Component design or location that fails to address human physical, anthropometrics, physiological, and perceptual-cognitive capabilities or limitations. Designs that are conductive to error, such as controls that are difficult to read, are confusing, or create excessive cognitive demands on the users.

B.2.2. Acceptable conditions. The following approaches are considered acceptable for correcting unacceptable conditions and will require no further analysis once mitigation measures are implemented and verified to an acceptance condition.

B.2.2.1. Nonsafety-critical independent errors or failures. For nonsafety-critical command and control functions, a system design requires two or more independent human errors, two or more independent failures, or a combination of independent failure and human error.

B.2.2.2. Safety-critical independent errors or failures. For safety-critical command and control functions, a system design requires at least three independent failures, three independent human errors, or a combination of three independent failures and human errors, unless verification proves that the risk is Improbable or the risk is accepted by the appropriate risk acceptance level for mishaps that occur due to two or fewer independent failures.

B.2.2.3. Error prevention. System designs that positively prevent errors in assembly, installation, or connections that could result in a mishap.

B.2.2.4. Damage propagation prevention. System designs that positively prevent damage propagation from one component to another or prevent sufficient energy propagation to cause a mishap.

B.2.2.5. Design limitations. System design limitations on operation, interaction, or sequencing that preclude occurrence of a mishap.

B.2.2.6. Design safety factors. System designs that provide an approved safety factor or a fixed design allowance that limits the possibility of structural failure or release of energy sufficient to cause a mishap.

B.2.2.7. Energy control. System designs that control energy build-up that could potentially cause a mishap (e.g., fuses, relief valves, or electrical explosion proofing).

B.2.2.8. Failure tolerance. System designs where component failure can be temporarily tolerated because of residual strength or alternate operating paths so that operations can continue with a reduced but acceptable safety margin. When feasible, consider providing a warning indicator when a primary control system fails or the alternative control system is engaged.

B.2.2.9. Alerts to hazardous situations. System designs that positively alert the controlling personnel to a hazardous situation where the capability for operator reaction can been provided.

B.2.2.10. Minimizing hazardous materials. System designs that limit or control the use of hazardous materials, including use of the least hazardous products and processes consistent with operational effectiveness and economy.

APPENDIX C
CONCLUDING MATERIAL

Custodians:

Army - AV

Navy – AS

Air Force – 40

Preparing activity:

Air Force – 40

Review activities:

OSD – AT&L/I&E

SD-4 project:

SAFT -2006-002

Industry Associations:

NDIA Systems Engineering Division