NOT MEASUREMENT SENSITIVE

MIL-STD-882F

TBD

SUPERSEDING

MIL-STD-882E

11 May 2012

~~SUPERSEDING~~

~~MIL-STD-882D~~

~~10 February 2000~~

Commented [PDANUAA1]: i-1
Version change & associated cleanup

DEPARTMENT OF DEFENSE STANDARD PRACTICE

SYSTEM SAFETY

AMSC N/A **AREA SAFT**

FOREWORD

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

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

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

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

ii.1 DoDI 5000.02 Change

Commented [PDANUAA2]: ii-2
GLOBAL ACTION – terminology cleanup
Hazards are **Controlled** through **Mitigation** (e.g. reducing probability) or **Amelioration** (e.g. reducing severity)
Granted most hazards are controlled through Mitigations, though some may be controlled through Amelioration or a combination of Mitigation and Amelioration. As such, 882F needs to reflect proper/consistent usage of these terms

Commented [PDANUAA3]: See ii-2

Commented [PDANUAA4]: See ii-2

Commented [PDANUAA5]: See ii-2

Commented [PDANUAA6]: ii-1
ACTION: Need to revise to appropriate DODI 5000.02 (or other) reference

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

~~a. Reintroduced task descriptions:~~
~~(1) 100-series tasks – Management.~~
~~(2) 200-series tasks – Analysis.~~

5. This revision incorporates changes to clarify software safety requirements, correct unclear language, and better align tasks with accepted common practices. This revision aligns with the standard practice with DoD policy; supports DoD strategic plans and goals; and adjusts the organizational arrangement of information to clarify the basic elements of the system safety process, clarify terminology, and define task descriptions to improve hazard management practices. This Standard strengthens integration of other functional disciplines into SE to ultimately improve consistency of hazard management practices across programs. Specific changes include:

a. Realigning with changes to DODI 5000.02
b. Refining all tasks to eliminate features not being utilized & redundant text
c. Tasks refocused to clarify expectations
d. Reworking paragraph 4.4 to address Software Safety Assurance
e. Adding guidance to address new/emerging technologies
f. Correct technical errors

Commented [PDANUAA7]: ii-3
Revised para 5 to address the highlights of the changes to 882F. (Additional editing needed)

FUTURE ACTION: Scrub all incorporated comments to ensure they are accounted for here

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

~~g. Emphasized the identification of applicable technical requirements.~~

~~h. Included additional tasks:~~

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

~~i. Applied increased dollar values for losses in severity descriptions.~~

~~j. Added "Eliminated" level for probability.~~

~~k. Added software system safety techniques and practices.~~

~~l. Updated appendices.~~

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

7. DISTRIBUTION A. Approved for public release: distribution unlimited.

Commented [PDANUAA8]: See ii-3

Commented [PDANUAA9]: iii-i
Added Distribution statement (was not included in 882E)

CONTENTS

PARAGRAPH **PAGE**

Commented [PDANUAA10]: See ii-2

Commented [PDANUAA11]: vi-1
Revised table of Contents to match revisions later in the document.
Para 4.4 retitled :Software Safety Assurance to better categorize activities. These are different software safety activities discussed in the 2xx Tasks

FUTURE ACTION: Page numbers will be added in a future draft.

Revise table of contents & page numbers as a result of changes

Commented [PDANUAA12]: iv-1

CONTENTS

PARAGRAPH **PAGE**

Commented [PDANUAA13]: FUTURE ACTION: Renumber Tasks to account for additions/deletions

Commented [PDANUAA14]: v-1
Delete Task – see rationale in task 101 description

Commented [PDANUAA15]: v-1
Delete Tasks – see rationale in task 103, 104, 105, & 106 descriptions

Commented [PDANUAA16]: v-1
Task Name Change? See Task 201 description

Commented [PDANUAA17]: v-1
Task 304 to be merged with Task 201. See Task 201 for rational

TASK SECTION 400 - VERIFICATION

CONTENTS

Commented [PDANUAA18]: vi-1
New Material added

Commented [PDANUAA19]: Revised/New Figures added for clarity

Commented [PDANUAA20]: vi-1
Revisions needed to align with later changes in the document

1. SCOPE

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

1-1 DoDI 5000.02 Change

Commented [PDANUAA21]: 1.2
Delete. Duplicates para 4.1

Commented [PDANUAA22]: 1-1
TBD Revision needed (see ii-1)

2. APPLICABLE DOCUMENTS

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

2.2 Government documents.

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

INTERNATIONAL STANDARDIZATION AGREEMENTS

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

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

DEPARTMENT OF DEFENSE HANDBOOKS

No Designator	-	Joint Software Systems Safety Engineering Handbook

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

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

DEPARTMENT OF DEFENSE INSTRUCTIONS

DoDI 5000.02 - Operation of the Defense Acquisition System

2.1 DoDI 5000.02 Change

DoDI 6055.07 - Mishap Notification, Investigation, Reporting, and Record Keeping

2.4 Granted mishap related information is a "feeder" into the hazard analyses process, but due to JAG rulings, Limited Use Mishap Data cannot be provided to OEMs, except under certain conditions. It follows that any documentation directly/indirectly citing such Limited Use Mishap Data must likewise be marked and protected. Violators could be subject to legal action, though it is not clear who is responsible for enforcing. One could argue that the government system safety practitioner could be considered culpable if they allow violations to exist without taking action. Data not properly protected undermines the legal argument to be able to protect similar data in the future. Thus, the de facto practice implied through this citation is poor guidance.

Based on these points, is this an appropriate citation since the OEM, suppliers, and vendors would not usually have access to this data? Recommend deleting this citation. If an OEM, supplier, or vendor needs access, this can be resolved on an exception basis.

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

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

2-2 DoDI 5000.02 Change

3. DEFINITIONS

3.1 Acronyms.

~~AFOSH Air Force Occupational Safety and Health~~
ANSI American National Standards Institute
AOP Allied Ordnance Publication
AMSC Acquisition Management Systems Control
ASSIST Acquisition Streamlining and Standardization Information System
ASTM American Society for Testing and Materials
AT Autonomous
CAS Chemical Abstract Service

Commented [PDANUAA23]: 2-1
TBD Revision needed (see ii-1)

Commented [PDANUAA24]: 2-4
Content question

Commented [PDANUAA25]: FURTURE ACTION: Ensure this is a correct link

Commented [PDANUAA26]: 2-2
TBD Revision needed (see ii-1)

Commented [PDANUAA27]:
FURTURE ACTION – search document to ensure each acronym cited in 3.1 are used in the document

FURTURE ACTION – search document to ensure all Acronyms have been identified in 3.1

Commented [PDANUAA28]: 2-3 Term no longer used

CDR	Critical Design Review
CFR	Code of Federal Regulations
COTS	Commercial-Off-the-Shelf
DAEHCP	Department of Defense Ammunition and Explosives Hazard Classification Procedures
DID	Data Item Description
DoD	Department of Defense
DoDI	Department of Defense Instruction
DODIC	Department of Defense Identification Code
DOT	Department of Transportation
DT	Developmental Testing
E3	Electromagnetic Environmental Effects
ECP	Engineering Change Proposal
EHA	Environmental Hazard Analysis
EMD	Engineering and Manufacturing Development
EO	Executive Order

EOD	Explosive Ordnance Disposal
ESD	Electrostatic Discharge
ESOH	Environment, Safety, and Occupational Health
FHA	Functional Hazard Analysis
FMECA	Failure Modes and Effects Criticality Analysis
FTA	Fault Tree Analysis
GFE	Government-Furnished Equipment
GFI	Government-Furnished Information
GOTS	Government-Off-the-Shelf
HAZMAT	Hazardous Material
HERO	Hazards of Electromagnetic Radiation to Ordnance
HHA	Health Hazard Analysis
HMAR	Hazard Management Assessment Report
HMMP	Hazardous Materials Management Plan
HMP	Hazard Management Plan
HRI	Hazard Risk Index
HSI	Human Systems Integration
HTS	Hazard Tracking System
IEEE	Institute of Electrical and Electronics Engineers
IM	Insensitive Munitions
IMS	Integrated Master Schedule
IPT	Integrated Product Team
ISO	International Organization for Standardization
replace RAC.	Note HRI was the term used in MIL-STD-
882C IV&V	Independent Verification and Validation
JCIDS	Joint Capabilities Integration and Development System
LOR	Level of Rigor
MANPRINT	Manpower and Personnel Integration
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
MSDS	Material Safety Data Sheet
MTA	Middle Tiered Acquisition
NATO	North Atlantic Treaty Organization
NAVMC	Navy and Marine Corps
NDI	Non-Developmental Item
NEPA	National Environmental Policy Act
NSI	No Safety Impact
NSN	National Stock Number
O&SHA	Operating and Support Hazard Analysis
OSH	Occupational Safety and Health
OSHA	Occupational Safety and Health Administration
OT	Operational Testing
PESHE	Programmatic Environment, Safety, and Occupational Health Evaluation
PDR	Preliminary Design Review
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PM	Program Manager

Commented [PDANUAA29]: 3-1
Change in Terminology (HRI replacing RAC)
See 12-2

Commented [PDANUAA30]: 3-2
New management approach

PPE	Personal Protective Equipment
~~RAC~~	~~Risk Assessment Code~~

Commented [PDANUAA31]: 3-3
Term being deleted to avoid confusion. Term used by other safety disciplines for different reasons. This term being replaced with HRI.

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

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

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

4.1	DoDI 5000.02 Change

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

Commented [PDANUAA32]: See ii-2

Commented [PDANUAA33]: 4-1
TBD Revision needed (see ii-1)

3.2.X Agile Software: An iterative and incremental (evolutionary) approach to software development which is performed in a highly collaborative manner by self-organizing teams within an effective governance framework with "just enough" ceremony that produces high quality software in a cost effective and timely manner which meets the changing needs of its stakeholders.

3.2.X Artificial Intelligence ➔ add Definition

TBD AI & Machine Learning related definitions

3.2.X Amelioration Measure. Action required to reduce the associated risk by lessening the severity of the resulting mishap.

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

Commented [PDANUAA34]: 4-2
New definition needed for (new) software development approach

Commented [PDANUAA35]: 4-3
New definition needed to address new technology being used in systems.

Commented [PDANUAA36]: FUTURE ACTION: Add TBD Machine Learning & AI definitions – see 4.4 subpara discussions.

Commented [PDANUAA37]: 4-4
New definition to address controls that reduce the severity. Note Mitigation Measure already defined through which probability (or likelihood of occurrence) are used to control a hazard.
See 3.2.21 & 4.3.4.2

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

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

3.2.X Control Measure: Action required to eliminate the hazard, or when a hazard cannot be eliminated, reduce the associated risk by lessening the severity (i.e. amelioration) of the resulting mishap or lowering the likelihood (i.e. mitigation) that a mishap will occur.

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

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

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

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

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

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

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

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

Commented [PDANUAA38]: New definition adjusted to align with new definitions for Amelioration & Mitigation Measures
See 3.2.21, 3.2.X, & 4.3.4.2

Commented [PDANUAA39]: 5-3
Clarification: Changes may be for the better or the worse

Commented [PDANUAA40]: 5-4
The ISO Standard 14001, EMS, defines an environmental impact is caused by an aspect. Environmental used "aspects" and "impacts", just like safety uses "hazards" and "risks". -So is important to add "aspect" to show a link from "aspect" to "impact".

FUTURE ACTION: Review 882F text to see where "Hazards" and "Risks" are being used. For each usage case, does text need to be adjusted to account for "aspects" and "impacts"?

Commented [PDANUAA41]: 5-1
Deleted non-value added verbiage

Commented [PDANUAA42]: 5-2
ESOH include more safety disciplines than just system safety

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

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

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

3.2.17 Initial risk. The first assessment of the potential risk of an identified hazard. Initial risk establishes a fixed baseline for the hazard and does not include hazard control measures.

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

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

4

3.2.X Loss of Equipment: Consequent of a hazard through which the equipment (or system) is lost.

3.2.X Loss of Functionality: Consequent of a hazard through which functionality of a component, subsystem, or system may be permanently lost or temporarily interrupted. This term is often used in conjunction with functionality realized through software.

3.2.X Machine Learning ➔ Add Definition

3.2.X Middle Tiered Acquisition ➔ Add Definition/Citation

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

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

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

Commented [PDANUAA43]: 6-4 Clarification of intent of term.

Commented [PDANUAA44]: FUTURE ACTION: Potentially revise for AI/Machine Learning LOR vs Software LOR (See para 4.4.8)

Commented [PDANUAA45]: 6-5 New Definition providing clarification of terminology
See para 4.3.3 & Table I

Commented [PDANUAA46]: 6-1
New technology needing to be addressed

Commented [PDANUAA47]: 6-2
New acquisition approach needing to be addressed

Commented [PDANUAA48]: Definition adjusted to align with new definition for Amelioration Measure
See 4.3.4.2

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

3.2.X Multi-Core Processor ➔ Add Definition

Commented [PDANUAA49]: 6-3
New technology needing to be addressed

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

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

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

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

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

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

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

7-2 Risk Level definition does not align with the possible risk level options derived from Table III. **Designed Out** had been added in MIL-STD-882E but this definition not adjusted. Designed Out reflects situations where the hazard no longer is possible in the design (e.g. Risk probability = 0).
Suggest adding Designed Out to Risk Level definition.

Commented [PDANUAA50]: 7-2
Technical Correctness Question

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

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

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

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

Commented [PDANUAA51]: See ii-2

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

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

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

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

7.1 Need to rework definition for software.
Software needs to address the application of logic to a system. This can be realized in several forms. (Note SW-like-HW is defined below in 3.2.X)
As written, this definition provides some examples, but many other technologies could also be included. As such, if the listed examples are viewed as a finite set of examples, these other devices/technologies could be excluded.
The focus is the set of logic, whether realized in hardward, programs, logic devices, etc

Commented [PDANUAA52]: 7-1
See text for issue that needs to be addressed

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

3.2.X Software-Like-Hardware: A catch-all term to address ALL logic that is embedded in hardware and is not readily considered software. This includes, but not limited to, all logic devices, firmware, ASICs, programmable gate arrays, etc.

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

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

3.2.X Split risk: TBD

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

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

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

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

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

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

Commented [PDANUAA53]: 8-1
New definition to fill gap between hardware and software. Experience has shown many instances where arguments were made to exclude many hardware oriented logic devices from software requirements, thus circumventing the intent on ensuring such logic has been appropriately vetted through the software safety requirements.

Commented [PDANUAA54]: 8-4
Inclusion of new term to aid in risk management. See para 4.3.3.6

Commented [PDANUAA55]: See ii-2

3.2.47 Systems engineering (SE). The overarching process that a program team applies to transition from a stated capability to an operationally effective and suitable system. ~~Systems Engineering~~ SE involves the application of SE processes across the acquisition life-cycle (adapted to every phase) and is intended to be the integrating mechanism for balanced solutions addressing capability needs, design considerations, and constraints. SE also addresses limitations imposed by technology, budget, and schedule. SE processes are applied early in material solution analysis and continuously throughout the total life-cycle to include SE participation in as required, but not limited to, program and technical reviews, program teams, program working groups, certification boards, mission readiness reviews, flight readiness reviews, audits, launch readiness reviews, National Environmental Policy Act (NEPA) document public hearings, etc. System safety engineering is a sub-discipline of SE.

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

Commented [PDANUAA56]: 8-2
Format Cleanup

Commented [PDANUAA57]: 8-3
Anchors SE's ubiquitous involvement in program acquisition/sustainment activities. Other documents provide guidance for this SE involvement. It is outside the scope of MIL-STD-882 to repeat such requirements in SE.
As a sub-discipline, system safety is likewise involved with these same activities.

Commented [PDANUAA58]: See ii-2

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

4 GENERAL REQUIREMENTS

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

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

4.2 System safety requirements. Section 4 defines the system safety requirements throughout the life-cycle for any system. When properly applied, these requirements should enable the identification and management of hazards and their associated risks during system developmental and sustaining engineering activities.

4.2.1 It is not the intent of this document to make system safety personnel responsible for hazard management in other functional disciplines. However, all functional disciplines using this generic methodology should coordinate their efforts as part of the overall SE process because ~~mitigation~~ control measures optimized for only one discipline may create hazards in other disciplines.

4.2.2 Other functional discipline application of MIL-STD-882F methodology should refer to identified risk as (functional) risk. *For example, environmental risks, Air-worthiness non-compliances, test safety risk, etc.*

9.6 Is additional guidance needed (to avoid confusion) that requires other disciplines to document how MIL-STD-882F will be used/interpreted for other discipline needs? This will help differentiate how applying MIL-STD-882F system safety methodology differs from the other discipline applications.

Commented [PDANUAA59]: 9-5
Addressing a technical error in MIL-STD-882E. Intent is for Sections 3 & 4 to apply whenever 882 is invoked on a contract. In addition, when specific 882 Tasks are called out, the requirements in those tasks are also applicable.

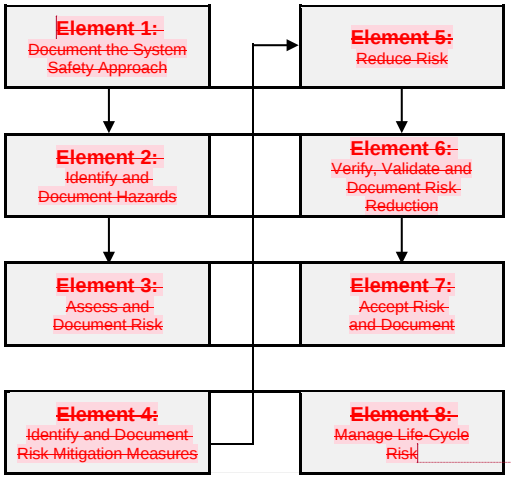
Commented [PDANUAA60]: 9-1
Format change to separate into distinct topics that make it easier to use/cite.

Commented [PDANUAA61]: See ii-2

Commented [PDANUAA62]: 9-2
Clarification to preclude non-system safety risks from being confused with system safety risks

Commented [PDANUAA63]: 9-6
Question needs to be addressed

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



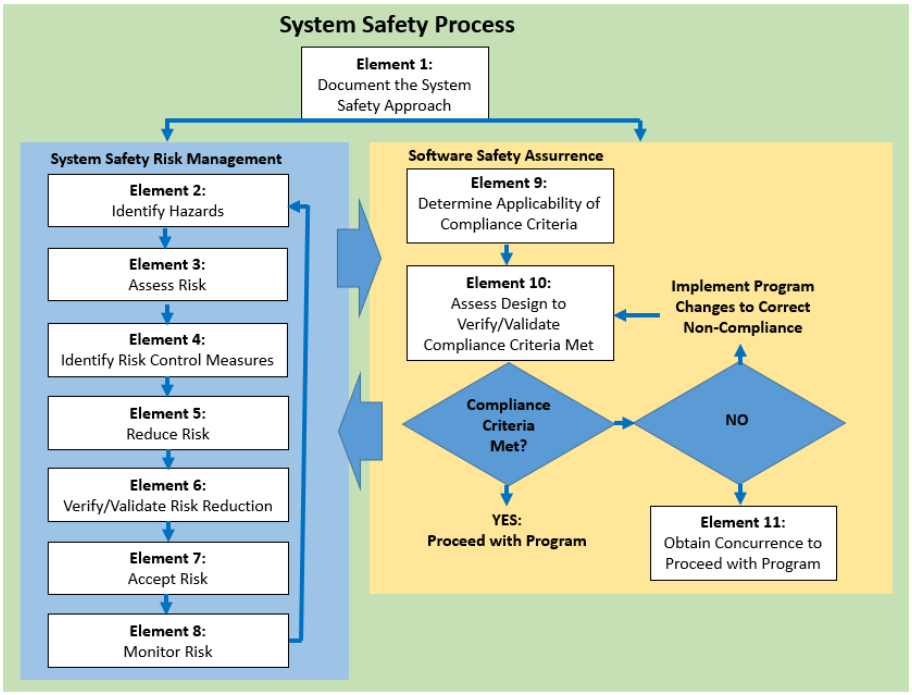


FIGURE 1. ~~Eight~~ elements of the system safety process

Commented [PDANUAA64]: 9-4
These 8 elements address the risk management process yet does not address software safety compliance. Therefore, this figure is incomplete.

See Revised process flow to address both the hazard analyses process as well as the software safety compliance activities.

Commented [PDANUAA65]: 9-7
Title revision to reflect revised figure

9-8
Are there other forms of compliance (beyond software safety assurance, AI & machine learning safety assurance) that needs to be addressed in 882F?

Commented [PDANUAA66]: 9-8
Question needing to be addressed

9-9
FUTURE ACTION: Realign text discussions corresponding to elements. An introduction section also needed to address the synergies between risk management and compliance. Ensure each element discussion addresses the entire life cycle.

Proposed revised outline
Para 4.3 System Safety Process overview (Element 1) top level discussion with pointers to para 4.4 and 4.5 as applicable. Emphasis on system safety over the life cycle
Para 4.4 System Safety Risk Acceptance Process (Elements 2-8) Detailed discussion currently in 4.3.2 through 4.3.8
Para 4.5 Software Safety Assurance (compliance / Elements 9-11)
Para 4.6 System Safety Challenges (addresses emerging software topics)

Commented [PDANUAA67]: 9-9
Additional restructuring required (lacked time to incorporate into this initial draft)

4.3.1 Element 1: Document the system safety approach. The PM and contractor shall document the system safety approach for managing hazards over the life cycle as an integral part of the SE process. The minimum requirements for the approach include:

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

4.3.1.2 Identifying and documenting the prescribed and derived requirements applicable to the system. ~~Examples include Insensitive Munitions (IM) requirements, Electromagnetic Environmental Effects (E3) requirements, pollution prevention mandates, design requirem cnts, technology considerations, and occupational and community noise standards.~~ Once the requirements are identified, ensure their inclusion in the system specifications and the flow-down of applicable requirements to subcontractors, vendors, and suppliers. *Examples include Insensitive Munitions (IM) requirements, Electromagnetic Environmental Effects (E3) requirements, pollution prevention mandates, design requirements, technology considerations, software safety assurance Level of Rigor (LOR) activities, and occupational and community noise standards*.

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

10.1 DoDI 5000.02 Change

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

4.3.1.4 A closed-loop Hazard Tracking System (HTS) shall be used to document hazards. The HTS shall include, as a minimum, the following data elements:

a. identified hazards,
b. associated mishaps,
c. causal factors
d. hazard effects
e. ~~risk assessments~~ hazard risk index (initial, target, event(s)),
f. identified risk control measures,
g. selected control measures,
h. verification of risk reductions
i. hazard status, and
j. risk acceptances.

Commented [PDANUAA68]: 10.6
Added "Element 1" to tie para to Figure 1
Underlined header

Commented [PDANUAA69]: 10.9
Emphasizing all of system safety should be considered over the life cycle

Commented [PDANUAA70]: Was 4.3.1.a.
Renumbered to make easier to cite.

Commented [PDANUAA71]: Was 4.3.1.b
Renumbered to make easier to cite

Commented [PDANUAA72]: 10.5
Format Change/Clarification – move example to end of para so discussion after example does not get confused with the example.
LOR activities added to example as this is another source that drives design/design process requirements into the design

Commented [PDANUAA73]: Was 4.3.1.c
Renumbered to make easier to cite

Commented [PDANUAA74]: 10-1
TBD Revision needed (see ii-1)

Commented [PDANUAA75]: 10-2
Was 4.3.1.d
Renumbered and split to make easier to cite discrete requirements
Format change to make easier to read
Revised list

Commented [PDANUAA76]: FUTURE ACTION: Scrub minimal HTS fields in this para and 2XX Tasks to remove duplications & unnecessary fields.

4.3.1.5 Additional unique HTS requirements are identified in each of the 2XX tasks and shall expand the lists of minimal data elements when task(s) are placed on contract.

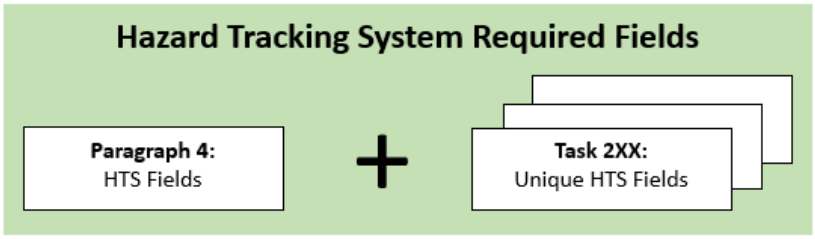


FIGURE 2. Hazard Tracking System Required Fields

4.3.1.6. Both the contractor and Government shall have access to the HTS with appropriate controls on data management.

4.3.1.7 The Government shall receive and retain "government purpose rights" of all the data recorded in the HTS and any other items (i.e., studies, analyses, test data, notes or similar data) generated in the performance of the contract with respect to the HTS.

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

4.3.2 Element 2: Identify and document hazards. Hazards are identified through a systematic analysis process that includes system hardware and software, system interfaces (to include human interfaces), and the intended use or application and operational environment.

4.3.2.1 Numerous sources may be considered to identify hazards to include, but not limited to:

a. mishap data
b. relevant environmental and occupational health data
c. user physical characteristics
d. user knowledge, skills, and abilities
e. lessons learned from legacy and similar systems.

4.3.2.2 The hazard identification process shall consider the entire system life-cycle and potential impacts to personnel, infrastructure, defense systems, the public, and the environment.

4.3.2.3 Identified hazards shall be documented in the HTS.

Commented [PDANUAA77]: See 10.2
Addresses additional unique Task 2xx HTS fields. These unique fields reflect the differences embedded in each hazard analyses task. In other words, PHA, SSHA, SHA, O&SHA, etc each have a different hazard analyses focus.

Commented [PDANUAA78]: See 10.2

Commented [PDANUAA79]: See 10.2

Commented [PDANUAA80]: 10.7
Added to tie para to Figure 1
Reformatted to ease readability

Commented [PDANUAA81]: See 10.7
FUTURE ACTION: Sources to consult to identify hazards need to be added to Appendix A.

4.3.3 Element 3: Assess and document risk. The severity category and probability level of the potential mishap(s) for each hazard across all system modes are assessed using the definitions in Tables I and II.

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

10.3 Add Loss/Compromise of data to severity categories. Proposed revision of para:

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

<develop revised words in Table 1 required to stratify severity categories>

Potential Issue: How to define the degree of harm as a result of loss of data..

10.4 The Hazard Severity Table does not address incapacitation.

<develop revised words in Table 1 required to stratify severity categories>

Possible factors to consider in stratifying the severity categories include Long term, Short Term, Congitive Degratation, Disortientation

10.10 The Hazard Severity Table does not address orbital mishaps

<develop revised words in Table 1 required to stratify severity categories>

Commented [PDANUAA82]: 10.8
Added to tie para to Figure 1

Commented [PDANUAA83]: 10.3
Should Loss/Compromise of data be included in severity definition?
<Need to develop new words in Table 1 is required>

Commented [PDANUAA84]: 10-4;
Should incapacitation be added to the severity definition?
<Need to develop proposed words & corresponding words in Table I to ensure stratification of severity categories for stratification is doable. >

Commented [PDANUAA85]: 10-10;
Should orbital mishaps be added to the severity definition?
<Need to develop proposed words & corresponding words in Table I to ensure stratification of severity categories for stratification is doable. >

TABLE I. Severity categories

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

Commented [PDANUAA86]: Table reworked.
See 11.1, 11.2, & 11.3 on page 11.a

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

Commented [PDANUAA87]: See 11.1
Commented [PDANUAA88]: See 11.2
Commented [PDANUAA89]: See 11.3
Commented [PDANUAA90]: See 11.1
Commented [PDANUAA91]: See 11.2
Commented [PDANUAA92]: See 11.3
Commented [PDANUAA93]: See 11.1
Commented [PDANUAA94]: See 11.2
Commented [PDANUAA95]: See 11.3
Commented [PDANUAA96]: See 11.1
Commented [PDANUAA97]: See 11.2
Commented [PDANUAA98]: See 11.3

11.1 The Hazard Severity Table does not include the loss of test data. Need to develop verbiage for each severity category to stratify levels of impact loss of data imposes.

Commented [PDANUAA99]: 11-1 (see 10-3)
Should loss/corruption of (test) data be added to the severity table

11.2 The Hazard Severity Table does not include the temporary incapacitation verbiage. Need to develop verbiage for each severity category to stratify levels of impact incapacitation imposes.

Commented [PDANUAA100]: 11-2 (see 10-4)
Should incapacitation be added to the severity table

11.3 The Hazard Severity Table needs to be adjusted for orbiting mishaps in space. Does "orbital mission capability" need to be defined/clarified? Does primary, secondary, tertiary capabilities need o be defined/clarified?

Commented [PDANUAA101]: 11-3
Should severity definition be adjusted for orbital loss/damage?

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

TABLE II. Probability levels

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

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

11.7 Example probability levels. A statement should be included that each program should determine their own quantitative values.

Commented [PDANUAA102]: 11-4;
Renumber (was subpara (4.3.3.b))

*Struck sentence moved to para 4.3.3.2.4 **see pg 12**

Commented [PDANUAA103]: 11-6
Expand verbiage on "Eliminated"
See 4.3.1.2.4

Commented [PDANUAA104]: 11-5
Correcting typo

Commented [PDANUAA105]: 11-7
Question needs to be addressed

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

4.3.3.2.3 All assumptions made in deriving the probability level shall be documented.

4.3.3.2.4 Probability level F is used to document cases where the hazard is no longer present in the design. No amount of doctrine, training, warning, caution, or Personal Protective Equipment (PPE) can move a mishap probability to level F.

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

TABLE III. ~~Risk assessment matrix~~ Hazard Risk Index

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

Commented [PDANUAA106]: 12-1
Incorporation of best practice

Commented [PDANUAA107]: See 11-4
Format change (discussion moved) to improve readability

Commented [PDANUAA108]: 12-2
Change RAC to HRI. Note HRI was the term used in MIL-STD-882C

Commented [PDANUAA109]: 12-3
Change RAC to HRI. Note HRI was the term used in MIL-STD-882C

Commented [PDANUAA110]: Delete Table & Replace with below (12-3 & 12-4)

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

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

4.3.3.5 The Program shall document all numerical definitions of probability used in risk assessments as required by 4.3.1.

4.3.3.5.1 Assessed risks shall be documented in the HTS.

4.3.3.6 Split Risk: Occasionally, a hazard is identified that has a spectrum of hazard severities and probabilities associated with it. Each realization of hazard on Table III may be valid and the corresponding controls may be different. Such a spectrum permits the PM to fully assess an issue so that controls can be better aligned. Risk acceptance shall be accomplished at the most demanding level. *For example, a hazard could be defined as a Catastrophic/Remote (e.g. ID), Critical/Occasional (e.g. IIC), Marginal/Probable (e.g. IIIB). It may be more effective to institute an inspection while the hazard is at a IIIB before more invasive repairs are needed when the hazard progresses to IIC or ID. Risk acceptance shall be accomplished as a Serious Risk.*

Commented [PDANUAA111]: 12-3
Chang title from RAC to HRI

Commented [PDANUAA112]: 12-4
Change colors of cells in table. "Stop light" scheme for High, Serious, Medium.
1.This is more intuitive than the Red/Orange/Yellow scheme
2.This color scheme provides greater contrast between colors. Depending of the projector/printer, Red & Orange often bleed together or Orange & Yellow often bleed together.

Commented [PDANUAA113]: 12-5
Change RAC to HRI

Commented [PDANUAA114]: 12-8
Added best practice that provides flexibility to the SSE to explain the nuances of the risk

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

4.3.4 Element 4: Identify and document risk control measures. Potential risk control(s) shall be identified, and the expected risk reduction(s) of the alternative(s) shall be estimated and documented in the HTS.

4.3.4.1 System Safety Design Order of Precedence: The system safety design order of precedence identifies alternative ~~mitigation~~ control approaches and lists them in order of decreasing effectiveness.

Commented [PDANUAA115]: 12-6 Format change to improve readabiltiy

Commented [PDANUAA116]: 12-7
Added to tie para to Figure 1

Commented [PDANUAA117]: 12-6
System Safety Order of Precedence is a key aspect of the system safety process. Having a separate para makes this easier to cite

Commented [PDANUAA118]: See ii-2

4.3.4.1.1 **Eliminate hazards through design selection**. Ideally, the hazard should be eliminated by selecting a design or material alternative that removes the hazard altogether. In other words, the hazard no longer exists in the design.

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

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

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

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

4.3.4.2 Risk control(s) are accomplished by mitigating the hazard (i.e. reducing the probability of the hazard) or by ameliorating the hazard (i.e. reducing the severity of the hazard).

4.3.4.2.1 Risk controls may be applied individually or in combination.

4.3.4.2.2 Risk controls may target hazard causal factors or hazard effects.

4.3.4.2.3 Each cause-effect path shall be controlled. In other words, each cause-effect path shall be interrupted by a control.

4.3.4.2.4 Controls used on the dominant cause-effect path shall be highlighted.

4.3.4.2.5 Probabilities shall be calculated for each cause-effect path. The sum of all cause-effect probabilities shall be used as the hazard probability.

4.3.4.2.6 All risk reduction control assumptions shall be documented.

4.3.4.2.7 Each risk reduction control should estimate the amount of risk reduction associated with the measure.

Commented [PDANUAA119]: 13-1
Clarification

Commented [PDANUAA120]: See ii-2

Commented [PDANUAA121]: See ii-2

Commented [PDANUAA122]: 13-8 Clarification of terminology:
- Control
- Mitigation
- Ameliorating

Commented [PDANUAA123]: The dominant cause-effect path has the greatest effect on controlling a hazard.

Commented [PDANUAA124]: 13-10
Best practice to ensure ALL cause-effect paths have been properly controlled

Commented [PDANUAA125]: 13-9
Best practices establishing rules of how controls shall be used

4.3.4.2.8 Applying warning device(s), or incorporating signage, procedures, training, and/or PPEs as controls by themselves shall not solely reduce the risk level by an order of magnitude.

4.3.4.3 The goal should always be to eliminate the hazard if possible.

4.3.4.4 When a hazard cannot be eliminated, the associated risk should be reduced to the lowest acceptable level within the constraints of cost, schedule, and performance by applying the system safety design order of precedence.

4.3.5 Element 5: Reduce risk. ~~Mitigation~~ Control measures are selected and implemented to achieve an acceptable risk level. Consider and evaluate the cost, feasibility, and effectiveness of candidate ~~mitigation~~ control methods as part of the SE and Integrated Product Team (IPT) processes. Present the current hazards, their associated severity and probability assessments, and status of risk reduction efforts at technical reviews.

4.3.5.1 The contractor shall define verification and validation approaches for each design requirement to control hazard risk.

4.3.6 Element 6: Verify, validate, and document risk reduction. Verify the implementation and validate the effectiveness of all selected risk ~~mitigation~~ control measures through appropriate analysis, testing, demonstration, or inspection. Document the verification and validation in the HTS.

13-8:

4.3.6.1 Documentation shall include a clear indication of which recommended control measure(s) program management concurred with and rational for rejected recommended control measure(s).

Pro: This builds a clear audit trail of what control measures were accepted or rejected and why. This could help future system safety efforts IF fielded system behavior shows that assumptions of risk reduction were in error. This will help accelerate subsequent risk control activities.

Con: The contractor may not have access to reasons why the government chose to incorporate or reject proposed control recommendations. This also represents a lot of additional work which could be argued to be not value added

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

Commented [PDANUAA126]: 13-11
Requirement to prevent abuse of controls inappropriately lowering High/Serious hazards without making fundamental design changes. These controls have documented limited effectiveness, hence they are inappropriate for SOLE control measures.

Commented [PDANUAA127]: 13-5
Added to tie para to Figure 1

Commented [PDANUAA128]: See ii-2

Commented [PDANUAA129]: See ii-2

Commented [PDANUAA130]: Moved from 882E para 203.2.1.c

Commented [PDANUAA131]: 13-6
Added to tie para to Figure 1

Commented [PDANUAA132]: See ii-2

Commented [PDANUAA133]: 13-8
Potential Add. Intention transferred from Task 203 (See comment 49-3)

Commented [PDANUAA134]: 13-14 Reformat to improve readability
(see pg 14 for continuation of para)

4.3.7 Element 7: Accept risk and document. Before exposing people, equipment, or the environment to known system-related hazards, the risks shall be accepted by the appropriate authority as defined in DoDI 5000.02.

DODI 5000.02 Change

4.3.7.1 The system configuration and associated documentation that supports the formal risk acceptance decision shall be provided to the Government for retention through the life of the system.

4.3.7.2 The definitions in Tables I and II, and the ~~RACs~~ HRIs in Table III, ~~and the criteria in Table VI for software~~ shall be used to define the risks at the time of the acceptance decision, unless tailored alternative definitions and/or a tailored matrix are formally approved in accordance with DoD Component policy.

4.3.7.3 The user representative shall be part of this process throughout the life-cycle of the system and shall provide formal concurrence before all Serious and High risk acceptance decisions.

Table VI criteria required; rewording needed as this suggests Table IV is used in risk management whereas Table IV is part of the Software Safety Assurance effort

Commented [PDANUAA135]: 13-7
Added to tie para to Figure 1

Commented [PDANUAA136]: 13-2
FUTURE ACTION: Reference to DODI 5000.02 will need to be revised

Commented [PDANUAA137]: 13-3
Change RAC to HRI

Commented [PDANUAA138]: 13-15
Incorrect reference. Table IV deals with programmatic safety risk, not hazards. As such, this is an incorrect reference.

Commented [PDANUAA139]: 13-4
FUTURE ACTION: Need to reword to differentiate software safety assurance (para 4.4) from hazards/risks (2xx tasks)

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

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

DODI 5000.02 Change

NOTE: 4.3.7.5 A single system may require multiple event risk assessments and acceptances throughout its life-cycle. Each event risk acceptance decision shall be documented in the HTS.

May need to expand the discussion associated with when event risk assessments are needed.

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

4.3.8 Element 8: Manage life-cycle risk. The program office use shall use the system safety process to iteratively identify hazards and maintain the HTS throughout the system's life-cycle.

4.3.8.1 Life-cycle management should consider any changes to include, but not limited to, the interfaces, users, hardware and software, mishap data, mission(s) or profile(s), and system health data.

4.3.8.2 Procedures shall be in place to ensure risk management personnel are aware of these changes, e.g., by being part of the configuration control process.

Commented [PDANUAA140]: (see pg 13a for 1st half of this para)

Commented [PDANUAA141]: 14-1
FUTURE ACTION: Reference to DODI 5000.02 will need to be revised

Commented [PDANUAA142]: 14-6 Format change. 2nd sentence has "Shall".

Commented [PDANUAA143]: 14-5
Reformat to increase readability

Commented [PDANUAA144]: 14-6
Bias to post fielding. Deleted so this para addresses the entire life cycle

Commented [PDANUAA145]: 14-4
Reworded to make contractually binding

Commented [PDANUAA146]: 14-5
Added to tie para to Figure 1

4.3.8.3 The program office and user community shall maintain effective communications to collaborate, identify, and manage new hazards and modified risks.

4.3.8.4 If a new hazard is discovered or a known hazard is determined to have a higher risk level than previously assessed, the new or revised risk shall be formally accepted in accordance with DoDI 5000.02.

DODI 5000.02 Change

4.3.8.5 In addition, DoD requires program offices to support system- related Class A and B (as defined in Department of Defense Instruction 6055.07) mishap investigations by providing analyses of hazards that contributed to the mishap and recommendations for materiel risk control measures, especially those that minimize human errors.

FUTURE ACTION: Revised **Figure 1** will require additional paras to discuss the new elements in the figure

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

4.4 Software Safety Assurance Approach. Throughout the Task 2xx series hazard analyses tasks, software's contribution to a system's hazard risk is explored. However, there are a number of software contributions related to system risks that are not easily addressed through hazard analyses. Therefore, a complementary approach shall be used to assess how the software is developed, tested, and certified. Through comparing potential risk severity with the degree of control software exercises over the system, level of rigor (LOR) criteria are defined. In addition, potential risk severity is compared to AI/machine learning develops LOR. Implementation of the combined LOR is used to build assurance that these contributions have been successfully managed. Thus, through these software safety assurance activities, many potential software safety issues are resolved. See Figure 2 below. Note these activities complement, not replace, the 2XX task hazard analyses.

Commented [PDANUAA147]: 14-4
Reworded to make contractually binding

Commented [PDANUAA148]: 14-2
FUTURE ACTION: Need to revise to appropriate DODI 5000.02 (or other) reference

Commented [PDANUAA149]: FUTURE ACTION: Verify reference is still correct

Commented [PDANUAA150]: 14-3
Para 4.4 completely reworked to provide clarification and greater requirement specificity.
New paras account for new aspects relating to software safety

Commented [PDANUAA151]: Para 4.4 has been completely overhauled to correct a number of technical errors, provide clarification, resolve sources of confusion, etc.

Para 4,4 is retitled "Software Safety Assurance" because, in essence, para 4.4 establishes a process to drive greater safety involvement in how software is designed, tested, and certified. Safety issues identified within this process do not adhere to the characteristics that define hazards (see 2XX tasks).

Safety issues identified in para 4.4 largely deal with "known unknowns", aka programmatic risks (e.g. cost, schedule, performance) with safety implications. Such safety issues are controlled through programmatic/systems engineering processes adjustments vice controls used for safety issues involving specific realizations of design requirements (aka safety hazard per Task 2XX tasks).

Retitling/refocusing/revising discussion more clearly differentiates it from the 2XX tasks.

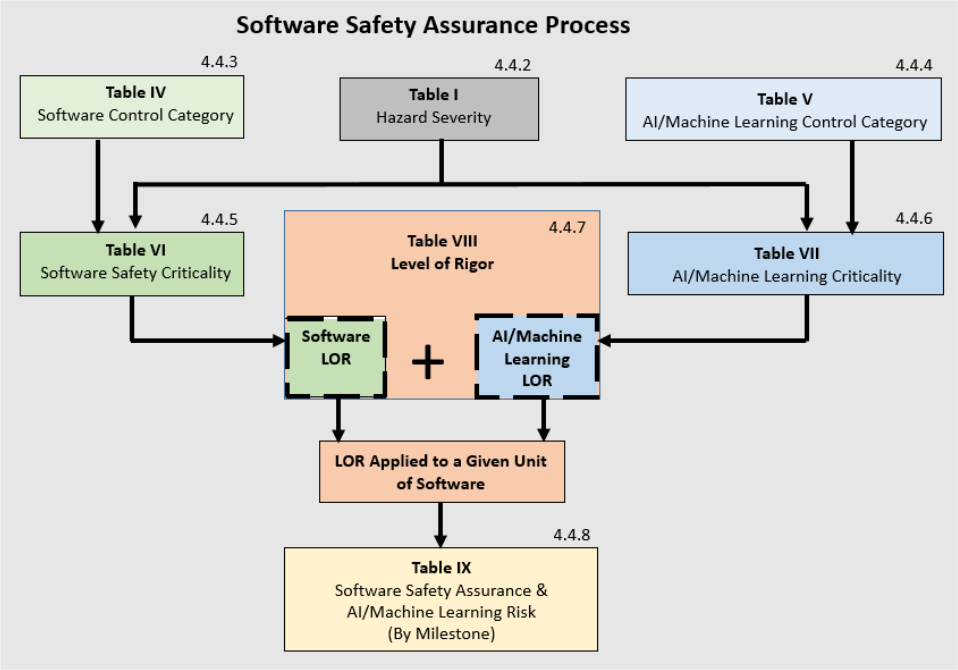


FIGURE 3: Software Safety Assurance Process

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

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

4.4.1 **Establishing the Software Safety Pedigree:** This activity lays the foundation for subsequent software safety assurance activities by ensuring the system elements hosting software or other logic embedded devices have been defined. The contractor shall document the following five areas to provide the framework defining the software safety pedigree.

Commented [PDANUAA152]: Added process flow to help navigate the software safety assurance process. Para references correlate the figure with corresponding discussion.

Commented [PDANUAA153]: 14.4 (See 14.3)

Commented [PDANUAA154]: This section to establish the baseline of how the software will be built, tested, and certified & environment the software will be run on.

4.4.1.1 **Software Development Environment:** This section comprises the tools that defines the environment in which the software in question shall be developed, tested, and certified. It is important to document any "settings" or other "options" that establish the configuration of these environment tools. Subsequent changes to "settings" or other "options" should be evaluated by the safety community to determine the potential safety impact to the object code. Such changes could introduce errors from the source code (which is typically analyzed) to how it is translated into the object code (which is typically executed in testing and during fielded systems).

4.4.1.2 **Software Architecture:** This section defines the architecture of the software being developed and how it fits into the hosting system(s). This includes software interfaces internal and external to the software project as well as associated control loops. This information may be used to establish the Task 208, Functional Hazard Analyses.

4.4.1.2.1 The contractor shall describe how software is decomposed into smaller software partitions/units.

4.4.1.3 **Hardware Architecture:** This section defines the architecture of the hardware hosting the software to include points where software affects control authority over hardware devices. This information may be used to establish in Task 208, Functional Hazard Analyses.

4.4.1.4 **Software-Like-Hardware:** Executed logic takes many forms. Logic recognized as software is addressed through software requirements. However, other logic forms act like software, but through technicalities, are not considered software.

4.4.1.4.1 All of these logical forms are deemed "Software-Like-Hardware" and shall be subject to all software requirements provided in this Military Standard.

4.4.1.4.2 All Software-Like-Hardware used in the system shall be defined as well as where in the hardware/software architecture these devices are being used.

4.4.1.4.3 Specifics on how the logic configuration of each of these devices is managed shall be included.

4.4.1.5 **Single Core Processing & Multi-Core Processing/Virtualization/ Containerization:** This section addresses specifically how the central processing units (CPUs) are being utilized within the design.

4.4.1.5.1 The contractor shall identify where single core processors and where multi-core processors are being used.

4.4.1.5.2 Through middleware (e.g. virtualization or containerization), a single processor may be used as a multi-core processor via virtualization and containerization techniques.

4.4.1.5.3 "Settings" and "options" that govern multi-core processing or the virtualization/containerization middleware shall be included.

Commented [PDANUAA155]: Being able to reference each software partition/unit is needed for (1) determining software control category [see 4.4.3], (2) assigning SwCI and corresponding LOR [see 4.4.5], (3) and to provide meaningful reference when the software partitions/units are cited in hazard analyses 2XX Tasks and other system safety documentation.

Referencing an OFP or CSCI is often too generic of a reference as the citation does not point to where in the software the issue/concern/control/etc resides.
This is akin to referencing a hydraulic system for a issue/concern/control/etc … but where in the hydraulic system is the interest? Being able to precisely identify the hydraulic component where the issue/concern exists allows for a specific control/ corrective action to be developed to resolve the issue.
System Safety documentation must be able to identify the same granularity with respect to software … what specific portion of the logic is of interest? Until such granularity is defined, then developing software controls for issues/concerns will be amorphous at best

4.4.1.5.4 The contractor shall identify design features incorporated to control common paths across multi-core processors, containerization, and/or virtualization to preclude one CPU (or virtual CPU) from interfering with other CPUs.

4.4.1.5.5 The contractor shall identify where in the architecture what CPUs are being used and how. This provides insight into potential common cause paths, system interdependencies, and system robustness.

4.4.2 **Determining Potential Software Severity:** The contractor shall determine the worst credible case potential consequence (see Table I) of the software unit if it does not function properly. Safety issues involved in software are categorized in two broad categories: (1) software control over hardware and (2) the information generated by software.

Commented [PDANUAA156]: Providing improved guidance on how software severities are derived.

4.4.2.1 **Software Control Over Hardware:** Where software is controlling hardware, there are numerous ways safety issues can be introduced. Incorrect commanding, latent commanding, and inadvertent commanding are a few examples of how safety hazards can result from software control over hardware.

4.4.2.2 **Software Generated Information:** Information generated by software can be used by either a human operator or other software. Incorrect information, latent information, and inadvertent commanding are a few examples of how safety hazards can result from software generated information. With respect to the human operator, one must consider the role of the human in the system's operation. In some systems, the human has time to contemplate and decide if the information the software is generating is correct and has time to override the system's operations. In other systems, the human is implicitly trusting the software and autonomously acting upon that software

4.4.2.3 **System Perspective:** Potential software issue effects must be translated to the impacts imparted upon the total system. *For example, the software operating on a single CPU may completely cease to function. However, if such a catastrophic effect on a CPU has a negligible effect on the system operation, then negligible severity is applicable*.

4.4.2.4 Considerations for determining potential software severity shall include:

a. How the software is being used in a system over all operational and maintenance modes
b. The time scale upon which software executes compared to that of the system and human operator operates
c. AI and machine learning implementation

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

4.4.3 **Software Control Category:** Table IV depict the degree of software control in a system.

4.4.3.1 For each software unit, the contractor shall use the lowest applicable software control category level (e.g. software control category 1 – Autonomous shall be used before software control category 2 – Semi-Autonomous).

TABLE IV. Software control categories

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

Commented [PDANUAA157]: See 14.3 & 14.4

Commented [PDANUAA158]: Table IV revision; cleaned up definitions

Commented [PDANUAA159]: 15-7
Establishing guidance of how to choose SWCI.

NOTE – it is important to identify the correct SWCI level early in a program, as the corresponding SW LOR drive programmatic actions/requirements. Identifying too low a SWCI may drive excessive requirements.

Likewise, too high a SWCI introduces the possibility of identifying a hazard which would is retroactively revise the SWCJ and corresponding LOR. Such revised requirements after the design baseline has been solidified imposes formal changes and hence additional cost.

Commented [PDANUAA160]: 15.1
Issues with Definition

Commented [PDANUAA161]: 15.2
Issues with Definition

Commented [PDANUAA162]: 15.3
Issues with Definition

Commented [PDANUAA163]: 15.4
Issues with Definition

TABLE IV: Software Control Categories

Software Control Categories		
Level	**Name**	**Description**
1	Autonomous	• Software functionality that exercises control authority over potentially safety-significant hardware systems, subsystems or components without the possibility of operator intervention to preclude the occurrence of a mishap or hazard. • Software generated information involving safety-significant time-sensitive system operations where the operator implicitly trusts the validity of the information.
2	Semi-Autonomous	• Software functionality that exercises control authority over potentially safety-significant hardware systems, subsystems, or components with the possibility (given time) of operator detection and intervention to control the mishap or hazard. • Software generated information involving safety-significant time-sensitive system operations where the operator has to opportunity to determine the validity of the information and correctly act.
3	Redundant Fault Tolerant	• Software functionality that exercises redundant, independent fault tolerant control authority over potentially safety-significant hardware systems, subsystems, or components that relies upon operator to complete the command function. • Software generated information involving redundant, independent fault tolerant control authority involving safety-significant system operations where the operator has to opportunity to determine the validity of the information and correctly act.
4	No Safety Impact	• Software functionality that does not possess command or control authority over safety significant hardware systems, subsystems, or components. • Software generated information that does not involve safety-significant systems.

15-7 Recommend focusing on number and/or degree of interlocks/controls that reduce the impact of the subject function. Parallel descriptions for control functions versus information providing functions would be useful.

Commented [PDANUAA164]: Revised definitions to address (1) technical errors (2) eliminate ambiguity (3) make easier to apply.

For each definition, two subbullets are included.
- The 1st subbullet addresses implications of where software is interfacing with hardware
- The 2nd subbullet addresses implications of where software if interfacing with software OR providing information to the Operator/Maintainer

Content for each definition has been refined for clarity & removal of a bias against software generated information.

(This definion …) was deleted as it redefined the stated definition in different terms, thereby introducing conflicts. It is unclear if the definition applied if part of the examples provided applied and other parts did not apply. Furthermore, technological advancements made this items listed OBEd in several respects.

"Influential" category was deleted as it only addressed safety related (e.g. Marginal, Neg.) severities & that it introduced a bias against software generated information.

Commented [PDANUAA165]: See 15--1

Commented [PDANUAA166]: See 15-2

Commented [PDANUAA167]: See 15-3

Commented [PDANUAA168]: 15-7 FUTURE ACTION to Consider

4.4.4 **Artificial Intelligence/Machine Learning Category:** Artificial Intelligence (AI) has become increasingly pervasive in a system designs. Part of AI is the ability of the system to learn, or Machine Learning. As with AI, there are different stratification levels that account for the different extents systems can learn. Table V provides a stratification of different levels of AI:

FUTURE ACTION: This discussion needs to be further defined.
Note that 4.4.4 is not intended to duplicate para 4.4.3, but rather to focus on those aspects of AI/Machine Learning that go beyond "traditional software". The algorithms realized through software code are what is of interest.

- How do these algorithms spot the patterns upon which machine learning is based?
- How does system safety determine if there is causation with correlation of these algorithms?

TABLE V: Artificial Intelligence Categories

Artificial Intelligence Categories		
Level	**Name**	**Description**
1	Add categories	• Add definitions
2	TBD	•
3	TBD	•
4	TBD	•
5	TBD	•
6	TBD	•
7	TBD	•
8	TBD	•
9	TBD	•
10	No AI/Machine Learning Incorporated	The system design does not possess AI or Machine Leaning in its design.

4.4.4.1 For each software unit, the contractor shall use the lowest applicable AI Control category level (e.g. AI/Machine Learning control category 1 – TBD shall be used before AI/Machine Learning control category 2 – TBD).

15-8: FUTURE ACTION: May need to make some distinction between the software that captures the machine learning versus the software that executes the learned behavior. A more conventional/deterministic approach for the learning software and a more probabilistic approach for the software executing the learning.

Commented [PDANUAA169]: Lead-in discussion to how AI / Machine Learning

See 15-5

The AI/Machine Learning Category is mirrored after the software control category (4.4.3) construct but with different content/objectives.

Commented [PDANUAA170]: FUTURE ACTION: Develop this table

Definitions in this table must be distinct from those in Table IV. Ideally, these definition will not be based on **Autonomous**, **Semi-Autonomous**, **Redundant Fault Tolerant** terms

Assumption is there are no interdependencies between AI or Machine Learning terms. If this assumption does not hold true, then each AI/Machine Learning LOR will be distinct list of activities vs cascading list as used in the SW LOR

The number of subcategories shall be aligned to the stratification of this table

Commented [PDANUAA171]: Required to make process work.
Software that does not involve AI or Machine Learning will not impose additional LOR activities. This category is an "off ramp" to make this process flow work.

Commented [PDANUAA172]: Establishing guidance of how to choose AICI (parallel approach to what used to determine SWCI).

NOTE – it is important to identify the correct SWCI level early in a program, as the corresponding SW LOR drive programmatic actions/requirements. Identifying too low a SWCI may drive excessive requirements.

Likewise, too high a SWCI introduces the possibility of identifying a hazard which would is retroactively revise the SWCJ and corresponding LOR. Such revised requirements after the design baseline has been solidified imposes formal changes and hence additional cost.

Commented [PDANUAA173]: 15-8

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

TABLE V. Software safety criticality matrix

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

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

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

Commented [PDANUAA174]: 16.1
Para 4.4.2 has been reworked into para 4.4.5

Commented [PDANUAA175]: 16.2
Table V has been reworked into Table VI. Further rework required due to changes in Table IV.

Commented [PDANUAA176]: Reworked into Table VIII

Commented [PDANUAA177]: 16-5
Neither of these documents provided the additional guidance needed. Therefore, these references are deleted.

4.4.5 **Software Criticality Index (SWCI):** The SWCI determination is used to determine the Level of Rigor (LOR) of software safety assurance activities to be imposed on the software. Correlating the results from Tables II and IV, a SWCI designation is derived.

TABLE VI. Software safety criticality matrix

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

FUTURE ACTION: Need to develop solid rationale as to why each SWCI level was determined for each cell. It has to be more than just "makes the chart look symmetrical"; there MUST be solid logic

Commented [PDANUAA178]: Describing process of deriving SWCL that will lead to SW driven LOR

Commented [PDANUAA179]: 16.2
Table V: Need to develop solid rationale as to why each SWCI level was determined for each cell. It has to be more than just "makes the chart look symmetrical"; there MUST be solid logic

FUTURE ACTION: Document in Appendix the rationale for why the SWCI level has been assigned to each cell.

4.4.6 **Artificial Intelligence Criticality Index (AICI):** The AICI determination is used to determine the LOR of software safety assurance activities to be imposed on the software. Correlating the results from Tables II and V, a AICI designation is derived.

TABLE VII: Artificial Intelligence Criticality Matrix

ARTIFICIAL INTELLIGENCE CRITICALITY MATRIX				
	SEVERITY CATEGORY			
AI / MACHINE LEARNING CONTROL CATEGORY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
1	AICI 1	AICI 1	AICI 3	AICI 4
2	AICI 1	AICI 2	AICI 3	AICI 4
…	…	…	…	…
#	AICI #	AICI #	AICI #	AICI #

FUTURE ACTION: Need to develop solid rationale as to why each AICI level was determined for each cell. It has to be more than just "makes the chart look symmetrical"; there MUST be solid logic

Commented [PDANUAA180]: Describing the process of deriving SAII that will lead to AI driven LOR
Note para 4.4.6 parallels para 4.4.5

Commented [PDANUAA181]: 16.2
FUTURE ACTION: Develop this table

Commented [PDANUAA182]: 16-3 (See 16-2)
Table VI Need to develop solid rationale as to why each AICI level was determined for each cell. It has to be more than just "makes the chart look symmetrical"; there MUST be solid logic
Document in Appendix

FUTURE ACTION: Document in Appendix the rationale for why the SWCI level has been assigned to each cell.

4.4.7 **Level of Rigor:** LOR defines a set of gradated activities that correlate activities required to build confidence that software was developed, tested, and certified in a safe manner.

4.4.7.1 LOR process overview: The LOR process is depicted in Figure 3.

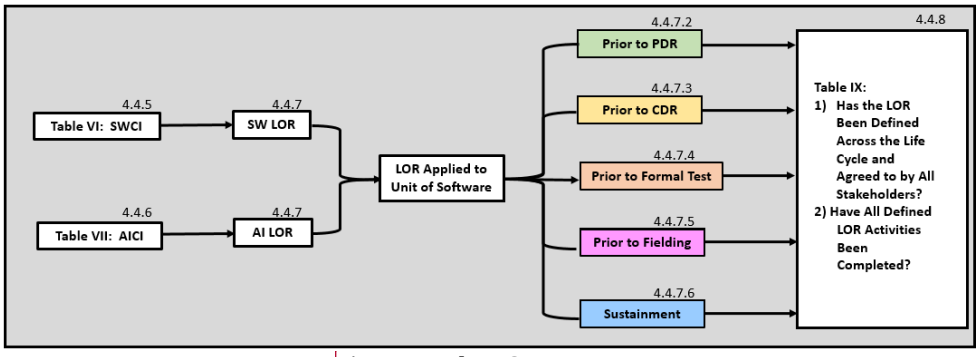


Figure 4: The LOR Process

4.4.7.1.1 Each SwCI or SAII level corresponds to a corresponding SW LOR or AI LOR designation for the designated unit of software. This is depicted in Table VIII.

4.4.7.1.2 Each SW LOR or AI LOR has a corresponding list of activities required for the designated unit of software.

4.4.7.1.3 LOR activities are phased over the program life cycle. Thus, corresponding life cycle events provide a definitive assessment point to evaluate LOR implementation.

4.4.7.1.4 The LOR activity list shall be jointly tailored between the contracting agency and the contracted agency as well as between the safety community and the software development community.

4.4.7.1.5 Each designated unit of software shall fully implement the resultant LOR activity list.

4.4.7.1.6 Examples of LOR activities are provided in Appendix C. These activities are arranged along a programs life cycle (or nearest equivalent) and are intended to be tailored.

TABLE VIII. Level of Rigor Activities

LEVEL OF RIGOR ACTIVITIES				
SwCI 1	SW LOR 1		AICI 1	AI LOR 1
SwCI 2	SW LOR 2		AICI 2	AI LOR 2
SwCI 3	SW LOR 3		…	….
SwCI 4	SW LOR 4		AICI #	AI LOR #

Commented [PDANUAA183]: Revised LOR description; Software safety assurance activities.
Also, links LOR structure to program milestones to better target/scope LOR activities. This allows incremental assessment of LOR implementation progress. LOR activity assessments could easily be incorporated into milestone entry/exit criteria, thus placing greater software safety emphasis on milestone completion. As such, LOR activities become a powerful tool anchored in the acquisition process for system safety to influence the safety of a system's software! (See 17-2 & para 4.4.8)
By extension, it better frames the LOR risks outlined in Figure 4 for the corresponding RAA. *For example, a LOR risk at CDR would be applicable from CDR to Formal Flight Test. When assessing the Formal Test LOR, if no further LOR non-compliances are noted, no further CDR LOR risk acceptance action is needed. Thus, this provides an incentive path for the program offices to "get well" (an aspect missing from 882E)*

Commented [PDANUAA184]: Added process flow chart to help navigate the software LOR process.
Para references correlate the figure with corresponding discussion.

Commented [PDANUAA185]: 16.4
FUTURE ACTION: Table V will need to be reworked to account for Table VII.

4.4.7.2 **Prior to Preliminary Design Review (PDR):** Approaching PDR, the tailored set of PDR LOR activities shall be accomplished. These activities focus on ensuring the foundation of the software safety assurance effort has been defined.

4.4.7.3 **Prior to Critical Design Review (CDR):** Approaching CDR, the tailored set of CDR LOR activities shall be accomplished. These activities focus on ensuring the software safety assurance efforts associated with the design development have been accomplished.

4.4.7.4 **Prior to Formal Testing:** Approaching formal testing, the tailored set of testing LOR activities shall be accomplished. These activities focus on ensuring the software safety assurance efforts associated with how the software shall be tested and certified have been accomplished.

4.4.7.4.1 **Testing & Certification:** Safety shall review of test results to determine if LOR criteria have been met, identify new hazards, monitor effectiveness of hazard control implementation.

4.4.7.4.2 **Anomalies:** Anomalies and other discrepancies identified during testing or fielding shall be reviewed for safety impacts.

4.4.7.5 **Prior to Fielding:** Approaching fielding of the system, the tailored set of fielding LOR activities shall be accomplished. These activities focus on ensuring the software safety assurance efforts associated with the fielding have been accomplished.

4.4.7.6 **Sustainment:** Approaching the sustainment phase of a program, the tailored set of sustainment LOR activities shall be accomplished. These activities focus on ensuring the software safety assurance efforts associated with the sustaining the software.

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

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

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

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

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

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

Commented [PDANUAA186]: 17.1
882E Table VI reworked into 882F Figure 4 & Table IX

4.4.8 **Software Safety Assurance Progress Check:** At each designated program event LOR activities are aligned to a program event (e.g. prior to PDR, prior to CDR, prior to test, prior to fielding, & sustainment). These progress checks should be incorporated into the program event's entry/exit criteria. The following questions shall be addressed for every "unit" of software:

4.4.8.1 **LOR Definition/Planning:**

4.4.8.1.1 Prior to PDR, has the LOR activities been defined?

4.4.8.1.2 At the completion of a program milestones (e.g. PDR, CDR, formal testing, fielding), has the defined LOR been validated for the following milestone (e.g. CDR, formal testing, fielding, sustainment)?

4.4.8.2 **LOR Execution:** Prior to each designated program event, have all of the associated LOR activities been completed?

Table IX: Software Safety Assurance Risk

SWCI	AICI	Software Safety Assurance Risk Level	Para 4.4.8.1/4.4.8.2 Non-Compliance Risk Acceptance Authority
I	I	High	SAE/CAE
II	II	Serious	PEO or Designated Equivalent
III	III	Medium/Low	PM
IV	IV	Not Safety	PM

4.5 **Additional System Safety Challenges**:

4.5.1 **NDI:** Applying existing design components to a new design introduces potential safety concerns. Changes in the design environment may result in NDI (to include COTS, GOTS, REUSED, etc) being subjected to an environment it was never designed for. Furthermore, there are limited options available to modify NDI components. In addition, the system safety practitioner often lacks insight into the details of NDI products, thus NDI products are frequently treated as "Black Boxes" in analyses. Additional risk is thereby assumed as details within the NDI product may result in introducing hazards.

4.5.1.1 The contractor shall identify all NDI hardware and software used in the system.

4.5.1.2 The contractor shall obtain MA approval of how NDI shall be addressed in hazard analyses.

4.5.1.3 The contractor shall obtain MA approval of how NDI software shall be addressed in LOR activities.

4.5.1.4 The contractor shall obtain MA approval of hazard controls directly impacting NDI items.

Commented [PDANUAA187]: 17-2
Questions (see 882E Table VI) reframed in current process. Aligning progress check to milestone entry/exit criteria is **"Should"** as 882F is not the parent document to define entry/exit criteria

Commented [PDANUAA188]: Intent here is to ensure the LOR is define early in the program so that the program can properly plan to accomplish all of the LOR element. Reduces the potential for programmatic surprises.

Commented [PDANUAA189]: Intent here is to acknowledge that during the acquisition life cycle, programmatic adjustments are needed. Thus, upon completion of PDR, the criteria for CDR LOR needs to be validated thereby providing ample opportunity for a program to properly plan & thus reduce the potential for programmatic surprises.

Commented [PDANUAA190]: FUTURE ACTION: Verify SWCI & AICI levels are correctly stated in this chart (earlier tables requiring additional work)

Commented [PDANUAA191]: This para addresses a number of new topics to 882 that are should be addressed. Though many have software safety linkage, they are actually much broader topics to include non-software safety

Commented [PDANUAA192]: This para addresses items that have been developed elsewhere and are being incorporated into the design.
NDI used as an umbrella term accounting for software in this category. Subsequent requirements focused on defining the rules of how a program will address these items as part of the system safety program.

Commented [PDANUAA193]: Addresses elements 2-8 and 2XX Tasks.

Commented [PDANUAA194]: Addresses through para 4.4

Commented [PDANUAA195]: Modifying NDI makes the item "modified NDI" which has life cycle acquisition impacts. MA must have a say before such impacts are made to protect government interests

4.5.2 **Middle Tiered Acquisition (MTA):** Programs under the MTA management construct operate in an accelerated manner that require safety products to be developed faster. This introduces additional challenges to the system safety practitioner to develop applicable safety products in a resource constrained environment with dynamically evolving requirements often using new technologies.

4.5.2.1 The contractor shall explain how system safety processes and products will be addressed in the MTA environment.

4.5.2.2 The contractor shall explain how system safety shall integrate MTA and non-MTA system safety efforts.

4.5.3 **Agile Software Development:** This management construct accelerates software development. The system safety practitioner is challenged with conducting system safety tasks/activities with a dynamically evolving requirements set.

4.5.3.1 The contractor shall explain how hazard analyses (e.g. 2xx Tasks) will be adapted to Agile Software Development to include integrating Agile Software program efforts with non-Agile Software program efforts.

4.5.3.2 The contractor shall explain how paragraph 4.4 and associated LOR activities will be adapted to Agile Software Development to include integrating Agile Software program efforts with non-Agile Software program efforts.

4.5.4 **Urgent Programs**: Urgent Programs operate in an accelerated manner that require safety products to be developed faster. This introduces additional challenges to the system safety practitioner to develop applicable safety products in a resource constrained environment with dynamically evolving requirements often using new technologies.

4.5.4.1 The contractor shall explain how system safety processes and products will be addressed in the urgent program environment.

4.5.4.2 The contractor shall explain how system safety shall integrate urgent and non- urgent program efforts to include hazard analyses tasks (e.g. 2xx Tasks).

4.5.4.3 The contractor shall explain how system safety shall integrate urgent and non- urgent program efforts to include LOR activities (e.g. para 4.4).

4.5.5 **Model Based Engineering:** Moving to a digital engineering environment offers some efficiencies while introduces new challenges.

4.5.5.1 The contractor shall explain how system safety will address incorporation of model based engineering into system safety processes and products to include LOR activities (e.g. para 4.4) and hazard analyses tasks (e.g. 2xx Tasks).

Commented [PDANUAA196]: This management construct is intended to accelerate acquisition timelines. As such, it introduces new challenges to the system safety program. How does one accomplish system safety activities in a shorter timeline with often more complex/emerging technologies?
Is highlighted text needed?

Commented [PDANUAA197]: This software development construct mirrors many MTA challenges in software safety

Commented [PDANUAA198]: Addresses elements 2-8 and 2XX Tasks

Commented [PDANUAA199]: Addresses through paragraph 4.4

Commented [PDANUAA200]: Further challenges are introduced into the system safety program with activities that are accelerated even faster than MTA

Can this para be merged with 4.5.2? Likewise, should address other non-traditional acquisition life cycle programs such as JION programs.

Commented [PDANUAA201]: Addresses elements 2-8 and 2XX Tasks

Commented [PDANUAA202]: Addresses through paragraph 4.4

Commented [PDANUAA203]: Model Based Engineering offers many opportunities to accelerate system safety activities while at the same time imposing significant challenges

Commented [PDANUAA204]: Addresses through paragraph 4.4

Commented [PDANUAA205]: Addresses elements 2-8 and 2XX Tasks

4.5.6 **Probabilistic vs Deterministic Software:** Software is often developed with a probabilistic expectation of producing a specific response. This presents new challenges in safety products which are often rooted in software deterministic requirements.

4.5.6.1 The contractor shall explain their rationale of how deterministic requirements are met in a probabilistic environment.

4.5.6.2 The contractor shall identify new tools and techniques used to conduct hazard analyses involving probabilistic software.

4.5.6.3 LOR activities shall be tailored to account for probabilistic software.

4.5.7 **Dead/Unused Code:** Code that has been abandoned or is not actively used in a system introduces potential software safety hazards in the system.

4.5.7.1 The contractor shall obtain MA approval on policy regarding Dead or Unused Code.

4.5.7.2 The contractor should eliminate Dead or Unused Code whenever possible, especially in the more severe SWCI levels. The contractor shall obtain MA approval on management or Dead or Unused Code and steps taken to ensure such code can never be exercised.

4.5.7.3 The contractor shall address how dead/unused code is accounted for in hazard analyses tasks.

4.5.7.4 The contractor shall address how dead/unused code is accounted for in LOR activities.

4.5.8 **Machine Learning/Deep Learning:** This poses a fundamental question of "how does system safety determine the safety of a lesson a machine has learned after being fielded?"

4.5.8.1 The contractor shall show how the causation is linked to correlation of patterns in data within a system.

4.5.8.2 The contractor shall address how machine learning/deep learning has been accounted for in hazard analyses tasks.

4.5.8.3 The contractor shall address how machine learning/deep learning has been accounted for in LOR activities.

4.5.9 **Artificial Intelligence:** AI is being introduced into systems in numerous applications. It is not uncommon for a system to possess multiple examples of AI. This introduces new complexities into system design

4.5.9.1 The contractor shall address how AI is being accounted for in hazard analyses tasks.

4.5.9.2 The contractor shall address how AI is being accounted for in the LOR activities.

Commented [PDANUAA206]: Since software has so many potential subtle influences, it can no longer be addressed from a deterministic perspective. Yet many of the legacy requirements are deterministic in nature. This impacts the system architecture as well as software

Commented [PDANUAA207]: Addresses elements 2-8 and 2XX Tasks

Commented [PDANUAA208]: Addresses through paragraph 4.4

Commented [PDANUAA209]: Dead/Unused code has been an acknowledged causal factor for decades, but frequently is allowed to remain in systems.

Commented [PDANUAA210]: Addresses elements 2-8 and 2XX Tasks

Commented [PDANUAA211]: Addresses through paragraph 4.4

Commented [PDANUAA212]: What additional safety implications does machine learning introduce? Paragraph 4.4 addressed the process of how machine learning will be categorized and used to define LOR levels. Paragraph 4.5.8 addresses specific questions related to machine learning.

Commented [PDANUAA213]: Addresses elements 2-8 and 2XX Tasks

Commented [PDANUAA214]: Addresses through paragraph 4.4

Commented [PDANUAA215]: What additional safety implications does AI introduce? Paragraph 4.4 addressed the process of how AI will be categorized and used to define LOR levels. Paragraph 4.5.8 addresses specific questions related to AI.

Commented [PDANUAA216]: Addresses elements 2-8 and 2XX Tasks

Commented [PDANUAA217]: Addresses through paragraph 4.4

4.5.9.3 The contractor shall address how multiple AI algorithms interact and how conflicts between AI algorithms are resolved.

4.5.10 **Cyber Safety:** Discrete systems are being fused into larger systems in unique and creative ways.

4.5.10.1 The contractor shall identify all cyber networks the program is connected to or interfaces with.

4.5.10.2 The contractor shall address how the program interfaces with cyber network(s).

4.5.10.3 The contractor shall address how cyber networks are accounted for in hazard analyses tasks.

4.5.10.4 The contractor shall address how cyber networks are accounted for in LOR activities.

Commented [PDANUAA218]: How should connectivity to cyber networks be addressed? Many new safety issues are introduced, such as distributed cyber components across many programs without contractual relationships

Commented [PDANUAA219]: Addresses elements 2-8 and 2XX Tasks

Commented [PDANUAA220]: Addresses through paragraph 4.4

5 DETAILED REQUIREMENTS

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

Appendices A, B, & C provide additional background/guidance/examples, but are not explicitly citable as being contractually binding. Does para 5.1 need to be reworded, because it implies they could be?

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

5.2 Tasks. The tasks in this Standard can be selectively applied to fit a tailored system safety effort. Each desired task shall be specifically called out in a contract because the task descriptions do not include requirements for any other tasks.

a. The 100-series tasks apply to management.
b. The 200-series tasks apply to analysis.
c. The 300-series tasks apply to evaluation.
d. The 400-series tasks apply to verification.

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

5.3.1 **Purpose:** The purpose explains the rationale for performing the task.

5.3.2 **Task Description:** The task description describes the work a contractor shall perform if the task is placed on contract. When preparing responses to proposals, the contractor may recommend inclusion of additional tasks ~~or deletion of specified tasks~~ with supporting rationale for each addition~~/deletion~~. 2XX Tasks are structured with the following additional paragraphs:

5.3.2.1 **Scope:** Description of what the hazard analyses task encompasses.

5.3.2.2 **Hazard Identification:** A listing of requirements associated with identifying hazards in the analyses.

5.3.2.3 **Hazard Characterization:** A listing of requirements associated with how hazards shall be characterized within the analyses.

5.3.2.4 **Assessing Risk:** A listing of requirements associated with how risk shall be derived from the hazards within the analyses.

Commented [PDANUAA221]: 18-6
Inclusion of additional materials (appendix C – LOR examples)

Commented [PDANUAA222]: 18-1
Format change to increase readability

Commented [PDANUAA223]: 18-2
Added header to increase readability

Commented [PDANUAA224]: 18-3
Added header to increase readability

Commented [PDANUAA225]: 18-4
Correcting incorrect scope

Commented [PDANUAA226]: New subparas outlining the structure of 2XX tasks.

5.3.2.5 **Identification of Potential Hazard Controls:** A listing of requirements associated with how hazard controls shall be derived within the analyses.

5.3.2.6 **Documentation:** A listing of requirements outlining the documentation of the analysis.

~~**5.3.c Details:** The details to be specified in each task description lists specific information, additions, modifications, deletions, or options to the requirements of the task that should be considered when requiring a task. This information is then included in the contractual document along with the task number. The list provided with each task is not necessarily complete and may be supplemented. Any task selected should be specifically imposed by task number in the Request for Proposal (RFP) and Statement of Work (SOW). The details to be specified that are annotated with an "(R)" are required. The Government provides these details to the contractor for proper implementation of the task.~~

5.3.3 **Hazard Tracking System (HTS) Fields:** In 2XX tasks, this paragraph documents those task unique fields that need to be included in the HTS.

6 NOTES

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

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

6.1.1 Other functional disciplines such as fire protection engineers, occupational health professionals, and environmental engineers may use the system safety standard practice. If this methodology is used by a different discipline, then guidance should be provided of detailing how MIL-STD-882F shall be adapted.

6.2 Acquisition requirements. Acquisition documents should specify the following:

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

Commented [PDANUAA227]: 18-5
Added header (Details) to increase readability

Paragraph deleted as it is not being followed. (R) details are not being included in SOW language.

Commented [PDANUAA228]: 18-7 clarification

Commented [PDANUAA229]: 18-8 reworded in 6.1.1 for clarification

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

DID Number	DID Title
DI-ADMIN-81250	Conference Minutes
DI-MISC-80043	Ammunition Data Card
DI-MISC-80370	Safety Engineering Analysis Report
DI-ILSS-81495	Failure Mode Effects and Criticality Analysis Report
DI-SAFT-80101	System Safety Hazard Analysis Report
DI-SAFT-80102	Safety Assessment Report (SAR)
DI-SAFT-80103	Engineering Change Proposal System Safety Report
DI-SAFT-80104	Waiver or Deviation System Safety Report (WDSSR)
DI-SAFT-80105	System Safety Program Progress Report
DI-SAFT-80106	Health Hazard Assessment Report
DI-SAFT-80184	Radiation Hazard Control Procedures
DI-SAFT-80931	Explosive Ordnance Disposal Data
DI-SAFT-81065	Safety Studies Report
DI-SAFT-81066	Safety Studies Plan
DI-SAFT-81299	Explosive Hazard Classification Data
DI-SAFT-81300	Mishap Risk Assessment Report
DI-SAFT-81626	System Safety Program Plan
DI-ENVR-82091	Contractor Hazardous Material Inventory Report
DI-HFAC-81202	Noise Control Program Plan (NCPP)

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

FUTURE ACTION – there are more safety DIDs than listed here; add to the list

FUTURE (SIDE) ACTION: Each DID needs to be revised to "talk" back to the corresponding 882F tasks. Are all task elements to be delivered traceable to the DIDs?

Commented [PDANUAA230]: FUTURE ACTION – there are more safety DIDs than listed here; add to the list

FUTURE (SIDE) ACTION: Each DID needs to be revised to "talk" back to the corresponding 882F tasks. Are all task elements to be delivered traceable to the DIDs?

Commented [PDANUAA231]: 19-1
Added DID references

6.4 Subject term (key word) listing.

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

FUTURE ACTION: Revise "Key Words" list as needed

System safety engineering
Systems Engineering

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

Commented [PDANUAA232]: This holds true for this revision as well.

TASK SECTION 100 - MANAGEMENT

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

Delete Task. Content of this task largely repeats paragraph 4 discussion

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

101.2 Task description. The contractor shall:

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

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

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

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

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

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

Commented [PDANUAA233]: 22-1
Duplication of 4.3.4.4 & 4.3.4.4 verbiage

Commented [PDANUAA234]: 22-2
Duplication of para 4

Commented [PDANUAA235]: 22-5
Duplication with Task 102

Commented [PDANUAA236]: 22-6
Flow down of requirements is part of the SE process. Thus, it is not a system safety unique activity.
Para 3 definition of SE expanded.

Commented [PDANUAA237]: 22-7
Inherently part of the system engineering process.
Duplicates task 104; see 3.1.47

Commented [PDANUAA238]: 22-3
Duplicates 4.3.1.d and Task 106

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

~~101.2.8 As a minimum, report the following:~~

~~a. Hazards and associated risks.~~

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

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

~~d. Recommended mitigation measures.~~

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

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

~~a. Imposition of Task 101. (R)~~

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

~~c. Requirements for incident processing.~~

~~d. Requirements and methodology for reporting on this task.~~

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

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

Commented [PDANUAA239]: 23-1
Redundant with 4.3.3.d

Commented [PDANUAA240]: This is a general overview of topics to report on; loosely duplicates para 4 but without the same level of detail that para 4 requires.

Commented [PDANUAA241]: 23-3
Part of the SE process

Commented [PDANUAA242]: 23-2
Since details are not being included in SOWs or RFPs as required, restructured tasks not to address these details in a manner that does not require inclusion in RFPs or SOW language.

Commented [PDANUAA243]: 22-4
Delete Task since it is repeating para 4 using slightly different words. This creates contractual conflicts.

After removing the duplications, very little is left of the task. Therefore, Task is deleted.

TASK 102
SYSTEM SAFETY PROGRAM PLAN

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

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

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

102.2.1 Scope and objectives. This Section shall account for all contractual hazard management requirements by providing a matrix that correlates these contractual requirements to the location(s) in the SSPP where each requirement is addressed. It shall also account for all software safety assurance activities. The SSPP shall describe, at a minimum:

102.2.1.1 The scope of the effort in terms of the system, subsystem(s), SoS and its life-cycle, to include size of fleet.

102.2.1.2 The operational envelop to include different operating/maintenance modes.

102.2.1.3 The overall approach for accomplishing the General Requirements in Section 4, other contractually required tasks, and derived requirements.

102.21.4 Integration of those efforts into SE and other Program Office management processes in order to support overall program objectives, and

102.2.1.5 Resource requirements (funding, qualified personnel, and tools) to execute the SSPP.

Commented [PDANUAA244]: See ii-2

Commented [PDANUAA245]: 24.8 Delete since not a hard requirement (e.g. "should") and this is not common practice. Most treat SSPP as a stand-alone document with mutual references between the SSPP & SEMP

Commented [PDANUAA246]: 24-1 redundant verbiage (see 4.3.4.3 & 4.3.4.4)

Commented [PDANUAA247]: 24-2
Format change and content reordered to increase readability Subparas renumbered in a consistent manner with the rest of the document

Commented [PDANUAA248]: Added subsystem and SoS to reflect the scope of SSPP Coverage

Commented [PDANUAA249]: Added fleet size

Commented [PDANUAA250]: Added envelop/modes

Commented [PDANUAA251]: Added derived requirements.

102.2.1.6 The approach to how NDI components will be addressed within the system safety program.

102.2.2 SSPP interfaces. The SSPP shall:

102.2.2.1 Identify the functional disciplines covered by the SSPP.

102.2.2.2 Describe the SSPP interfaces between system safety and:

102.2.2.2.1 System Engineering ~~SE~~

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

102.2.2.2.3 Other involved disciplines involved with software development, testing, and certification.

102.2.2.3 Define System of Systems (SoS) that shall be considered in the hazard analyses.

102.2.2.4 Address how system safety shall participate with new/emerging management structures such as model based engineering, middle tiered acquisition, agile software development, etc.

Define subsystems that should be considered in the hazard analyses

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

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

102.2.3.2 The responsibility and authority of the system safety organization.

102.2.3.3 The interrelationships between system safety with other organizations, systems engineering disciplines (to include configuration control and data management, reliability, maintainability, Human Systems Integration (HSI)) and with the other functional elements of the program, including, but not limited to, program management, test and evaluation, logistics, financial, and contracting.

~~(102.2.3) b. The staffing (manpower loading and schedule) of the system safety efforts by each of the involved functional disciplines and organizational units for the duration of the contract. The~~

Commented [PDANUAA252]: New (aligns with other NDI discussions)

Commented [PDANUAA253]: 24-7
Clarification.

Commented [PDANUAA254]: 24-3
New verbiage strengthening interface between system safety and the software community

Commented [PDANUAA255]: 24-4
New verbiage to address SoS in the SSPP

Commented [PDANUAA256]: 24-5
Establishes an expectation to address new and emerging managerial approaches to system development

Commented [PDANUAA257]: 24-7
Should define what subsystems should be considered; e.g. define all what compromises a system

Commented [PDANUAA258]: Was 882E 102..2.3.a

Commented [PDANUAA259]: Moved from 101.2.3

Commented [PDANUAA260]: Moved from 101.2.3 & revised

Commented [PDANUAA261]: 24-6
Format Change to increase readability
Change "Will" to "Shall"

Unaddressed
- SSPP typically written to address "as of today" and often does not project planned organizational changes in the future
- Manpower per task/activity not visible thereby making it harder for government to provide appropriate oversight

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

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

102.2.3.4.1 The SSPP shall identify responsibility and authority of each person and organizational unit involved in executing each of the contractual system safety requirements.

102.2.3.4.2 The SSPP shall also identify key personnel, and provide a summary of the qualifications and credentials of the key system safety personnel.

102.2.3.4.3 The SSPP shall describe how and when the Contractor shall notify the Government prior to changes of key system safety personnel.

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

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

25-2
Clarification needed. Is this ("Total System") the program on contract or is it the system of systems?

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

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

This assumes an IPT structure or Working Groups is being used. With the advent of new management practices, is this construct still valid? If not, delete.

102.2.3.5.4 Describing any specific SoS integration roles and responsibilities.

102.2.3.5.5 Integrating hardware and software provided by the Government.

25-4 Need to expand to address COTS and other NDI being incorporated into the system.

25-7 Need to expand to address integrating Human-System Integration (HIS) into the system.

Commented [PDANUAA262]: 25-1
Was 882E 102.2.3.c
Will ➔ shall

Commented [PDANUAA263]: 25-2
Was 882E 102.2.3.c.1
Question needing to be addressed

Commented [PDANUAA264]: See 25-2
Was 882E 102.2.3.c.2

Commented [PDANUAA265]: 25-3
Was 882E 102.2.3.c.3
Update for other (non-IPT) management structures?

Commented [PDANUAA266]: See 25-2

Commented [PDANUAA267]: 25-4
Was 882E 102.2.3.c.4
GFE? Need to account for other NDI

Commented [PDANUAA268]: 25-7
Was 882E 102.2.3.c.5
Need to account for HSI

102.2.3.5.6 Assigning requirements to action organizations and subcontractors.

102.2.3.5.7 Coordinating associated contractor and subcontractor system safety engineering efforts.

102.2.3.5.8 Facilitating safety reviews.

102.2.3.5.9 Recommending ~~mitigation~~ control measures; assessing feasibility, cost, and effectiveness of the measures; and allocating implementation responsibility to associate contractors and subcontractors.

102.2.3.5.10 Reporting on program safety status and metrics.

102.2.3.5.11 Describing procedures for documenting and addressing safety issues between associate contractors and subcontractors.

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

102.2.3.6. The process through which contractor management decisions shall ~~will~~ be made to include: ~~including~~

102.2.3.6.1 Timely notification of hazards with Catastrophic and Critical severity levels, ~~as well as~~

102.2.3.6.2 High and Serious risks to the Government;

102.2.3.6.3 Determining actions necessary in the event of mishaps, incidents, or malfunctions;

102.2.3.6.4 Determining actions necessary for ~~and~~ requesting waivers for safety requirements, ~~and~~ program deviations, and Engineering change proposals, and modification work orders.

102.2.4 Milestones. The SSPP shall, at a minimum:

Commented [PDANUAA269]: Was 882E 102.2.3.c.6

Commented [PDANUAA270]: 25-5; (add associated contractor)
Was 882E 102.2.3.c.7
See 25-2

Commented [PDANUAA271]: Was 882E 102.2.3.c.8

Commented [PDANUAA272]: See ii-2
Was 882E 102.2.3.c.9

Commented [PDANUAA273]: See 25-2

Commented [PDANUAA274]: Was 882E 102.2.3.c.10

Commented [PDANUAA275]: 25-8
Was 882E 102.2.3.c.11
Need to address documentation of how safety issues are addressed

Commented [PDANUAA276]: See25-2

Commented [PDANUAA277]: 25-10
Format change

Commented [PDANUAA278]: 25-6 change will to shall

Commented [PDANUAA279]: 25-9
Including ECP & mods

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

Commented [PDANUAA280]: was 882E 102.2.4.a

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

Commented [PDANUAA281]: 26-1
was 882E 102.2.4.b
FUTURE ACTION: Rewording required

26-1: FUTURE ACTION: "recommending their inclusion" is not a definitive action; needs rewording

Commented [PDANUAA282]: 26-2
FUTURE ACTION: Need to address linkage to new management constructs & milestones

26-2: FUTURE ACTION: New management construct linkage (Agile SW, MTA, other initiatives to Milestones) not addressed

102,2,4,3 Identify the schedules for subsystem, component, and software activities applicable to the system safety activities but specified in other engineering studies and development efforts.

Commented [PDANUAA283]: Was 882E 102.2.4.c

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

Commented [PDANUAA284]: was 882E 102.2.4.d

26-3 FUTURE ACTION: New para to address milestones associated with Software Safety Assurance LOR activities

Commented [PDANUAA285]: 26-3
FUTURE ACTION: Need to account for para 4.4 activity milestones associate with LOR

26-2: FUTURE ACTION: New management construct (Agile SW, MTA, other intiatives) linkage to Milestones not addressed

Commented [PDANUAA286]: See 26-2
FUTURE ACTION: Need to address linkage to new management constructs & milestones

102.2.5 General safety requirements and criteria. The SSPP shall:

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

Commented [PDANUAA287]: 26-4
Was 882E 102.2.5.a
Clarification

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

Commented [PDANUAA288]: Was 882E 102.2.5.b

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

Commented [PDANUAA289]: Was 882E 102.2.5.c

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

Commented [PDANUAA290]: See ii-2
Was 882E 102.2.5.d

102.2.5.5 LOR activities per para 4.4.X.

Commented [PDANUAA291]: 26-5
Need to account for para 4.4. activities associated with LOR

26-6 FUTURE ACTION: Expand discussion to include documentation of 882E tables IV, V, VI (or updated counterparts) of how software safety assurance is applied

Commented [PDANUAA292]: 26-6
FUTURE ACTION: Need to account for para 4.4 tables

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

102.2.6.1 Describe the processes for hazard identification, risk assessment, risk ~~mitigation~~ control, risk communication, and support to risk acceptance by the contracting agency.

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

~~102.2.6.1.2~~ For risk assessment, the SSPP shall list the severity categories, probability levels, and HRI ~~Risk Assessment Codes (RACs)~~ that shall be followed. ~~The definitions in Tables I and II, and the RACs in Table III shall be used, unless tailored alternative definitions and/or a tailored matrix are formally approved in accordance with Department of Defense (DoD) Component policy.~~

Commented [PDANUAA293]: See ii-2
Was 882E 102.2.6.a

Commented [PDANUAA294]: 26-7
Clarification

Commented [PDANUAA295]: was 882E 102.2.6.a(1)

Commented [PDANUAA296]: 26-8 (was 102.2.6.a(2))
Terminology standardization

Commented [PDANUAA297]: 26-9
Redundant language. Requirement already stated para 4

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

~~102.2.6.a(4) For risk acceptance, the SSPP shall describe the plan to address Government risk acceptance to include the procedures for communicating to the Government that a risk acceptance decision is required and providing the risk assessment documentation. In addition, the plan should include the procedures the Government has provided on how the Government will communicate to the Contractor the results of the proposed risk acceptance decision. In accordance with Department of Defense Instruction (DoDI) 5000.02, the Government may have to accept an event risk at multiple points in the life-cycle.~~

102.2.6.1.4 For risk acceptance, the SSPP shall describe the plan to address Government risk acceptance to include the procedures for communicating to the Government that a risk acceptance decision is required and providing the risk assessment documentation.

102.2.6.1.4.1 In addition, the plan should include the procedures the Government has provided on how the Government will communicate to the Contractor the results of the proposed risk acceptance decision.

102.2.6.1.4.2 In accordance with Department of Defense Instruction (DoDI) 5000.02, the Government may have to accept an event risk at multiple points in the life-cycle.

27-2 FUTURE ACTION: DODI 5000.02 Change

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

27-3 FUTURE ACTION: Extent of safety involvement when these items are modified or used in a new way.

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

27-4 FUTURE ACTION: Discussion needs to be adjusted to account for differences required by each 2xx task.

Commented [PDANUAA298]: See ii-2
Was 882E 102.2.6.a(3)

Commented [PDANUAA299]: 27-1
Deleting redundant verbiage
Reinforcing design order of precedence

Commented [PDANUAA300]: See ii-2

Commented [PDANUAA301]: Was 882E 102.2.6.a(4)
Reformat for clarity

Commented [PDANUAA302]: 27-2
FUTURE ACTION: DODI 5000.02 change

Commented [PDANUAA303]: FUTURE ACTION: Rework references as NDI defined to include COTS, GOTS, GFE, etc

Commented [PDANUAA304]: 27-3
Was 882E 102.2.6.b
FUTURE ACTION: Need to address using in a new way/modifications

Commented [PDANUAA305]: Standardized usage of NDI to include COTS, GOTS, GFE

Commented [PDANUAA306]: 27-4
Was 882E 102.2.6.c
FUTURE ACTION: Revised discussion needed

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

102.2.6.5 Identify the hazard analyses tasks to be performed (e.g., Tasks 202 - Preliminary Hazard Analysis [PHA], Tasks 204 - Subsystem Hazard Analysis [SSHA]), analytical techniques to be used (e.g., Fault Tree Analysis [FTA], Failure Modes and Effects Criticality Analysis [FMECA]), and documentation of the results in the HTS.

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

~~102.2.6.g When conducting SoS hazard analyses, the plan shall describe how analysis of the integrated system design, operations, and the interfaces between the products of each associate contractor, or subcontractor, and the end item will be executed. Data or analyses provided by associate contractors and subcontractors (and suppliers and vendors as applicable) shall be used in the conduct of this effort.~~

102.2.6.7 When conducting or contributing to SoS hazard analyses, the plan shall describe how analysis of the integrated system design, operations, and the interfaces between the products of each associate contractor, ~~or~~ subcontractor, or larger SoS coordinating activities and the end item will be executed.

102.2.6.7.1 Data or analyses provided by associate contractors and subcontractors (and suppliers and vendors as applicable) shall be used in the conduct of this effort.

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

102.2.6.9 Describe a systematic software system safety analyses approach (not to be confused with software safety assurance activities) to:

Commented [PDANUAA307]: 27-5
Was 882E 102.2.6.d

Commented [PDANUAA308]: 27-5
Was 882E 102.2.6.e
Clarification

Commented [PDANUAA309]: Was 882E 102.2.6.f

Commented [PDANUAA310]: Reformat

Commented [PDANUAA311]: 27-6
Distributed SoS analyses would have each program contributing "their portion" of the analyses. Clarification permits this approach to SoS analyses efforts

Commented [PDANUAA312]: Was 882E 102.2.6.h

Commented [PDANUAA313]: 27-7
Was 882E 102.2.6.i
Clarification

102.2.6.9.1 For each software partition, identify and describe the software contributions to system hazards.

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

102.2.6.9.3 Identify the safety requirements associated with safety-significant software components and ~~safety-related~~ items.

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

102.2.6.9.5 Identify and assign the AI Criticality Index (AICI) for each software partition and its associated requirements.

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

~~102.2.7.a Describe the approach for collecting and processing pertinent hazard, anomaly, mishap, and lessons learned data. This should include both historical data from similar or legacy systems used to assist in hazard identification and associated risk assessment, and current system data, e.g., the HTS.~~

102.2.7.1 Describe the approach for collecting and processing pertinent hazard, anomaly, mishap, and lessons learned data.

102.2.7.1.1 This should include both historical data from similar or legacy systems used to assist in hazard identification and associated risk assessment, and current system data, e.g., the HTS.

FUTURE ACTION – clarification. Reference to HTS: Is this the HTS of the contracted system OR is this the HTS of similar or legacy systems?

~~102.2.7.b Identify all documents or other media incorporating hazard management data by title, contract number, date(s) of delivery, and proposed means of delivery (hard copy, electronic, or real-time access) intended to be delivered to the Government under this contract, including documents or other media with other than unlimited rights for the Government. At a minimum, deliverable data shall include HTS data provided during contract execution and at contract closeout.~~

102.2.7.2 Identify all documents or other media incorporating hazard management data by title, contract number, date(s) of delivery, and proposed means of delivery (hard copy, electronic, or real-time access) intended to be delivered to the Government under this contract, including documents or other media with other than unlimited rights for the Government.

102.2.7.1.1 At a minimum, deliverable data shall include HTS data provided during contract execution and at contract closeout.

Commented [PDANUAA314]: 28-1
Was 882E 102.2.6.i.1
Imprecise language ➔ added words for clarification

Commented [PDANUAA315]: Was 882E 102.2.6.i.2

Commented [PDANUAA316]: 28-2
Was 882E 102.2.6.i.3
Improper scope ➔ clarification through deleted words. Safety Related, per para 3, included only marginal & negligible severities. Intent to include Catastrophic and Critical severities.

Commented [PDANUAA317]: 28-3
Was 882E 102.2.6.i.4
Revised per new para 4.4
NOTE: Software deemed not to have a safety impact still gets an SwCI value assigned ➔ SwCI = No Safety (or how it is modified in the revised chart)

Commented [PDANUAA318]: Added for completeness (see para 4.4)
NOTE: Software deemed not to have a safety impact still gets an AICI value assigned = No AI

Commented [PDANUAA319]: FUTURE ACTION: Cleanup needed
102.2.7.1 & 102.2.7.2 are invoked by this "Shall".
102.2.7.1.1 & 102.2.7.2.1 are also invoked by "Shall" but have their own "Shall" statements

Commented [PDANUAA320]: 28-9
During testing & for fielded systems, evaluating (software) anomalies is essential to identify emerging safety issues. Also, this is the data that would populate the hazards as documented through the HTS

Commented [PDANUAA321]: Reformat to improve readability

Commented [PDANUAA322]: 28-10
Unclear intent

Commented [PDANUAA323]: 28-4
FUTURE ACTION: Clarification - Government access to contractor generated uniquely formatted data

FUTURE ACTION: Does 102.2.7.2 & 102.2.7.2.1 need to be reworked as it make intent clearer?

- Properly citing sources that are being incorporated into the system safety effort?
- Or is this properly citing those documents generated under the contract?
- Is the intent to cover the various types of media hazard management data may be delivered under the contract?

Perhaps this discussion needs context to better understand what is this para's purpose.

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

102.2.8.1 Verify, validate, and document effectiveness of ~~mitigation~~ hazard control measures in reducing risk through test, analysis, inspection, etc.

28-6 FUTURE ACTION:

- Is the focus on the control measures working as projected?
- Or, is the focus on justifying the probability reduction of the control measures?
- Or, is the focus on how control measures will be verified, validated, and documented (which appears to duplicate Spec Validation)

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

28-7 FUTURE ACTION:

- Not sure the focus of this statement. **Hazard Management requirements** focuses on how hazards are managed?
  ** Are these agreed to (vs just identified potential) hazard controls?
- Or, should this be focused on how hardware, software, and procedures comply with hazard control measures (or the requirements establishing such measures)?
- Or, is the focus on how hardware, software, and procedure comply with

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

28-12 FUTURE ACTION: Presumably, these are requirements beyond those derived to control specific hazards

Commented [PDANUAA324]: 28-5
Will ➔ shall

Commented [PDANUAA325]: 28-11
Was 882E 102.2.8.a
Terminology realignment
See ii-2

Commented [PDANUAA326]: 28-6
FUTURE ACTION: Unclear intent

Commented [PDANUAA327]: 28-7
Was 882E 102.2.8.b
FUTURE ACTION: Unclear intent

Commented [PDANUAA328]: 28-12
Was 882E 102.2.8.c
FUTURE ACTION: Unclear Intent. Presumably, these are requirements beyond those derived to control specific hazards

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

28-8 FUTURE ACTION:

- These are fundamentally program management/contracting/configuration roles.
- Should this be refocused to System Safety's role in this activity? *For example, part of the government's system safety role is to provide an independent V&V of data submitted. Specifically, Prior to the RAA accepting a risk, the government system safety engineer should be reviewing the content of the system safety hazard package to ensure information being provided to the RAA is technically correct and relevant to the associated hazard.*

102.2.8.4.1 Ensure, for each control measure, the verification and validation of the corresponding risk reduction claimed.

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

Do the requirements outlined in 102.2.9 need to be expanded to include derived requirements from this list?

Commented [PDANUAA329]: 28-8
Was 882E 102.2.8.d
FUTURE ACTION: Proper scope?

Commented [PDANUAA330]: 28-13
Added
Many hazard controls are cited; some with exaggerated risk reduction claims. Added words provide a check to reinforce the integrity of system safety products.

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

29-3 Unclear intent.
- Is this how system safety personnel will be trained to follow the system safety process?
- Is this how the non-systems safety practitioner will be trained what the system safety process is?
- Is this training measures incorporated to control specific hazards?

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

29-1 Does the scope need to be defined to only address system's under the contractor's authority (aka manufacturing, test, selective fielding where the contractor operates/maintains the system(s) in question?

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

~~a. Imposition of Task 102. (R)~~

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

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

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

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

~~f. Qualification requirements for key functional personnel.~~

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

Commented [PDANUAA331]: 29-3
Unclear Intent

Commented [PDANUAA332]: 29-1
Clarification needed of the expected scope of this activity

Commented [PDANUAA333]: 29-2
See 23-2
Since details are not being included in SOWs or RFPs as required, restructured tasks not to include these details

Commented [PDANUAA334]: **FUTURE ACTION:**
Review 882B, 882BN1, 882C, & 882C-Change 1 to see if additional topics need to be added to this task as requirements.

Commented [PDANUAA335]: **FUTURE ACTION:**
Reviewing corresponding SSPP DID to ensure the Task & DID are talking to each other appropriately

TASK 103
HAZARD MANAGEMENT PLAN

30-15: Reviewing Task 103 shows that is mirrors Task 102 with minor edits (e.g. SSPP ➔ HMP). However, the methodology outlined in Task 103 is NOT the methodology the environmental community employs to work environmental issues. Since the purpose of Task 103 is to outline the foundation of how environmental issues will be worked, content of this task was reexamined to determine what revisions were needed. Consultations with environmental SMEs highlighted Task 108 covers what is needed. As a result, Task 103 could be **DELETED.**

Comments/questions have been left in the task though no action required with respect to those comments/questions. If Task 103 is NOT deleted, then such comments/questions would need to be addressed.

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

30-2 Is this a common practice?
Is the HMP treated as a stand-alone document?
Note this is a "soft" requirement (aka "should") ➔ see 24-8

30-3 Essentially the same sentence in 102.1 with SSPP changed to HMP. Is the terminology hazard analyses, risk assessment, and risk management correct terminology in the HAZMAT/Environmental community?

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

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

Commented [PDANUAA336]: 30-14

Commented [PDANUAA337]: 30-15
Deletion of Task 103

Commented [PDANUAA338]: See ii-2

Commented [PDANUAA339]: 30-2
Potentially delete (see 24-8)

Commented [PDANUAA340]: 30-3
Is this the proper Scope?

Commented [PDANUAA341]: 30-1
Deleting Redundant verbiage

Commented [PDANUAA342]: 30-4
Format change and content reordered to increase readability
Subparas renumbered in a consistent manner with the rest of the document

~~103.2.1 Scope and objectives. This Section shall account for all contractual hazard management requirements by providing a matrix that correlates these contractual requirements to the location(s) in the HMP where each requirement is addressed. The HMP shall describe, at a minimum:~~

30-5: Is "**Contractual hazard management requirements**" correct construct for the HMP?

~~103.2.1.1 The scope of the effort in terms of the system and its life cycle.~~

30-6: Does the HMP need to account for Subsystems or System of Systems? Does size of fleet need to be accounted for? (see 102.2.1.1)

~~103.2.1.2 The overall approach for accomplishing the General Requirements in Section 4 and other contractually required tasks, and derived requirements.~~

~~103.2.1.3 Integration of those efforts into SE and other Program Office management processes in order to support overall program objectives~~

~~103.2.1.4 Resource requirements (funding, qualified personnel, and tools) to execute the HMP.~~

Does NDI need to be accounted for in the HMP?

~~103.2.2 HMP interfaces. The HMP shall:~~

~~103.2.2.1 Identify the functional disciplines covered by the HMP.~~

~~103.2.2.2 Describe the HMP interfaces between:~~

~~103.2.2.2.1 System Engineering SE~~

~~103.2.2.2.2 Functional disciplines using the system safety methodology as described in Section 4 of this Standard (e.g., system safety, range safety, fire protection engineering, environmental engineering, explosive and ordnance safety, chemical and biological safety, directed energy, laser and radio frequency safety, software system safety, industrial hygiene, occupational health, and Human Systems Integration (HSI)).~~

30-10 This para is problematic. "System Safety methodology" is being used for a number of different dissimilar activities. By extension, all of these diverse activities are all grouped as system safety. As this is a list of examples, other organizations also may "claim" system safety methodology further expanding the system safety swim lane.

30-11 Para 4 methodology is contractually binding and does not need to be referenced here.

Commented [PDANUAA343]: 30-5 Revised format of 103.2.1 to increase readability.

Commented [PDANUAA344]: 30-6

Commented [PDANUAA345]: 30-7
Added derived requirements

Commented [PDANUAA346]: 30-8

Commented [PDANUAA347]: 30-9
Spelled out for clarity

Commented [PDANUAA348]: 30-10
New para 6.3 addresses Intended use and largely repeats this para.

Commented [PDANUAA349]: 30-11
Para 4 methodology is contractually binding and does not need to be referenced here.

30-12 Does the HMP need to account for new/emerging management structures such as model based engineering, middle tiered acquisition, etc?

Commented [PDANUAA350]: 30-12

~~103.2.2.2.3 Other involved disciplines (e.g., logistics, maintainability, quality control, reliability, software development, system integration, and test, etc.).~~

Quality control vs quality assurance (see 102.2.2.2.2)??? SSPP cites Quality assurance whereas HMP is citing quality control. Otherwise these paras are the same.

HMP involvement in software development?

Commented [PDANUAA351]: 30-13

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

~~103.2.3.1 The organization or function of the HMP efforts within the SE process. Use charts to show the organizational and functional relationships and lines of communication.~~

~~(103.2.3) b. The staffing (manpower loading and schedule) of the HMP efforts by each of the involved functional disciplines and organizational units for the duration of the contract. The HMP will identify responsibility and authority of each person and organizational unit involved in executing each of the contractual HMP requirements. The HMP will also identify key personnel, and provide a summary of their qualifications and credentials. The HMP will describe how and when the Contractor shall notify the Government prior to changes to key personnel implementing the HMP .~~

~~103.2.3.2 The staffing (manpower loading and schedule) of the HMP efforts by each of the involved functional disciplines and organizational units for the duration of the contract.~~

~~103.2.3.2.1 The HMP shall identify responsibility and authority of each person and organizational unit involved in executing each of the contractual HMP requirements.~~

~~103.2.3.2.2 The HMP shall also identify key personnel, and provide a summary of their qualifications and credentials.~~

~~103.2.3.2.3 The HMP shall describe how and when the Contractor shall notify the Government prior to changes to key personnel implementing the HMP .~~

31-1 Is the HMP typically written to address "as of today" and therefore does not project planned organizational changes in the future?

31-1.1 Is the manpower per task/activity visible for government to provide appropriate oversight. Or is greater visibility needed?

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

31-3 Is the HMP effort limited to the system under contract? If so, then the scope is incorrect here as system of systems would be applying to one of many systems under contract.

~~103.2.3.3.1 Defining the roles of each associate contractor and subcontractor (and suppliers and vendors as applicable) to integrate HMP requirements for the total system.~~

31-4
(1) Associated contractors discussion does not address contractors who share in a SOS? As worded, this task assumes the program is in charge of the SOS system. The program may not be, or there may be a decentralized management approach for the SOS
(2) Is this the program or the larger system of systems?

Commented [PDANUAA352]: 31-1
Format change to increase readability
Change will to shall

Unaddressed
- Is the HMP typically written to address "as of today" and therefore does not project planned organizational changes in the future?
- Is the manpower per task/activity visible for government to provide appropriate oversight. Or is greater visibility needed?

Commented [PDANUAA353]: See 31-1
will ➔ shall

Commented [PDANUAA354]: See 31-1
Will ➔ shall

Commented [PDANUAA355]: See 31-1
Will ➔ shall

Commented [PDANUAA356]: 31-2
Will ➔ Shall

Commented [PDANUAA357]: 31-3

Commented [PDANUAA358]: 31-4

~~103.2.3.3.2 Defining the HMP interfaces between each associate contractor and subcontractor (and suppliers and vendors as applicable), e.g. integrating hazard analyses.~~

~~103.2.3.3.3 Establishing Integrated Product Teams (IPTs) or Working Groups (WGs) with representatives from each associate contractor and subcontractor (and suppliers and vendors as applicable).~~

31-5 This assumes an IPT structure is being used. With the advent of new management practices, is this construct still valid? If not, delete.

31-6: **associated contractor** should be added to para 3

~~103.2.3.3.4 Describing any specific SoS integration roles and responsibilities.~~

~~103.2.3.3.5 Integrating hardware and software provided by the Government.~~

31-7 How does the HMP address COTS and other NDI being incorporated into the system.? What about GFE?

~~103.2.3.3.6 Assigning requirements to action organizations and subcontractors.~~

~~103.2.3.3.7 Coordinating associated contractor and subcontractor HMP engineering efforts.~~

~~103.2.3.3.8 Recommending mitigation~~ control ~~measures; assessing feasibility, cost, and effectiveness of the measures; and allocating implementation responsibility to associate contractors and subcontractors.~~

31-8: Terminology cleanup needed. Hazards are Controlled via Mitigation (e.g. reducing the probability) or via amelioration (e.g. reducing the severity). For environmental issues, is this the correct term? Or, is something like remediation a better term to use?

~~103.2.3.3.9 Reporting on hazard management status and metrics.~~

31-9: System Safety issues are generally worked as **Hazards**. Para 4 defines what hazards are, how hazards are characterized, how risk is assigned, management of hazards, etc. Does the environmental/HAZMAT community use the term Hazard (or is there another term used) to denote HMP issues that need to be worked? If so, then a terminology change is appropriate

~~103.2.3.3.10 Describing procedures for~~ documenting and ~~addressing hazard management issues between associate contractors and subcontractors.~~

31-10 (see 25-8) Assumption is there a need to address documentation of how HMP issues are addressed

Commented [PDANUAA359]: See 31-4

Commented [PDANUAA360]: 31-5

Commented [PDANUAA361]: 31-6

Commented [PDANUAA362]: 31-7
GFE? Need to account for other NDI

Commented [PDANUAA363]: 31-4 (add associated contractor)
See 31-4

Commented [PDANUAA364]: 31-8
Terminology cleanup
See ii-2

Commented [PDANUAA365]: See 31-4

Commented [PDANUAA366]: 31-9

Commented [PDANUAA367]: 31-10

~~(103.2.3) d. The process through which contractor management decisions will be made including timely notification of High and Serious risks to the Government; determining actions necessary in the event of mishaps, incidents, or malfunctions; and requesting waivers for hazard management requirements and program deviations.~~

~~103.2.3.4 The process through which contractor management decisions shall be made to include:~~

~~103.2.3.4.1 timely notification of High and Serious risks to the Government;~~

31-13 How contractually binding is "Timely Notification"? How is Timely Notification defined?

31-14 High and Serious risks used in this para; in corresponding 102.2.3.6.1 (SSPP) uses the terms Catastrophic and Critical. This raises questions of why High/Serious terms used? Note – have not seen any High/Serious (HMP driven) system safety risks

~~103.2.3.4.2 determining actions necessary in the event of mishaps, incidents, or malfunctions;~~

~~103.2.3.4.3 determining actions necessary for requesting waivers for hazard management requirements and program deviations.~~

Commented [PDANUAA368]: 31-11
Reformat

Commented [PDANUAA369]: 31-12
Will➔shall

Commented [PDANUAA370]: 31-13

Commented [PDANUAA371]: 31-14

~~103.2.4 Milestones. The HMP shall, at a minimum:~~

~~103.2.4.1 Provide a schedule of hazard management activities including required inputs and outputs, and start and completion dates that support the SE process.~~

~~103.2.4.2 Relate the hazard management activities to integrated system-level activities (e.g., design analyses, tests, and demonstrations), technical reviews, program reviews, and major program milestones by recommending their inclusion in the Integrated Master Schedule (IMS).~~

32-1: "**recommending their inclusion**" is not a definitive action; needs rewording

32-2: change from **"… milestones by recommending their …"** ➔ **"… milestones by documenting their …."**

32-3: New management construct linkage(Agile SW, MTA, other initiatives to Milestones not addressed

~~103.2.4.3 Identify the schedules for subsystem, component, and software activities applicable to the hazard management activities but specified in other engineering studies and development efforts.~~

~~103.2.4.4 Include a schedule of technical meetings between associate contractors and subcontractors to discuss, review, and integrate the safety effort.~~

32-3: New management construct (Agile SW, MTA, other intiatives) linkage to Milestones not addressed

~~103.2.5 General HMP requirements and criteria. The HMP shall:~~

~~103.2.5.1 List the standards and system specifications containing hazard management requirements that the contractor shall use in the execution of the contract. Cite Include titles, dates, and where applicable, paragraph numbers.~~

~~103.2.5.2 Describe general engineering requirements and design criteria for hazard management during system design and development.~~

~~103.2.5.3 Identify hazard management requirements, to include procedures, for test, operations and support, and disposal.~~

~~103.2.5.4 Describe the method for ensuring flow-down of hazard identification and mitigation~~ control ~~functions as well as associated requirements to subcontractors/suppliers.~~

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

Commented [PDANUAA372]: (was 103.2.4.a)

Commented [PDANUAA373]: 32-1
32-2

Commented [PDANUAA374]: 33-3

Commented [PDANUAA375]: See 31-9

Commented [PDANUAA376]: 32-4
Clarification

Commented [PDANUAA377]: See 31-9

Commented [PDANUAA378]: See 31-9

Commented [PDANUAA379]: See ii-2

Commented [PDANUAA380]: See 31-9

Commented [PDANUAA381]: 32-6

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

~~103.2.6.1.1 For hazard identification, the HMP shall describe the systematic identification process that evaluates the system throughout its life cycle. This evaluation should include as a minimum system hardware and software, system interfaces (to include human interfaces), the intended use or application and operational environment, and disposal.~~

~~103.2.6.1.2 For risk assessment, the HMP shall list the severity categories, probability levels, and Hazard Risk Index (HRI) Risk Assessment Codes (RACs) that shall be followed. The definitions in Tables I and II, and the HRIs RACs in Table III shall be used, unless tailored alternative definitions and/or a tailored~~

Commented [PDANUAA382]: See ii-2

Commented [PDANUAA383]: 32-7

Commented [PDANUAA384]: 32-8

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

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

33-2 Are the trade-off discussions documented and included?

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

33-4: DODI 5000.02 change

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

33-5 Extent of safety involvement when these items are modified or used in a new way.

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

33-6 Discussion needs to be adjusted to account for differences required by each 2xx task.

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

33-6: Append to read: "… for a given hazard and include justification."

103.2.6.5 Identify the hazard analyses tasks to be performed (e.g., Tasks 202 – Preliminary Hazard Analysis [PHA], Tasks 204 – Subsystem Hazard Analysis [SSHA]), analytical techniques to be used (e.g., Fault Tree Analysis [FTA], Failure Modes and Effects Criticality Analysis [FMECA]), and documentation of the results in the HTS.

Commented [PDANUAA385]: See 32-8

Commented [PDANUAA386]: See ii-2

Commented [PDANUAA387]: 33-1

Commented [PDANUAA388]: See ii-2

Commented [PDANUAA389]: 33-2

Commented [PDANUAA390]: 33-3

Commented [PDANUAA391]: 33-4
Pending DODI 5000.02 change

Commented [PDANUAA392]: 33-5

Commented [PDANUAA393]: 33-6

Commented [PDANUAA394]: 33-7

Commented [PDANUAA395]: 33-8

~~103.2.6.6 Identify the scope of each analysis, integration of associate contractor and subcontractor hazard analyses with overall system hazard analyses, and the depth within the system that each analytical technique will be used (e.g., system level, subsystem level, component level).~~

~~103.2.6.7 When conducting or contributing to SoS hazard analyses, the plan shall describe how analysis of the integrated system design, operations, and the interfaces between the products of each associate contractor or subcontractor, or larger SoS coordinating activities and the end item will be executed. Data or analyses provided by associate contractors and subcontractors (and suppliers and vendors as applicable) shall be used in the conduct of this effort.~~

Commented [PDANUAA396]: Action: Check 2xx tasks to see if scope defined

Commented [PDANUAA397]: 33-9
Distributed SoS analyses would have each program contributing "their portion" of the analyses. Clarification permits this approach to SoS analyses efforts

~~103.2.6.7 Describe the efforts to identify and control hazards associated with materials used during the system's life-cycle.~~

34-1 This is vague and leaves too much to interpretation

34-2 Is this the proper scope

103.2.6.8 Describe a systematic software system safety approach to:

34-3 How much does the HMP get involved with software safety? This is logic, not material

~~103.2.6.8.1 Identify and describe the software contributions to system hazards.~~

~~103.2.6.8.2 Identify safety-significant (safety-critical and safety-related) software functions and software requirements.~~

~~103.2.6.8.3 Identify the safety requirements associated with safety-significant software components and safety-related items.~~

~~103.2.6.8.4 Identify and assign the Software Criticality Index (SwCI) for each safety-significant software function (SSSF) and its associated requirements.~~

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

~~103.2.7.1 Describe the approach for collecting and processing pertinent hazard, mishap, and lessons learned data. This should include both historical data from similar or legacy systems used to assist in hazard identification and associated risk assessment, and current system data, e.g., the HTS.~~

34-4: Lack of definition of what the HMP covers results in lack of understand of what issues the HMP would engage in. Thus, it is not feasible at this time to determine if such issues follow para 4 hazard characterization and subsequent inclusion into the HRS.

34-5 Unclear intent. Is this the HTS of the contracted system OR is this the HTS of similar or legacy systems?

Commented [PDANUAA398]: 34-1
This is vague and leaves too much to interpretation.
34-2
Proper scope?

Commented [PDANUAA399]: 34-3

Commented [PDANUAA400]: 34-4

Commented [PDANUAA401]: 34-5

~~103.2.7.2 Identify all documents or other media incorporating hazard management data by title, contract number, date(s) of delivery, and proposed means of delivery (hard copy, electronic, or real-time access) intended to be delivered to the Government under this contract, including documents or other media with other than unlimited rights for the Government. At a minimum, deliverable data shall include HTS data provided during contract execution and at contract closeout.~~

Commented [PDANUAA402]: 34-6
Duplication of CDRL?

34-6: Duplication of CDRL? Government access to contractor generated uniquely formatted data?
34-8: Does this need to be reworked as it make intent clearer?

- Properly citing sources that are being incorporated into the system safety effort?
- Or is this properly citing those documents generated under the contract?
- Is the intent to cover the various types of media hazard management data may be delivered under the contract?

Perhaps this discussion needs context to better understand what is this para's purpose

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

Commented [PDANUAA403]: 34-7
Will ➔ shall

~~103.2.8.1 Verify, validate, and document effectiveness of mitigation hazard control measures in reducing risk through test, analysis, inspection, etc.~~

Commented [PDANUAA404]: 28-11
Terminology realignment
See ii-2

~~103.2.8.2 Verify, validate, and document that hardware, software, and procedures comply with identified hazard management requirements.~~

Commented [PDANUAA405]: 34-9

- Not sure the focus of this statement. **Hazard Management requirements** focuses on how hazards are managed?
  ** Are these agreed to (vs just identified potential) hazard controls?
- Or, should this be focused on how hardware, software, and procedures comply with hazard control measures (or the requirements establishing such measures)?

Or, is the focus on how hardware, software, and procedure comply with

~~103.2.8.3 Identify requirements for certifications, independent review board evaluations, and special testing (e.g., insensitive munitions tests, Hazards of Electromagnetic Radiation to Ordnance (HERO), Electrostatic Discharge (ESD), and render-safe /emergency disposal procedures).~~

Commented [PDANUAA406]: 34-10
Unclear intent; presumably, these are requirements beyond those derived to control specific hazards.

34-11: Is there a reason para 103.2.8.3 has expanded examples from 102.2.8.3? Besides reference to HERO and ESD, the rest of the text is identical

Commented [PDANUAA407]: 34-11

~~103.2.8.4 Ensure procedures are in place to transmit verification and validation information to the Government.~~

Commented [PDANUAA408]: 34-12
Proper Scope?

34-12

- These are fundamentally program management/contracting/configuration roles.
- Should this be refocused to System Safety's role in this activity? *For example, part of the government's system safety role is to provide an independent V&V of data submitted. Specifically, Prior to the RAA accepting a risk, the government system safety engineer should be reviewing the content of the system safety hazard package to ensure information being provided to the RAA is technically correct and relevant to the associated hazard.*

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

Such system safety requirements need to include other contractually mandated requirements as well as any derived system safety requirement.

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

- Is this how system safety personnel will be trained?
- Is this how the non-systems safety practitioner will be trained?
- Is this training measures incorporated to control specific hazards?

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

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

a. Imposition of Task 103. (R)

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

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

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

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

f. Qualification requirements for key functional personnel.

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

Commented [PDANUAA409]: 35-1
Improper Scope

Commented [PDANUAA410]: 35-2
Unclear Intent

Commented [PDANUAA411]: 35-3
Clarification needed of the expected scope of this activity

Commented [PDANUAA412]: 35-4
See 23-2
Since details are not being included in SOWs or RFPs as required, restructured tasks not to include these details

TASK 104
SUPPORT OF GOVERNMENT REVIEWS/AUDITS

36-4 System Safety is a part of Systems Engineering Process.
Systems Engineering (SE) has established guidance to address government reviews/audits. Therefore, applying SE guidance to System Safety means this task is redundant to established SE guidance. What value to being added through this task?
It is not within the Scope of MIL-STD-882 to repeat guidance established in other formal documentation. (Besides, there are many aspects of SE that MIL-STD-882 does not address; should those aspects be replicated in MIL-STD-882 as additional tasks?)

Thus, **Delete Task**.

NOTE: Para 3.2.47, Definition for Systems Engineering has been expanded amplifying above logic.

Comments/questions have been left in the task though no action required with respect to those comments/questions. If Task 104 is NOT deleted, then such comments/questions would need to be addressed.

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

~~104.2 Task description. The contractor shall:~~

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

~~104.2.1 Support Government reviews, audits, and boards such as, but not limited to:~~
~~a. program and technical reviews,~~
~~b. munitions safety boards,~~
~~c. laser safety boards,~~
~~d. directed energy safety boards,~~
~~e. nuclear safety boards,~~
~~f. mission readiness reviews,~~
~~g. flight readiness reviews,~~
~~h. test readiness reviews,~~
~~i. launch readiness reviews,~~
~~j. flight safety review boards,~~
~~k. National Environmental Policy Act (NEPA) document public hearings.~~

Commented [PDANUAA413]: FUTURE ACTION: How does Middle Tiered Acquisitions (MTA) and other new management approaches/structures affect this task?

Commented [PDANUAA414]: 36-5
Format/increased readability

Commented [PDANUAA415]: 36-1
Accounting for new board

~~104.2.2 Provide technical support to mishap investigations.~~

~~Move to para 4.X?~~
~~Alternatively, change task title to "Support of Government Reviews/Audits/Investigations".~~

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

~~a. Imposition of Task 104. (R)~~

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

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

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

Commented [PDANUAA416]: 36-2
Misleading task action.
This was added to MIL-STD-882E.
Note supporting mishap investigations was not in MIL-STD-882C(C1), 882C, 882B(N1), 882B versions of Task 104.

Commented [PDANUAA417]: 36-3
See 23-2
Since details are not being included in SOWs or RFPs as required, restructured tasks not to include these details

TASK 105
INTEGRATED PRODUCT TEAM/WORKING GROUP SUPPORT

37-1 System Safety is a part of Systems Engineering Process.
Systems Engineering (SE) has established guidance to address Integrated Product Team/Working Group Support.
Therefore, applying SE guidance to System Safety means this task is redundant to established SE guidance. What value to being added through this task?
It is not within the Scope of MIL-STD-882 to repeat guidance established in other formal documentation. (Besides, there are many aspects of SE that MIL-STD-882 does not address; should those aspects be replicated in MIL-STD-882 as additional tasks?)
Furthermore, new management structures are being introduced via MTA and other sources. This task (or parallel tasks) would need to be adjusted to account for these new management structures.

Thus, **Delete Task**.

NOTE: Para 3.2.47, Definition for Systems Engineering has been expanded amplifying above logic.

Comments/questions have been left in the task though no action required with respect to those comments/questions. If Task 105 is NOT deleted, then such comments/questions would need to be addressed.

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

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

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

~~b. Identifying issues or problems associated with risk mitigations controls.~~

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

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

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

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

Commented [PDANUAA418]: 37-1

Commented [PDANUAA419]: 37-2
Other management & meeting structures exist that are not accounted for in this task

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

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

Commented [PDANUAA420]: 37-3
See discussion in box

The nature of contractor participation in IPTs/WGs is incorrect. The core part of system safety is analyzing/evaluating systems for hazards. However, the stated participation expectations do not address this aspect. The role reserved for the contractor is addressing the indirect activities that results in the scope being too narrowly defined. Subparas a-h are very prescriptive – to the point that some interpret these are the only areas the contractor is expected to support. How to expand scope and what other activities need to be added?:

a. Summarizing hazard analyses … ➔ not accomplishing hazard analyses?
b. Identifying issues or problems … ➔ granted needs to occur, but what about developing risk control measures?
c. Working toward agreement on effectiveness … ➔ subjective and does not provide a concrete resolution
d. Presenting incident .. assessment results … ➔
   (1) What about software anomalies?
   (2) Needed, but this is AFTER system design is finalized. What about involvement in earlier life-cycle activities?
e. Responding to action items … ➔ what about the collaborative activities of the IPT/WG? Not everything needs to be an action item.
f. Reviewing & validating risk reduction requirements … ➔ granted needed, but what about deriving risk reduction requirements?
g. Planning and coordinating support for required reviews and certification processes ➔ what about providing support from these activities?

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

~~a. Imposition of Task 105. (R)~~

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

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

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

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

Commented [PDANUAA421]: 37-4
See 23-2
Since details are not being included in SOWs or RFPs as required, restructured tasks not to include these details

TASK 106
HAZARD TRACKING SYSTEM

38-1
Para 4.3.1 addresses Hazard Tracking System (HTS). In addition, Task 101 (proposed to be deleted) also covers HTS. This task duplicates 4.3.1.4 with slightly different words which introduces potential conflicts – which source takes precedent? Since 4.3.1.4 is automatically "on contract", there is no additional value being added with this task.

Delete task & revise 4.3.1.4 to include a master listing of the minimum required fields in the FTS. In 2XX tasks, task unique HTS fields will be added to the 4.3.1.4. (See Figure 2, pg 10a)

Comments/questions have been left in the task though no action required with respect to those comments/questions. If Task 106 is NOT deleted, then such comments/questions would need to be addressed.

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

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

~~a. Hazard.~~

~~b. System.~~

~~c. Subsystem (if applicable).~~

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

~~e. Requirements references.~~

~~f. System mode.~~

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

~~h. Effects.~~

~~i. Mishap.~~

~~j. Initial HRI risk assessment code.~~

~~k. Target HRI risk assessment code.~~

~~l. Event HRI risk assessment code(s).~~

Commented [PDANUAA422]: 38-1

Commented [PDANUAA423]: FUTURE ACTION – reconcile with HTS DID

Commented [PDANUAA424]: 38-2
Nomenclature change

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

n. Hazard status to include risk acceptance authority decisions.

~~o. Verification and validation method.~~

~~p. Action person(s) and organizational element.~~

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

Commented [PDANUAA425]: See ii-2

Commented [PDANUAA426]: 38-3 completeness

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

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

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

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

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

a. Imposition of Task 106. (R)

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

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

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

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

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

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

h. Additional HAZMAT data elements and report requirements.

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

Commented [PDANUAA427]: 39-1
No action in this para. Do these tasks contain additional requirements or don't they? As written, the do not. Revised 2XX task structure adds task unique HTS fields.

Commented [PDANUAA428]: 39-2
See 23-2
Since details are not being included in SOWs or RFPs as required, restructured tasks not to include these details

TASK 107
HAZARD MANAGEMENT PROGRESS REPORT

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

40-1: Rewording needed.
"**The reporting period**" has not been defined, therefore, where would this reporting period be defined?
This task should be restructured to develop periodic reports and rely upon the CDRL/DID to define the periodic reporting period

107.2 Task description. The contractor shall prepare periodic progress reports summarizing general progress made on hazard management efforts during the specified reporting period and forecasting projected work for the next reporting period.

107.2.1 The report ~~will~~ shall contain, at a minimum, the following information:

~~(107.2)a A brief summary of the activities, progress, and status of the hazard management efforts relative to the scheduled program milestones. The summary shall highlight significant achievements and issues.~~

107.2.1.1 A brief summary of the activities, progress, and status of the hazard management efforts relative to the scheduled program milestones.

107.2.1.1.1 The summary shall highlight significant achievements and issues.

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

107.2.1.3 Identification of significant changes in controlling the risk of known hazards.

107.2.1.4 Implementation status of recommended ~~mitigation~~ control measures.

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

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

107.2.1.7 Status of High/Serious hazards.

Commented [PDANUAA429]: 40-1
See boxed text

Commented [PDANUAA430]: Will ➔ Shall

Commented [PDANUAA431]: Format change to increase readability. Subparas renumbered

Commented [PDANUAA432]: 40-2
Was 882E 107.2.b
format change to increase readability. One thought per line (hence 2 lines).

Commented [PDANUAA433]: See ii-2
Was 882E 107.2.c

Commented [PDANUAA434]: Was 882E 107.2.d

Commented [PDANUAA435]: Was 882E 107.2.e

Commented [PDANUAA436]: 40-3
Added scope of what is needed to be reported

40.5 Any other information needed in this periodic report? HRIs associated with hazards? Other HTS fields?

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

~~a. Imposition of Task 107. (R)~~

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

~~c. Progress reporting period. (R)~~

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

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

Commented [PDANUAA437]: 40-5
See boxed text

Commented [PDANUAA438]: 40-4
See 23-2
Since these details are not being included in SOWs or RFPs as required, restructured tasks not to require these details

TASK 108
HAZARDOUS MATERIALS MANAGEMENT PLAN

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

41-2: This task is assuming an HMMP already exists. Who writes the HMMP? Who evaluates the HMMP to determine if it is acceptable?

41-3: This statement appears to be a creative way to avoid requiring a CDRL item yet still gain access of it. If this task is invoked in a SOW, does the underlined statement create any issues? One must assume there would **NOT** be a CDRL item associated with the HMMP.

??? asserts integral part of the System Engineering process is already stated in para 3.1.47 & 4.2.1. So what value is added by asserting again here?
??? using this Standard's methodology? 882 methodology is automatically invoked so it does not need to be restated in the Task.

108.1 Purpose: Task 102 is to develop a Hazardous Material Management Plan (HMMP) that is an integral part of the hazardous material management effort within the program's SE process. The HMMP shall detail the tasks and activities that are required to implement a systematic approach to manage hazardous materials used on the program.

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

108.2 Task description. The contractor shall use the HMMP to define contractor roles, responsibilities, and procedures needed to accomplish HAZMAT management and tracking.

108.2.1 The plan shall account for contractually required HAZMAT management tasks and responsibilities.

41-1: Why doesn't Task 108 have a Scope and Objectives Section like Task 102 and 103? (see below; added new para 108.2.2)

108.2.2 Scope and objectives At a minimum, the HMMP shall identify the following:

Commented [PDANUAA439]: 41-2

Commented [PDANUAA440]: 41-3

Commented [PDANUAA441]: See Text box

Commented [PDANUAA442]: Purpose reworded to more closely parallel Task 102 purpose. As such, the focus of the task is to develop the HMMP.
The rewording resolves confusion between Task 108 and potential CDRL(s) that would accompany it – thereby avoiding potential contractual language issues.

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

41-4 Definition of HAZMAT risk? Is this based on para 4 methodology? This does not appear to align with hazards per para 4 methodology.
If not, is "risk" the correct term? How would HAZMAT "risks" be characterized? Would this characterization involving something other than Tables 1, II, and III?

108.2.2.2 Procedures for tracking and reporting HAZMAT.

41-5 Note that this is tracking the materials and is not the HTS. As such, this is something outside of para 4 methodology.

- What governing guidance describes how these materials will be tracked?
- Do additional HAZMAT tracking/reporting requirements need to be added as subparagraphs to 108.2.2.2?

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

41-6 This is a definition of HAZMAT;
What task/action actually IDENTIFIES that HAZMAT in question? (Header suggests that what this para should be addressing. By extension, this suggests a different methodology that what is laid out in para 4, & as such, deserves additional guidance outlining the methodology of how HAZMAT should be addressed.) Possible requirement may be:

108.2.3.1 The contractor shall identify HAZMATs associated with the program.

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

108.2.4 HAZMAT NAS-411 Categorization.

41-7 What is NAS-411 and why should it be added?

108.2.4.1 Following contract award, the contractor and MA shall mutually develop a list of HAZMAT materials expected to be used in the system, subsystems, and support equipment or planned for system operation or support.

Commented [PDANUAA443]: Was 108.2.a

Commented [PDANUAA444]: 41-4

Commented [PDANUAA445]: Was 108.2.b
41-5

Commented [PDANUAA446]: was 108.2.1
41-6

Commented [PDANUAA447]: Was 108.2.2
NAS-411 was requested to be added to the header.
41-7

Commented [PDANUAA448]: 41-8
Restructured to clarify intent.
- Develop List
- Categorize List
- Definitions for List
- Obtain authorization to use HAZMAT on the list

Requirement split into 2 statements (108.2.2.1 & 108.2.2.2) for clarity. Each is categorizing in a different manner.

108.2.4.2 Each HAZMAT on the list shall be categorized as prohibited, restricted, or tracked.

41-9 *categorizing HAZMAT material as prohibited, restricted, or tracked*. This is not addressed in para 4 methodology or elsewhere in this draft. This structure and associated terms must be defined to ensure proper intent is met. Presumably, these terms and usage is defined in environmental engineering. Do they need to be defined as subparagraphs to 108.2.3.2?

~~(108.2.2)a. Prohibited HAZMAT require the contractor to obtain Government approval before those materials can be included in the system, subsystems, and support equipment or planned for system operation or support.~~

108.2.4.2.1 **Prohibited HAZMAT:** Those materials that are not to be used.

108.2.4.2.1.1 However, if the contractor needs to use such materials within the delivered hardware and/or required for system operation and support, then the contractor shall obtain MA written approval prior to use of the HAZMAT to be used.

41-10 Alternant revision of this para (108.2.4.2.1.1) include:
The contractor shall, in writing, obtain Government approval prior to using prohibited HAZMAT materials in the system, subsystems, and support equipment or planned for system operation or support.

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

108.2.4.2.2 **Restricted HAZMAT**: Those materials that the contractor shall eliminate or minimize with Government involvement

41-11 **Government Involvement** needs clarification. Or does this need to reworded to *108.2.4.2.1 Those materials that the contractor shall eliminate. This also include those HAZMAT that cannot be eliminated but whose usage shall be minimized with Government involvement/concurrence.*

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

108.2.4.2.3 **Tracked HAZMAT:** Those materials that do not require specific contractor action other than tracking and reporting.

41-12 Alternate verbiage:
Tracked HAZMAT shall be documented for tracking and reporting by the contractor.

Commented [PDANUAA449]: 41-9

Commented [PDANUAA450]: Was 882E 108.2.2.a
Format aligned to provide a definition. Case base requirement to account for exceptions to the rule as stated in the definition.

41-10 alternate verbiage for 108.2.2.2.1.

Commented [PDANUAA451]: Was 882E 108.2.2.b
41-11
Format; Verbiage changed

Commented [PDANUAA452]: Was 882E 108.2.2.c
41-12
Format; Verbiage changed

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

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

41-13
Potential contractual issue for the case where mutual agreement is not reached.
Is there other Federal Law/policy that is applicable even if mutual agreement is not reached?

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

~~108.2.6 HAZMAT data tracking. The contractor will be required to track and report all prohibited, restricted, and tracked HAZMAT included in the delivered system, subsystems, and~~

41-16
HAZMAT tracking is NOT account ted for in para 4.
Task 103 (being deleted) incorrectly references the HTS & does not link to reporting HAZMAT.
Task 210 is being split into 3 tasks; one of which deals with HAZMAT. Therefore, there should be a para 4 discussion (the HTS discussion does not suffice) to lay out the expectations of the HAZMAT tracking. Is the expectation/intent to have a closed loop HAZMAT tracking system?
See 108.2.3

108.2.6 HAZMAT data tracking. The contractor shall track and report all prohibited, restricted, and tracked HAZMAT included in the delivered system, subsystems, and support equipment or planned for system operation or support.

108.2.6.1 The minimum data elements required for HAZMAT tracking and reporting shall ~~i~~nclude:

Commented [PDANUAA453]: Was 882E 108.2.2.d
41-13
Will ➔ shall

Commented [PDANUAA454]: Was 108.2.3
41-14
Will ➔ shall

Commented [PDANUAA455]: Was 108.2.4 (carry over onto pg 42)
41-15
Will ➔ shall
Reformatted

Commented [PDANUAA456]: 41-16

Commented [PDANUAA457]: 41-16

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

108.2.6.1.1 HAZMAT item or substance name.

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

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

108.2.6.1.4 Location of HAZMAT with NSN (if known) within the system.

42-1 What about HAZMAT usage in off-system processing (e.g. heavy maintenance)? Not part of the system but is needed to maintain/sustain a system?

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

42-3 Does order of magnitude/unit need to be specified? e.g. nearest ton, pound, ounce, gram, gallon, liter, cup, pint, quart, etc

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

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

108.2.6.1.8 ~~Reasonably anticipated~~ Anticipated HAZMAT (whether categorized or not) generated during mishap occurence.

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

Commented [PDANUAA458]: 41-15
Reformatted (see 41c for 1st half of para)
Will ➔ Shall

Commented [PDANUAA459]: Was 882E 108.2.4.a

Commented [PDANUAA460]: Was 882E 108.2.4.b

Commented [PDANUAA461]: Was 882E 108.2.4.c
42-1

Commented [PDANUAA462]: Was 882E 108.2.4.d
42-2

Commented [PDANUAA463]: Was 882E 108.2.4.e
42-3

Commented [PDANUAA464]: Was 882E 108.2.4.f

Commented [PDANUAA465]: Was 882E 108.2.4.g
42-4

Commented [PDANUAA466]: Was 882E 108.2.4.h
42-5

Commented [PDANUAA467]: Was 882E 108.2.4.i
42-6
MSDS ➔ SDS for correctness

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

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

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

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

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

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

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

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

Commented [PDANUAA468]: 42-7
This section is being deleted.
See 23-2
Since details are not being included in SOWs or RFPs as required, restructured tasks not to address these details in a manner that does not require inclusion in RFPs or SOW language.

TASK SECTION 200 – ANALYSIS

TASK 201
PRELIMINARY HAZARD LIST

44-18 Title Change Needed? (Due to merging Tasks 201 & 304)

201.1 Purpose. Task 201 is to compile a list of potential hazards early in development or during later life cycle phases where changes/modifications are being contemplated. Such changes may be derived from, but not limited to, Engineering Change Proposals, Change Notices, Deficiency Reports, Trade Studies, Mishaps, Requests for Deviations/Waiver, and related change documentation.

201.2 Task description. The contractor shall assess the proposed change for system safety impacts either at the start of program (e.g material solution), during trade studies, or as a result of a temporary or permanent proposed change to the program (e.g. Engineering Change proposals (ECPs), change notices, deficiency reports, requests for deviations, waivers, etc).

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

201.2.1 System safety impacts shall include identification of new potential hazards as well as impacts to prior identified hazards.

Commented [PDANUAA469]: 44-18

Commented [PDANUAA470]: 44-1
By itself, Task 201 is limited to material solution; or very early in the life cycle..
Likewise, Task 304 is noble in its intent but scope is misdirected. Instead of identifying – and by extension populating – hazards to support change activity, what is needed by the government is to understand what the potential hazards are that may be introduced as the result of a program change. The OEM typically has minimal time/budget to conduct an in depth inquiry to understand full implications of a proposed change. There is also a need to realign producing system safety products in a more expedition method.

The merger between Tasks 201 & 304 revolves around brainstorming **potential** hazards (or hazardous areas). For proposed changes (no matter what the source of the change is), focusing on developing a proposed hazard list serves both the government and the OEM. The government is served by obtaining better insight into potential impacts a proposed change may have on a system. The OEM is served by lowering workload required into developing a realistic assessment the change has on the system. It also reduces system safety analyses rework after the change has been approved in that the detailed hazard analyses is accomplished AFTER the change has been approved instead of BEFORE and AFTER. Expansion of the scope of the task increases the flexibility of the task to be applied to the initial establishment of a program as well as any potential change or trade study the program may be considering. The end product of this task is a listing of potential safety impacts.
Revised to merge Task 201 and Task 304 into a common task that would be applicable across the entire life cycle.

Commented [PDANUAA471]: 44-2
Task description adjusted due to 882E Task 201 & 304 merger here.

201.2.2 PHL Scope: The PHL scope shall include all aspects of the proposed material solution or proposed change.

201.2.2.1 The PHL shall consider interfaces with existing systems.

201.2.3 Hazard Identification: The contractor shall:

201.2.3.1 ~~Review~~ Consider historical documentation on similar ~~and~~ or related legacy systems, including but not limited to:

44-19: Reword 201.2.3.1.1 through 201.2.3.1.13 to focus on considering causal factors and associated potential hazards.
The appendix could more easily talk about all of the sources (of potential hazards/hazardous areas for all 2XX hazard analyses tasks) in one place.
Thus, repetitious discussions in each 2XX are eliminated and potential conflicts (where a source is listed in one task but not in another task) are avoided.

201.2.3.1.1 Sanitized ~~Mishap~~ mishap and incident reports.

44-7 Remove limited use mishap data from 882F. Changing JAG interpretations makes such as references problematic.

201.2.3.1.2 Hazard tracking systems.

201.2.3.1.3 Lessons learned.

201.2.3.1.4 Safety analyses and assessments.

201.2.3.1.5 Health hazard information to include occupational heath.

201.2.3.1.6 Test documentation.

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

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

201.2.3.1.9 Demilitarization and disposal plans.

Commented [PDANUAA472]: 44-5
Was 882E para 201.2.2
Requirement reordered to a subpara under 201.2.1 for better logical flow.
Rephrased to better capture extent.

Commented [PDANUAA473]: 44-6
Was 201.2.2.a
Reworded to align with scope of information that can be made available to contractors.

Commented [PDANUAA474]: 44-7
Current policy does not permit Limited Use Mishap data to be (easily) provided to contractor

Commented [PDANUAA475]: Was 882E para 201.2.2.b

Commented [PDANUAA476]: Was 882E para 201.2.2.c

Commented [PDANUAA477]: Was 882E para 201.2.2.d

Commented [PDANUAA478]: Was 882E para 201.2.2.e
Environmental and the Occupational Health reviews often get left off of the change requests and it would be good to strengthen the language

Commented [PDANUAA479]: Was 882E para 201.2.2.f

Commented [PDANUAA480]: Was 882E para 201.2.2.g

Commented [PDANUAA481]: Was 882E para 201.2.2.h

Commented [PDANUAA482]: Was 882E para 201.2.2.i

201.2.3.1.10 Software anomalies reports, backlogs, etc

201.2.3.1.11 Involvement with System Of Systems (SOS)

201.2.3.1.12 Human system integration

201.2.3.1.13Emerging technologies

201.2.4 Hazard Characterization: Hazardous areas are not characterized into specific hazards for this task. The contractor should characterize hazardous areas within the constraints of available information.

201.2.5 Risk Assessment: Risk is not assessed for identified hazardous areas for this task.

201.2.6 Identification of Potential Hazard Controls.

201.2.6.1 The contractor shall identify opportunities within the material solution or proposed change where potential hazards may be eliminated or controlled.

201.2.6.2 **PHL Documentation:** The contractor shall compile a Preliminary Hazard List (PHL) identifying system safety impacts and potential hazards/hazardous areas inherent to the initial concept or proposed change.

201.2.6.1 PHL content, as a minimum, shall address:

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

201.3.1 A brief description of ~~the~~ potential hazards/hazardous areas

Commented [PDANUAA483]: 44-8
Software anomalies are a valuable source of safety issues.

Commented [PDANUAA484]: 44-9
For systems incorporated in a SOS, other issues associated with the SOS should be considered.

Commented [PDANUAA485]: 44-10
The interface between the human and a machine is a source of hazards that need to be considered

Commented [PDANUAA486]: The task is to brainstorm potential hazardous areas. Lack of design maturity at this stage of the life cycle limits the ability to properly characterize hazards. That will occur is subsequent hazard analyses tasks.

Commented [PDANUAA487]: The task is to brainstorm potential hazardous areas. Since these areas have not been characterized, risk cannot be determined. That will occur in subsequent hazard analyses tasks.

Commented [PDANUAA488]: 44-3
Brainstormed controls based solely on potential hazards without the benefit of detailed hazard analyses being accomplished. At this stage, hazards have not been fully characterized, only identified. Identifying potential controls (within limits of understanding the hazardous area) provides the decision makers options of strategies that could be employed to control identified potential issues

Commented [PDANUAA489]: 44-4
Charges the contractor to compile a listing of potential hazards.

Commented [PDANUAA490]: 44-11
Was 882E para 201.2.The PHL does not incorporate key fields common to the rest of the 2xx hazard analyses tasks. When used for evaluating changes that are NOT formally approved, it is impracticable to populate with the HTS with potential issues that will not be further developed. Eventually, such records will make the HTS unmanageable Thus, PHL potential hazard documentation does not meet the rigor of the HTS but needs to be readily adapted to the HTS once the potential issues are transformed into hazards

Commented [PDANUAA491]: 44-12
(was 201.2.3.a)
Clarification

201.3.2 Where in the proposed system or associated change the potential hazard could exist to include subsystems, involved software, external System of Systems (SoS) interfaces, etc.

201.3.3 ~~The causal~~ If characterized, the initial causal factor(s) for each identified potential hazard.

201.3.4 Linkage to existing hazards and associated system safety risk levels.

201.3.5 Mode(s) of operation(s) of the potential hazard.

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

~~a. Imposition of Task 201. (R)~~

Commented [PDANUAA492]: 44-13
Clarification to establish context of the hazard

Commented [PDANUAA493]: 44-14
(was 201.2.3.b)
Grammar & Clarification
Initial causal factors are those initially identified during the PHL brainstorming activity. Subsequent 2XX hazard analyses will refine the initial causal factors into hazard causal factors,

Commented [PDANUAA494]: 44-15
For proposed changes, understanding how potential hazards are related to existing hazards is important

Commented [PDANUAA495]: 44-16
Modes are a potential hazard causal source

Commented [PDANUAA496]: 44-19
See 23-2
Since details are not being included in SOWs or RFPs as required, restructured tasks not to address these details in a manner that does not require inclusion in RFPs or SOW language.

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

~~c. Guidance on obtaining access to Government documentation.~~

~~d. Content and format requirements for the PHL.~~

~~e. Concept of operations.~~

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

~~g. References and sources of hazard identification.~~

201.3 Upon approval of the proposed change, trade study, material solution, etc, the PHL shall be incorporated into the HTS and subsequent hazard analyses activities.

Commented [PDANUAA497]: See 44-19
See 23-2
Since details are not being included in SOWs or RFPs as required, restructured tasks not to address these details in a manner that does not require inclusion in RFPs or SOW language.

Commented [PDANUAA498]: 45-1
Establishing the expectation to take the PHL list for a change and then incorporate into the HTS once the proposed change has been approved.
Thus, initial PHL work is flown into subsequent system safety activities without having to rework.

TASK 202
PRELIMINARY HAZARD ANALYSIS

NOTE: Task 202 format has been restructured to align with format conventions used in other 2XX Tasks. As such, content has been rearranged to align with the new format

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

202.1 Purpose. Task 202 is to perform, document, and maintain a Preliminary Hazard Analysis (PHA) to:

202.1.1 Identify hazards

202.1.2 Preliminary hazard characterization

202.1.3 Assess the initial risks,

202.1.4 Identify potential conterol measures.

202.1.5 Document hazard analyses in the Hazard Tracking System (HTS)

202.2 Task description. The contractor shall perform and document a PHA to determine initial risk assessments of identified hazards. ~~Hazards associated with the proposed design or function shall be evaluated for severity and probability based on the best available data, including (but not limited to) mishap data (as accessible) from similar systems, legacy systems, other hazard analyses, and other lessons learned. Provisions, alternatives, and mitigation measures to eliminate hazards or reduce associated risk shall be included.~~

202.2.1 PHA Scope: The PHA is accomplished early in the acquisition life cycle, often when the design has not matured into a stable configuration.

202.2.2 **Hazard Identification:** The contractor shall assess the proposed design, function or change/modification for safety hazards.

46.3 The old 202.2.2 subparas will be addressed in appendix A. Most of the 2XX Tasks each described hazardous sources to consider – yet, lists of sources are inconsistent. A single discussion outlining sources for hazard analyses reduces redundant language while eliminating the potential inconsistent items on the source list

202.2.3 **Hazard Characterization:** The contractor shall use the best available data to characterize each hazard by applying paragraph 4 methodology. Such characterization is preliminary and may change as the design matures/evolves. Characterization details shall include, but not limited to:

202.2.3.1 Hazard Description to include a brief overview of the safety issue.

Commented [PDANUAA499]: 46-1
Format realigned to match other 2XX Tasks.
Added preliminary hazard characterization ➔ these are the details that define the hazard as derived from the hazard analyses. This step needs to occur BEFORE initial risk can be assessed.
Added maintenance of PHA so task will be applicable over life cycle
Added documentation link to the HTS.

Commented [PDANUAA500]: 46-2
Hazard sources are inconsistently listed among 2XX Tasks. Though there is some overlap, but many sources are unique to a particular task.
As hazard sources listed are not an all-inclusive list, this material is being moved to Appendix A. This reduces the redundant verbiage.

Commented [PDANUAA501]: See 46-2.
Before system safety risks can be assessed, hazards must be defined.
FUTURE ACTION: 882E para 202.2.2 subparas a-t will be addressed in appendix A

Commented [PDANUAA502]: 46-3

Commented [PDANUAA503]: See 46-2
Detailing factual design based details to properly frame the hazard.
The following subparas were based on brainstorming details that would be useful in the PHA. It is understood that such characterization is PRELIMINARY and may change as the design matures.

202.2.3.2 Hazard Causal Factors to include hardware, software, human involvement, and environmental considerations.

202.2.3.3 Hazard Effects to include hazard consequences to the subsystem, system, SOS, personnel, software, etc.

202.2.3.4 Identification of where in the system the hazard exists. e.g. hardware components, what "unit" of software, etc.

202.2.3.4.1 Software "units" shall include the corresponding SWCI and AICI levels

202.2.3.4.2 Emergency systems shall focus on preserving the function for when needed during an emergency.

202.2.3.5 Identification of when the hazard asserts itself (e.g. phase of operation or maintenance, mode of operation or maintenance, etc)

202.2.3.5.1 Identification of test unique aspects of the hazard.

202.2.3.6 Identification of interfaces between subsystems, hardware, software "units', human, and SOS where applicable

202.2.3.6.1 Software contributions shall include software developed by other sources.

202.2.3.7 Identification of (safety) functions impacted by the hazard

202.2.3.8 Identification of NDI (e.g. COTS, GOTS, REUSE Software, GFE, etc) associated with the hazard.

202.2.3.8.1 Evaluation of NDI to determine if usage is different from what the NTI was originally designed for.

202.2.3.8.2 Unless otherwise approved by the government, hazard analyses shall be limited to NDI inputs, outputs, and other interfaces. Details internal to the NDI whall be treated as a "black box".

202.2.3.9 Identification of Control Loop impacts

202.2.4 **Initial Hazard Risk Assessment:** The contractor shall develop an initial assessment of the system safety risk of the current system without consideration of additional controls.

202.2.4.1 The definitions in Table I shall be used to characterize hazard severity.

202.2.4.2 The definitions in Table II shall be used to characterize hazard probability.

202.2.4.3 Table III shall be used to derive the **Initial HRI** of the hazard**.**

Commented [PDANUAA504]: See 46-2
Reformat 882E para 202.2.3 to more clearly state specific requirements as detailed in suparas.

202.2.5 **Identification of Potential Control Methods:** The contractor shall identify potential control measures to lower the system safety risk to an acceptable level.

202.2.5.1 The risk control measures shall use the safety design order of precedence as specified in 4.3.4.1.

202.2.6 **PHA Documentation:** The contractor shall document each PHA hazard in the HTS.

202.3 HTS Fields: The following fields shall be incorporated into the HTS. Additional HTS fields may be added as necessary.

a. Unique Hazard Tracking Number
b. Hazard Description
c. System/Subsystems Involved with Hazard
d. Hazard Causal Factors
e. Hazard Effects
f. Hazard Location
g. Hazard Phase
h. Hazard Mode of Operation
i. Associated Functions
j. Hazard Probability
k. Hazard Severity
l Initial HRI
m. Potential Control Measures
n. Hazard Status
o. Link to Other Related Hazards

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

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

~~a. System components.~~
~~b. Energy sources.~~
~~c. Ordnance~~
~~d. Hazardous Materials (HAZMAT).~~
~~e. Interfaces and controls.~~
~~f. Interface considerations to other systems when in a network or System-of-Systems (SoS) architecture.~~
~~g. Material incompatibilities compatibilities.~~
~~h. Inadvertent activation.~~
~~i. Commercial-Off-the-Shelf (COTS), Government-Off-the-Shelf (GOTS), Non-Developmental Items (NDIs), and Government-Furnished Equipment (GFE) to include usage different from what the COTS, GOTS, NDI, or GFE was originally designed for.~~

Commented [PDANUAA505]: See 46-2
It is understood that potential hazard control methods may change as the result of the design maturation/evolution

Commented [PDANUAA506]: 46-4
Each 2XX Tasks has a different set of HTS Fields pertinent to that analyses. As such, required HTS fields include those identified in para 4.3.1.5

FUTURE ACTION: Review 4.3.1.5 and all 2XX.3 HTS Fields eliminate duplications.

Commented [PDANUAA507]: See new 202.2.6

Commented [PDANUAA508]: 46-3
See 202.2.2 – Hazard Identification
FUTURE ACTION: Move source of hazard discussion to appendix

Commented [PDANUAA509]: 46-5
Clarification needed. What aspect of ordnance is of concern? Malfunction/Detonation?
See 46-3 ➔ move source of hazard discussion to the appendix

Commented [PDANUAA510]: 46-6
Typo
See 46-3 ➔ move source of hazard discussion to the appendix

Commented [PDANUAA511]: 46-7
An important aspect of COTS, GOTS, NDI and GFE is not addressed. When using such items outside the design envelope is a significant source of hazards.
See 46-3 ➔ move source of hazard discussion to the appendix

~~*j. Safety significant software* Software *developed by the contractor or* , including software developed by other contractors or sources. Design criteria to control safety-significant software commands, and responses (e.g., inadvertent command, failure to-command, untimely command or responses, and inappropriate magnitude) shall be identified, and appropriate action shall be taken to incorporate these into the software (and related hardware) specifications. *Software contributions shall consider software's control over hardware or the generation of information.*~~

~~k. Operating environment and constraints.~~

Commented [PDANUAA512]: 46-8
Incorrectly worded requirement.
See 46-3 ➔ move source of hazard discussion to the appendix

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

m. Modes *of operation to include maintenance modes*.

n. Health hazards.

o. Environmental impacts.

47-11 May need a clarification statement next to it.
i.e. flammable atmosphere, corrosion or is it a NEPA thing?

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

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

r. Event-unique hazards. (i.e. test)

47-12 Are there other examples other than test that could better clarify this potential hazard contribution?

s. Interfaces with Built built infrastructure, real property installed equipment, and support equipment.

47-13 Are there other aspects besides interfaces that need to be considered here?

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

u. Control loops

v. Artificial Intelligence

w. Historical performance of related systems, subsystems, components, etc

47-6 Is this list complete? Crew management?

47-7 Should this list be reordered to better group hazardous sources? For example, is C & L are very similar

Commented [PDANUAA513]: 47-1
Mode of operation does not suggest maintenance modes which often function significantly differently from operation modes. Thus, hazards unique to maintenance are often overlooked
See 46-3 ➔ move source of hazard discussion to the appendix
FUTURE ACTION: Move source of hazard discussion to appendix

Commented [PDANUAA514]: 47-11
See 46-3 ➔ move source of hazard discussion to the appendix

Commented [PDANUAA515]: 47-2
- A hazard is realized in a system, not a requirement. The requirement is a means to help shape a system.
- Emergency system covers systems not accounted for above.

See 46-3 ➔ move source of hazard discussion to the appendix

Commented [PDANUAA516]: 47-12
See 46-3 ➔ move source of hazard discussion to the appendix

Commented [PDANUAA517]: 47-13
See 46-3 ➔ move source of hazard discussion to the appendix

Commented [PDANUAA518]: 47-3
Control Loop interaction with hazards not accounted for in analyses
See 46-3 ➔ move source of hazard discussion to the appendix

Commented [PDANUAA519]: 47-4
Artificial Intelligence not account for in analyses
See 46-3 ➔ move source of hazard discussion to the appendix

Commented [PDANUAA520]: 47-5
See 46-3 ➔ move source of hazard discussion to the appendix

Commented [PDANUAA521]: 47-6
See 46-3 ➔ move source of hazard discussion to the appendix

Commented [PDANUAA522]: 47-7
See 46-3 ➔ move source of hazard discussion to the appendix

202.2.3 ~~For each identified hazard, the PHA shall include an initial risk assessment (e.g. no mitigations considered). The definitions in Tables I and II, and the Hazard Risk Index (HRI) Risk Assessment Codes (RACs) in Table III shall be used, unless tailored alternative definitions and/or a tailored matrix are formally approved in accordance with Department of Defense (DoD) Component policy~~.

~~202.2.4 For each identified hazard, the PHA shall identify potential risk mitigation measures using the system safety design order of precedence specified in 4.3.4.1.~~

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

~~a. Imposition of Task 202. (R)~~

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

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

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

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

Commented [PDANUAA523]: 47-8
(1) Scope of PHA expectation open ended
(2) RAC term replaced by HRI
(3) duplicating 4.3.8
See 46-3 ➔ move source of hazard discussion to the appendix

Commented [PDANUAA524]: 47-9
Incorrect para reference. 4.3.4 ➔ 4.3.4.1
See 46-3 ➔ move source of hazard discussion to the appendix

Commented [PDANUAA525]: 47-10
Since details are not being included in SOWs or RFPs as required, restructured tasks not to include these details
See 23-2

~~f. Concept of operations.~~

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

Commented [PDANUAA526]: See 47-12

TASK 203
SYSTEM REQUIREMENTS HAZARD ANALYSIS

Commented [PDANUAA527]: 49-1

49-1
Hazard Analyses and Compliance/Verification are distinct different activities. Both these activities are needed for different reasons and are complementary to the goal of identifying hazards associated with a system.

- Compliance with a list (e.g. requirement listing, checklist, etc) leverages knowledge gained from history (e.g. accidents, material characteristics, research) of known consequences
- Systemic Hazard Analyses applied to designs often reveals design aspects that have never been realized before; therefore prompting questions that have never been asked before.

But fundamentally, even though these different approaches are complementary, different questions are being asked for different reasons. Focus of Task 203 should be on hazard analyses; move compliance/verification aspects to a new task
FUTURE ACTION: Review MIL-STD-882C Task 203 (SRHA) – which does not cite compliance -to determine if analytical tasks listed below are correct.
FUTURE ACTION: Move Compliance/verification aspects of Task 203 to a new 3XX task.

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

Commented [PDANUAA528]: Reformat to increase readability;
minor edits to clarify operating and maintenance modes; revised scope to focus task on hazard analyses. Issues with existing purpose:
* "*determine design requirement to eliminate hazards or reduce risks for a systems; to incorporate these requirements into the appropriate system documentation*" ➔ These aspects are the results of other 2XX Hazard analyses tasks;
* *assessing compliance of the system with these requirements* ➔ see 49-1

203.1 Purpose. Task 203 is to perform, document, and maintain a System Requirements Hazard Analysis (SRHA) for all life-cycle phases and operating/maintenance modes to:

Commented [PDANUAA529]: Added maintenance of SRHA to keep relevant over life cycle

a. analyze design requirements to identify safety concerns with requirement gaps and conflicts.

b. analyze design requirements to identify impacts to hazards and associated hazard controls.

~~c.~~ document each requirement gap, requirement conflict, and impact to previously identified hazard. ~~Documentation to include a clear indication of which recommended control measure(s) program management concurred with and rational for rejected recommended control measure(s).~~

Commented [PDANUAA530]: 49-3
Purpose revised to focus on perceived SRHA outputs.

The statement "Documentation to include a clear indication of which recommended control measure(s) program management concurred with and rational for rejected recommended control measure(s)." ➔ move to para 4.3.6.1 as this applies to all hazards, regardless of the task that drives them. (comment 13-8)

49-3 & 49-43

a. Reviewing (hard and derived) design requirements may identify safety concerns with requirement gaps and conflicts. **This is often done before a design has been formulated, and as a result, it is not possible to properly characterize hazards.** Therefore, the task output is not identifying hazards, but rather identifying the requirement gaps/conflicts and associated (broad) safety concerns. The other 2XX tasks use this output to identify/characterize hazards.

b. A second way requirements can be analyzed is to determine the impacts to previously identified hazards (or the associated controls for the hazard). This is more obvious when considering proposed modification requirements where hazards have already been identified against the pre-modification baseline design.

But this could also be viewed as taking outputs from other 2XX tasks and looking back to the requirements. When a control is identified against a hazard, does the control introduce impacts with other requirements?

c. Issues with requirements introduce safety concerns, but what is the proper way to document a & b? If the design is not mature enough to properly characterize a hazard, then a "proto-hazard" or safety concern construct is needed.

For a proposed modification, one must be careful of how a previously identified hazard is updated/revised. If the proposal is not incorporated, the resulting documentation cannot suggest that it was incorporated.

FUTURE ACTION: Determine the construct/format/minimal content required to document policy gaps, policy conflicts, and impacts to previously identified hazards/controls.

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

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

203.2.1 **Scope:** Using best available data, systematically analyze design requirements to identify safety requirement issue through applying hazard analysis techniques per the System Safety Process Element 2 (i.e. para 4.3.2).

a. Requirement gaps
b. Requirement conflicts
c. Impacts to previously identified hazards or associated hazard controls

203.2.2 **SRHA Safety Concern Identification**: The contractor shall:

203.2.2.1 ~~203.2.3.1 The contractor shall~~ Analyze ~~identify~~ applicable requirements by reviewing military and industry standards and specifications; historical documentation on similar and legacy systems; Department of Defense (DoD) requirements (to include risk ~~mitigation~~ control technology requirements); system performance specifications; other system design requirements and documents; applicable Federal, military, State, and local regulations; and applicable Executive Orders (EOs) and international agreements for safety impacts.

Commented [PDANUAA531]: 49-3 & 49-4
Scope & Direction: This task should focused on reviewing the requirements for potential safety issues. Issues with existing task include:
- Evaluating the requirement set to determine if the requirements are correct and complete is suggested by the title of the task. Hazards can thus be identified from such disconnects – but characterization of the hazard occurs in a subsequent 2xx Tasks. Characterization needs to occur BEFORE the remainder of the task can be accomplished since knowing what the hazard set is is required BEFORE identifying requirements to control these hazards.
- As written, this Tasks appears to be redundant with other 2xx Tasks, at least from the hazard control perspective. Controlling hazards frequently rely on invoking standards in the specs to "adjust" the design. If redundant, then **what is the value of this task?**

Proposed focus would be to analyses a system's requirement set to identify potential safety issues.
Task title states this is a hazard analyses task – yet where are hazards are being identified as part of this task?
- Early in a program when the focus is on ensuring correct requirements are being identified, the system architecture is very fluid. So, what will a hazard look like in this phase of the life cycle? What could be identified as hazards are hard & derived requirement gaps/conflicts? For mods/trade studies, it may be easier to anchor a hazard into the system design. At the concept of a program, creative writing will be needed. Agile SW has some implications as incremental derived requirements could be evaluated.

The output of the task should be focusing around identifying issues/gaps with the requirements. The other 2xx Tasks cover the hazard characterization.

Commented [PDANUAA532]: 49-5
882E Para 203.2.1 issue:
- Focus on system design requirements
- Statement could be interpreted as an overreach outside the system safety sphere of responsibility.

Reworked into Scope para (see rational for revising purpose) to focus Task 203.2.1 on the products of Task 203.
- Requirement Gaps/Conflicts can feed other 2XX tasks.
- Identifying impacts to previously identified hazards & associated hazard controls can likewise feed other 2XX tasks

Commented [PDANUAA533]: See ii-2

Commented [PDANUAA534]: 49-7
Clarify activity.
Limit scope to safety impacts.

203.2.2.2 Through analyses, identify requirement gaps and associated safety concerns.

203.2.2.3 Through analyses, identify requirement conflicts and associated safety concerns.

203.2.2.4 Through analyses, identify requirement impacts to previously identified hazards or associated hazard controls.

203.2.3 **SRHA Characterization**: Hazardous areas are not characterized into specific hazards for this task. The contractor shall characterize hazardous areas within the constraints of available information using the System Safety Process Element 2 (i.e. para 4.3.2) & Element 3 (i.e. para 4.3.3) and shall address:

a. Requirement citation
b. Description of requirement issue (e.g. gap, conflict, etc)
c. Portion of the design affected
d. Identification of affected interfaces (hardware, software, human-machine, cyber networks, other systems, etc)
e. Identification of affected control laws
f. Projected hazard causal factors.
g. Identification of affected NDI (e.g. COTS, GOTS, RESUSE Software, GFE, etc)
h. Evaluation of NDI to determine if usage is different from what the NDI was
i. HTS reference to previously identified hazards with requirement safety impacts and/or associated controls.
j. HTS reference to hazards where safety issues have been analyzed and characterized.

203.2.4 **Assess SRHA Risk**: Risk is not assessed for identified hazardous areas for this task.

203.2.5 **Identify Potential SRHA Corrective Actions**:

~~203.2.3.1 The contractor shall recommend appropriate system design requirements to eliminate hazards or reduce the associated risks identified in accordance with Section 4 of this Standard.~~

~~203.2.3.2 The contractor shall define verification and validation approaches for each design requirement to eliminate hazards or reduce associated risk.~~

203.2.5.1 The contractor shall identify appropriate design requirements to address identified requirement gaps.

203.2.5.2 The contractor shall identify appropriate design requirements to address identified requirement conflicts.

203.2.5.3 The contractor shall identify appropriate design requirements to address identified impacts to previously identified hazards or associated hazard controls.

Commented [PDANUAA535]: The task is to analyze requirements to identify potential hazardous areas. Lack of design maturity at this stage of the life cycle limits the ability to properly characterize hazards. That will occur is subsequent hazard analyses tasks.

FUTURE ACTION: Determine how requirement safety issues be tracked. If unable to characterize as a hazard, then the HTS is not appropriate. Likewise, resolved requirement safety issues are OBEed and are often forgotten about.
QUESTION – Should requirement gaps & conflicts be tracked in a closed loop fashion?

Commented [PDANUAA536]: The task is to analyze requirements potential hazardous areas. Since these areas have not been characterized, risk cannot be determined. That will occur in subsequent hazard analyses tasks.

Commented [PDANUAA537]: 49-8
Revised discussion to align with other restructuring changes in this Task. Intent addressed in 203.2.5.1, 203.2.5.2, & 203.2.5.3
Ambiguous reference (Section 4)

Commented [PDANUAA538]: Issue: Open ended ➔ potentially beyond safety responsibility. If this is for every hazard identified, this would be an ongoing task throughout the entire program and overlaps with other 2XX Tasks wrt Hazard Controls.
Issue: Verification and Validation (V&V) for hazard control requirements.
Moved to para 4.3.5 (as this should apply to ALL hazard controls involving requirements)

203.2.6 **SRHA Documentation**: The contractor shall:

203.2.6.1 Document identified requirement gaps with safety impacts and the associated corrective action opportunities.

203.2.6.2 Document identified requirement conflicts with safety impacts and the associated corrective action opportunities.

203.2.6.3 Document identified impacts to previously identified hazards, previously identified hazard controls, and associated corrective action opportunities.

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

203.2.6.4 Incorporate approved design requirements into the engineering design documents, ~~and~~ hardware, software, and system test plans, as appropriate.

- Scope? As written, this transcends safety and duplicates standard systems engineering process.

FUTURE ACTION: Revise to limit scope to requirement related safety impacts

- This does not align well with revised purpose. It is also applicable to all hazards, and thus, should this be moved to 4.3.5?

FUTURE ACTION: Move to 4.3.5 or revise requirement

203.2.6.5 As the design evolves, ensure applicable design requirements flow down into the system and subsystem specifications, preliminary hardware configuration item development specifications, software requirements specifications, interface requirements specifications, and equivalent documents.

- Scope? As written, this transcends safety and duplicates standard systems engineering process.

FUTURE ACTION: Revise to limit scope to requirement related safety impacts

- This does not align well with revised purpose. It is also applicable to all hazards, and thus, should this be moved to 4.3.5?

FUTURE ACTION: Move to 4.3.5 or revise requirement

Commented [PDANUAA539]: 49-8 reformat

Commented [PDANUAA540]: 49-9 reword for clarity; corrected poor grammar

203.2.6.6 As appropriate, use engineering change proposals to incorporate applicable design requirements into these documents.

- Scope? As written, this transcends safety and duplicates standard systems engineering process.

FUTURE ACTION: Revise to limit scope to requirement related safety impacts

- This does not align well with revised purpose. It is also applicable to all hazards, and thus, should this be moved to 4.3.5?

FUTURE ACTION: Move to 4.3.5 or revise requirement

203.2.6.7 ~~203.2.3~~ The contractor shall assess compliance of the development of the system hardware and associated software with the identified requirements. The contractor shall:

This is a different activity than addressed in the revised purpose/scope above.
FUTURE ACTION: Move to a new TBD Compliance Tasks.

~~203.2.3.a Address safety requirements at all contractually required technical reviews, including such as design reviews (such as Preliminary Design Review (PDR) and Critical Design Review (CDR)) and the Software Specification Review. The contractor shall address the hazards, mitigation control measures, means of verification and validation, and recommendations.~~

~~203.2.3.b Review test plans and results for verification and validation of hardware and software compliance with requirements. This includes verification and validation of the effectiveness of risk mitigation measures.~~

50-1
FUTURE ACTION: Delete & Move verification and validation is a Task 3XX effort. Move to a 3XX Task.

203.2.5.2 Ensure that hazard ~~mitigation~~ control information are incorporated into the operator, maintenance, user, training, logistics, diagnostic, ~~and~~ demilitarization and disposal manuals and plans, and other documentation.

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

~~a. Imposition of Task 203. (R)~~

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

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

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

Commented [PDANUAA541]: 49-10

Commented [PDANUAA542]: 49-11
Delete Requirement.
There is a scope issue where safety could be construed as reviewing ALL requirements at all required meetings. This is outside the scope of MIL-STD-882's authority (already being covered by Systems Engineering)
In addition, this requirement overlaps the other 2XX Tasks (e.g. hazard controls actions involving revisions to formal requirements).
Furthermore, an inclusive list of meetings is provided; what about meetings outside this list that discuss requirement of safety interest?
This is a different activity than addressed in the revised purpose/scope above.
See also rationale for deletion of Tasks 104 & 105.

Commented [PDANUAA543]: See ii-2

Commented [PDANUAA544]: 50-1

Commented [PDANUAA545]: See ii-2

Commented [PDANUAA546]: 50-2
Append "… and other documentation"
This is not a comprehensive list; therefore need to make the expectation open ended.

~~e. Concept of operations.~~

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

FUTURE ACTION: Add a new 203.3 to define the minimum issue tracking fields required as the result of this task. See 203.2.3.a -203.2.3.j

(HTS is not really applicable since, as above comments indicate, the output of this task is not hazards, but rather safety issues resulting from requirements. Thus a different tracking system is needed … unique to this task?)

Commented [PDANUAA547]: 50-3 Delete
Since details are not being included in SOWs or RFPs as required, restructured tasks not to include these details
See 23-2

Commented [PDANUAA548]: 50-4

TASK 204
SUBSYSTEM HAZARD ANALYSIS

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

204.1 Purpose. Task 204 is to perform, ~~and~~ document, and maintain a Subsystem Hazard Analysis (SSHA) to:

a. ~~verify subsystem compliance with requirements to eliminate hazards or reduce the associated risks~~;

51-2 **FUTURE ACTION:** Verification should be in Task 3xx
- Granted, incorrect/incomplete requirements do lead to hazards. But need to be very careful here that compliance is being looked at by system safety to identify hazards. It is NOT being done as a formal requirement compliance verification activity. As such, need to revise to make this distinction
- This assumes/asserts **non-compliance = hazards** which is also incorrect

b. identify ~~previously unidentified~~ hazards associated with the design of the designated subsystem(s) ~~subsystems~~; If no subsystem(s) are specifically designated, a separate SSHA shall be accomplished for each subsystem in the design.

c. characterize subsystem hazards

d. assess initial/current risks

e. identify potential control measures per design order of precedence (ref. 4.3.4.1)

f. ensure potential control measures do not introduce new safety issues

g. document hazard analyses in the Hazard Tracking System (HTS)

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

204.2 Task description: The contractor shall perform, document, and maintain an SSHA to identify hazards, characterize hazards, assess safety risk, identify control measures, and verify implementation of control measures of identified subsystem components and equipment.

~~204.2.1 At a minimum, the analysis shall:~~

~~204.2.1.a Verify subsystem compliance with requirements to eliminate hazards or reduce the associated risks.~~

Commented [PDANUAA549]: Reformat for improved readability

Commented [PDANUAA550]: Clarification. Even after CDR, maintaining the SSHA is important to account for any modifications/changes to the design. In addition, incorporating trends/anomalies/failures/etc from fielded systems keeps the analyses relevant to the fielded configuration(s)

Commented [PDANUAA551]: 51-2
See text box.
FUTURE ACTION: Move to Task 3xx

Commented [PDANUAA552]: 51-3
(moved from 204.2.1.b)
"previously unidentified" is non-value added text
Wordsmithing to focus scope of task

Additional bullets outline different aspects of hazard development/management

Commented [PDANUAA553]: 51-4
Links action to Element 4 as this is a major feature of the system safety process

Commented [PDANUAA554]: •Reformatted to increase readability
•COTS, GOTS, GFE, and NDI moved to scope (moved to 204.2.1.7)
•"Areas to consider …" are an incomplete list of potential causal areas. Such a discussion is more appropriate for the appendix.
•"While conducting …" (moved to 204.2.1.8)

Commented [PDANUAA555]: 51-5
Task restructured into a standard format with other 2XX Tasks. Content adjusted to fit new format and focus on subsystems.

Commented [PDANUAA556]: 51-6
See 51-2
Verification/Validation are valid activities, but they are not hazard analyses. Delete for SSHA.
FUTURE ACTION: Move Validation & Verification to 3xx Tasks

~~204.2.1.a(1) Validate applicable flow-down of design requirements from top-level specifications to detailed design specifications for the subsystem.~~

~~204.2.1.a(2) Ensure design criteria in the subsystem specifications have been satisfied and that verification and validation of subsystem mitigation measures have been included in test plans and procedures.~~

~~204.2.1.b Identify new previously identified hazards or implacts to existing hazards associated with the design of subsystems to include:~~

~~204.2.1.b(1) Ensure implementation of subsystem design requirements and mitigation measures have not introduced any new hazards~~

~~204.2.1.b(2) Determine modes of failure, including component failure modes and human errors, single point and common mode failures, the effects when failures occur in subsystem components, and from functional relationships between components and equipment comprising each subsystem. Consider the potential contribution of subsystem hardware and software events (including those developed by other contractors/sources, COTS, GOTS, NDIs, and GFE hardware or software), faults, and occurrences (such as improper timing).~~

202.2.1 SSHA Scope

204.2.1.1 This analyses shall include NDI (e.g. COTS, GOTS, GFE, etc.).

204.2.1.1.1 NDI shall be treated as "Black Boxes" in the analyses unless (1) sufficient design details are available to analyze appropriately and (2) government approval for analyses on the NDI has been granted.

204.2.1.1.2 If NDI are used in an environment or manner other than originally designed for, and detail analyses has not been accomplished for the expanded environment, then the expanded operating environment shall be documented in the hazard analyses as an "Assumption that such expansion has not introduced additional hazards".

204.2.1.2 Software associated with a subsystem shall be clearly identified so that future references to aspects of the software supporting subsystem are unambiguous.

204.2.1.3 The contractor shall obtain PM approval of hazard analysis techniques to be used before performing the analysis.

204.2.1.4 When software to be used in conjunction with the subsystem, the contractor performing the SSHA shall monitor, obtain, and integrate the output of each phase of the software development process in evaluating the software contribution to the SSHA.

204.2.1.4.1 The contractor shall coordinate with the PM hazard control actions involving software development.

204.2.1.5 The contractor shall updated, as necessary, the SSHA following system design changes, including software ~~design~~ changes.

Commented [PDANUAA557]: 51-7
Moved to Purpose (para 204.1.b). See 51-3

Commented [PDANUAA558]: 51-8
Moved to 204.2.5.2

Commented [PDANUAA559]: 51-13
Too densely written. Reformat to be less dense so each area is more easily absorbed.
Intent moved to 204.2.3

Commented [PDANUAA560]: 51-9
Non-Developmental Items (NDI) from the government perspective includes any item developed elsewhere to include COTS, GOTS, GFE, etc. See 3.1.24. If the item development is not being done within the program, then that item is NDI. Citing NDI with the understanding that COTS, GOTS, GFE, etc simplifying text without losing the intent.

NDI frequently has inherent limitations that affects the extent the NDI can be analyzed. As such, NDI must be treated as "Black Boxes" from an analytical perspective. In addition, these items often are used in environments other than what they were originally designed for. As such, hazards may be introduced from the envelop expansion BUT NOT ABLE TO BE ANALZED

Commented [PDANUAA561]: See 52-1

Commented [PDANUAA562]: 51-16
Was 204.2.5
Verbiage adjusted to account for a variety of software development approaches available to be used. 882 needs to work with any of these approaches.
Verbiage adjusted to focus contractor requirement better. PM involvement does not belong into the contractor requirements.

Commented [PDANUAA563]: 51-17
Moved from 204.2.4
Minor edit

204.2.1.6 The contractor shall re-evaluate the subsystem if the subsystem's operating environment changes.

204.2.1.7 Additional areas ~~Areas~~ to consider, but not limited to, include performance, performance degradation, functional failures, timing errors, design errors, ~~or~~ defects, control law failures, and inadvertent functioning.

51-11
New para 204.2.1.3 is only a partial list of things to consider in SSHA. The intent is not to limit the scope to these activities.
A discussion in the appendix addressing a host of potential hazard causal factors needs to be include (instead of repeating the same discussion outlining the areas to consider in each 2XX task)
There is also a partial list of causal factors (see MIL-STD-882E para 204.2). Is it needed to repeat the PHA list of causal factors/hazard sources?
What about control loop impacts?
What about interfaces to other subsystems?

204.2.1.8 While conducting this analysis, the human shall be considered a component within a subsystem, receiving both inputs and initiating outputs.

204.2.2 **Hazard Identification:** The contractor shall apply systematic hazard analyses techniques to identify new safety hazards or impacts to existing hazards to the subsystem, interfaces, control laws, functions, and other software interacting with the subsystem.

204.2.2.1 The contractor shall obtain government approval of hazard analyses techniques to be used before performing the hazard analyses.

204.2.2.2 As necessary, the contractor shall incorporate supporting subsystem component data for hazard analyses developed by associate contract agreements, government organically developed items, and/or other NDI sources.

204.2.3 **Hazard Characterization:** The contractor shall use the best available data to characterize each subsystem hazard by applying paragraph 4 methodology to include, but not limited to:

204.2.3.1 Subsystem name

204.2.3.2 Hazard Description

204.2.3.3 Hazard Causal Factors to include hardware, software, human involvement, and environmental considerations.

204.2.3.4 Hazard Effects

204.2.3.5 Proposed hazard controls (e.g. mitigation or amelioration measures)

Commented [PDANUAA564]: 51-18
New requirement to address guidance gap.

Commented [PDANUAA565]: 51-10
Was 204.2
Added to preclude viewing the following examples as the only thing that needs to be considered
Grammar; rewording to flow better with format change

Commented [PDANUAA566]: 51-11
Between the 2XX tasks, there needs to be a clear & concise means to summarize what should be considered.

Commented [PDANUAA567]: Was 204.2

Commented [PDANUAA568]: 51-12
Accounts for distributed development of subsystem components

Commented [PDANUAA569]: Much intent drawn from 882E para 204.2.1.b(2)

Commented [PDANUAA570]: 51-14
Old 204.2.b(2)
Generic reference needed as an explicit list will be too burdensome. Also, such a list is common across all 2XX Tasks.

204.2.3.6 Identification of where in the system the hazard exists. (e.g. hardware components, what "unit" of software, etc.)

204.2.3.6.1 Software "units" shall include the corresponding SWCI and AICI levels

204.2.3.6.2 Emergency systems shall focus on preserving the function for when needed during an emergency.

204.2.3.7 Identification of when the hazard asserts itself. (e.g. phase of operation or maintenance, mode of operation or maintenance, etc.)

204.2.3.7.1 Identification of test unique aspects of the hazard.

204.2.3.8 Identification of interfaces between subsystems, hardware, software "units', human, and SOS where applicable

204.2.3.8.1 Software contributions shall include software developed by other sources.

204.2.3.9 Identification of functions impacted by the hazard

204.2.3.10 Identification of NDI (e.g. COTS, GOTS, REUSE Software, GFE, etc.) associated with the hazard.

204.2.3.10.1 Evaluation of NDI to determine if usage is different from what the NTI was originally designed for.

204.2.3.10.2 Unless otherwise approved by the government, hazard analyses shall be limited to NDI inputs, outputs, and other interfaces. Details internal to the NDI shall be treated as a "black box".

204.2.3.11.1 Identification of Control Loop impacts

204.2.4 **Assess hazard risk level:** The contractor shall develop:

204.2.4.1 An initial assessment of the subsystem risk of the current system without consideration of additional controls.

204.2.4.2 Maintain a current risk assessment of the subsystem risk accounting for all of the hazard controls that have been implemented

204.2.4.3 Project an end state risk assessment of the subsystem risk accounting for all planned and implemented hazard controls.

204.2.4.4 The definitions in Table I shall be used to characterize subsystem hazard severity.

204.2.4.5 The definitions in Table II shall be used to characterize subsystem hazard probability.

204.2.4.6 Table III shall be used to derive the respective subsystem HRIs of the hazard.

~~204.2.1.c Recommend actions necessary to eliminate previously unidentified hazards or mitigate their associated risk. Ensure system-level hazards attributed to the subsystem are analyzed and adequate mitigations of the potential hazards are implemented in the design.~~

204.2.5 **Identification of Potential Hazard Control Methods:** The contractor shall identify potential subsystem hazard controls to lower the system safety risk to an acceptable level.

204.2.5.1 The hazard controls shall be follow the system safety order precedence as defined in paragraph 4.3.4.1.

204.2.5.2 Ensure implantation of subsystem hazard controls have not introduced new hazards or adversely impacted other subsystem hazards.

204.2.6 Subsystem Hazard Analyses Documentation: The contractor shall document the subsystem hazard analyses.

204.2.6.1 The contractor shall develop a subsystem description to include:

a. Subsystem physical characteristics,
b. Software associated with the subsystem
c. Subsystem functionality
d. Subsystem interfaces and associated input/output data
e. Subsystem boundaries
f. Subsystem control loops,
g. Expected subsystem operating environment,
h. Subsystem operating and maintenance modes.
i. NDI components

204.2.6.2 The contractor shall document each applicable subsystem hazard per the Hazard Tracking System (HTS).

204.2.6.3 The contractor shall maintain the currency and correctness of the SSHA. This would include anomalies, changes to the system impacting the subsystem, changes to the subsystem, changes to functionality, etc.

204.2.6.4 The contractor shall describe hazard analyses methods and techniques employed in the subsystem analyses.

204.2.6.5 The contractor shall describe LOR activities (per para 4.4) activities applicable to the subsystem.

Commented [PDANUAA571]: 51-15
Intent not clear.
Reworded in 204.2.5

Commented [PDANUAA572]: 51-16 This is a Task 205 (SHA) activity. Delete from Task 204 (SSHA)

Commented [PDANUAA573]: Was 204.2.5.a

Commented [PDANUAA574]: Was 204.2.5.c

Commented [PDANUAA575]: Was 204.2.5.b
Reworded

204.2.6.5.1 Reference to more detailed system and subsystem descriptions, including specifications and detailed review documentation, shall be supplied when such documentation is available.

52-4

- Should analysis limitations, such as those introduced by NDIs, be identified?
- Should subsystem input/output data be summarized?

204.3: HTS Fields: The following fields shall be incorporated into the HTS. Additional HTS fields may be added as necessary.

a. Unique Hazard Tracking identifier for each hazard
b. Hazard Description
c. Hazard Causal Factors
d. Hazard Effects
e. Hazard Location
f. Hazard Phase
g. Hazard Mode
h. Associated Functions
i. Hazard Probability
j. Hazard Severity
k. Initial HRI
l. Current HRI
m. End-state HRI
n. Potential control measures (aka mitigation or amelioration methods)
o. Hazard Status
p. Hazard control validation/verification
q. Software involvement in the hazard
r. Software in or interfacing with the Subsystem (definitive reference to the portion of the software that relates to the hazard)
s. Mode(s) of subsystem operation
t. Interfaces to other subsystems
u. Link to related hazards

Commented [PDANUAA576]: 52-4
Was 204.2.5.a

Commented [PDANUAA577]: 52-3
FUTURE ACTION: Compare this list with para 4 and delete duplications. Scrub remainder of list to add/delete HTS fields as necessary.
(See 46-4)

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

204.2.3 When software to be used in conjunction with the subsystem is developed under a separate software development effort, the contractor performing the SSHA shall monitor, obtain, and use the output of each phase of the formal software development process in evaluating the software contribution to the SSHA. Hazards identified that require mitigation action by the software developer shall be reported to the PM in order to request appropriate direction be provided to the software developers.

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

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

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

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

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

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

a. Imposition of Task 204. (R)

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

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

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

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

Commented [PDANUAA578]: 52-1
- Moved to 204.2.1.3
- deleted potentially conflicts with para 4
- Clarification of intend (techniques ➔ hazard analyses techniques)

Commented [PDANUAA579]: Moved to 204.2.1.4

Commented [PDANUAA580]: Moved to 204.2.1.5

Commented [PDANUAA581]: Moved to 204.2.4.1

Commented [PDANUAA582]: Moved to 204.2.6.1 & 204.2.6.5.1

Commented [PDANUAA583]: Moved to 204.2.6.4

Commented [PDANUAA584]: Moved to 204.2.6.2

Commented [PDANUAA585]: 52-2
Delete
Since details are not being included in SOWs or RFPs as required, restructured tasks not to include these details
See 23-2

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

~~g. Concept of operations.~~

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

Commented [PDANUAA586]: See 52.2

TASK 205
SYSTEM HAZARD ANALYSIS

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

54-1 Move to 3xx
Verification is not the focus of the system hazard analyses task. It should be addressed in a 3xx task.

205.1 Purpose. Task 205 is to perform, document, and maintain a System Hazard Analysis (SHA) to:

a. identify ~~previously unidentified~~ hazards associated with the subsystem interfaces, subsystem faults; and integrated system design,
b. characterize system hazards
c. assess initial/current risks
d. identify potential control measures per design order of precedent (see 4.3.4.1)
e. ensure potential control measures do not introduce new safety issues
f. document hazard analyses in the Hazard Tracking System (HTS)

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

205.2 Task description. The contractor shall perform, document, and maintain an SHA to identify hazards, characterize hazards, assess safety risk, identify control measures, and verify implementation of control measures of identified system hazards.

205.2.1 **SHA Scope**

205.2.1.1. The SHA analyses shall include NDI such as COTS, GOTS, GFE, etc.

205.2.1.1.1. NDI shall be treated as "Black Boxes" in the analyses unless (1) sufficient design details are available to analyze appropriately and (2) government approval for analyses on the NDI has been granted.

Commented [PDANUAA587]: 54-1
Reformat
See 51-2 concerning verification

Commented [PDANUAA588]: Added maintenance of SSHA to keep relevant over life cycle

Commented [PDANUAA589]: 54-2
See 51-3
"previously unidentified" not needed
Wordsmithing to focus scope of task

Commented [PDANUAA590]: 54-3
Ambiguous inference to design order of precedent clarified.
See 51-4

Commented [PDANUAA591]: 54-4/Realignment
Reformat
Task restructured into a standard forma with other 2XX Tasks. Content adjusted to fit new format and focus on the system

Last line moved to 205.2.1.8

Commented [PDANUAA592]: 54-5
See 51-9

205.2.1.1.2 If NDI (to include COTS, GOTS, GFE) are used in an environment or manner other than originally designed for, and detail analyses has not been accomplished for the expanded environment, then the expanded operating environment shall be documented in the hazard analyses as an "Assumption that such expansion has not introduced additional hazards".

205.2.1.2 System software shall be clearly identified so that future references to aspects of the software supporting the system are unambiguous.

205.2.1.3 The contractor shall obtain PM approval of hazard analyses techniques to be used before performing the analysis.

205.2.1.4 The contractor performing the SHA shall monitor, obtain, and integrate the output of each phase of the software development process in evaluating the software contribution to the SHA.

205.2.1.4.1 The contractor shall coordinate with the PM hazard control actions involving software development.

205.2.1.5 The contractor shall updated, as necessary, the SHA following system design changes, including software ~~design~~ changes.

205.2.1.6 The contractor shall re-evaluate the system if the system's operating environment changes.

205.2.1.7 Additional areas to consider include, but not limited to, include performance, performance degradation, functional failures, timing errors, design errors, defects, control law failures, and inadvertent functioning.

54-10 New para 205.2.1.7.1 is only a partial list of things to consider in SHA. The intent is not to limit the scope to these activities. ➔ FUTURE ACTION: Move this partial list to the appendix addressing a host of potential hazard causal factors
There is also a partial list of causal factors. Is it needed to repeat PHA list of causal factors/hazard sources? What about control loop impacts? What about interfaces to other subsystems?

205.2.1.8 While conducting this analysis, the human shall be considered a component within the system, receiving both inputs and initiating outputs.

205.2.2. **Hazard Identification:** The contractor shall apply systematic hazard analyses techniques to identify new safety hazards or impacts to existing hazards to the system, interfaces, control laws, functions, and other software interacting with the system.

Commented [PDANUAA593]: 54-6
Reworded to remove condition statement on task
See 52-1

Commented [PDANUAA594]: 54-7
Was 205.2.3
Verbiage adjusted to account for a variety of software development approaches.
Verbiage adjusted to focus contractor requirement better.
PM involvement does not belong into the contractor requirements.
See 51-16

Commented [PDANUAA595]: 54-8
Moved from 205.2.1.d
Minor edit
See 51-17

Commented [PDANUAA596]: 54-9
New requirement to address guidance gap. There are already requirements to reevaluate if software changes are made. However, there are no requirements for reevaluating if the environment the software will see changes.
See 51-18

Commented [PDANUAA597]: See 54-10
Between the 2XX tasks, there needs to be a clear & concise means to summarize what should be considered.

Commented [PDANUAA598]: Text moved
Was 205.2

205.2.2.1 As necessary, the contractor shall incorporate supporting system component data for hazard analyses through associate contract agreements government organically developed items, and/or other NDI sources.

54-11
Need to reword for clarity, but think the general intent is captured. If a different group is developing a portion or impacting a subsystem, the safety analyses needs to account for those relevant details. This can be either HW or SW

205.2.3 **Hazard Characterization:** The contractor shall use the best available data to characterize each system hazard by applying paragraph 4 methodology to include, but not limited to:

205.2.3.1 Hazard Description

205.2.3.2 Hazard Causal Factors to include hardware, software, human involvement, and environmental considerations.

205.2.3.3 Hazard Effects to include cascading system level effects.

205.2.3.4 Proposed hazard controls (e.g. mitigation or amelioration measures)

205.2.3.5 Identification of where in the system the hazard exists. (e.g. subsystem/ components, what "unit" of software, etc.)

205.2.3.5.1 Software "units" shall include the corresponding SWCI and AICI levels

205.2.3.5.2 Emergency systems shall focus on preserving the function for when needed during an emergency.

205.2.3.6 Identification of when the hazard asserts itself. (e.g. phase of operation or maintenance, mode of operation or maintenance, etc)

205.2.3.6.1 Identification of test unique aspects of the hazard.

205.2.3.7 Identification of interfaces between subsystems, hardware, software "units', human, and SOS where applicable

205.2.3.7.1 Software contributions shall include software developed by other sources.

205.2.3.8 Identification of functions impacted by the hazard

205.2.3.9 Identification of NDI (e.g. COTS, GOTS, REUSE Software, GFE, etc) associated with the hazard.

205.2.3.9.1 Evaluation of NDI to determine if usage is different from what the NTI was originally designed for.

Commented [PDANUAA599]: 54-11
See 51-12

Commented [PDANUAA600]: 54-14
Old 204.2.b(2)
Generic reference needed as an explicit list will be too burdensome. Also, such a list is common across all 2XX Tasks. FUTURE ACTION ➔ Expand Appendix to discuss specific considerations.

205.2.3.9.2 Unless otherwise approved by the government, hazard analyses shall be limited to NDI inputs, outputs, and other interfaces. Details internal to the NDI shall be treated as a "black box".

205.2.3.10 Identification of Control Loop impacts

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

Commented [PDANUAA601]: Was 882E 205.2.1.c 54-15

54-15: FUTURE ACTION: Move 205.2.3.11 to appendix. These are all system-related causal factors

205.2.3.12 Subsystem/component degradation impacts on the system

205.2.4 **Assess Hazard risk level:** The contractor shall develop:

205.2.4.1 An initial assessment of the system risk of the current system without consideration of additional controls.

205.2.4.2 Maintain a current risk assessment of the system risk accounting for all of the hazard controls that have been implemented.

205.2.4.3 Project an end state risk assessment of the system risk accounting for all planned and implemented hazard controls.

205.2.4.4 The definitions in Table I shall be used to characterize system hazard severity.

205.2.4.5 The definitions in Table II shall be used to characterize system hazard probability.

205.2.4.6 Table III shall be used to derive the respective subsystem HRIs of the hazard.

205.2.4.7 Ensure system-level hazards attributed to the subsystem are analyzed and adequate controls of the potential hazards are implemented in the design.

Commented [PDANUAA602]: Adapted from 204.2.1
51-16 This is a Task 205 (SHA) activity.

205.2.5 **Identification of Potential Hazard Control Methods:** The contractor shall identify potential subsystem and system hazard controls to lower the system safety risk to an acceptable level

205.2.5.1 The hazard controls shall be follow the system safety order precedence as defined in paragraph 4.3.4.1.

205.2.6 **System Hazard Documentation:** The contractor shall document each system hazard in the Hazard Tracking System (HTS)

205.2.6.1. The contractor shall develop a system description to include:

a. System physical characteristics,
b. Software associated with the system
c. System functionality
d. System interfaces and associated input/output data
e. System boundaries
f. System control loops,
g. Expected system operating environment,
h. System operating and maintenance modes.
i. NDI components

205.2.6.2 The contractor shall document each applicable system hazard per the Hazard Tracking System (HTS).

205.2.6.3 The contractor shall maintain the currency and correctness of the SHA. This would include anomalies, changes to the system, changes to functionality, etc.

205.2.6.4 The contractor shall describe hazard analyses methods and techniques employed in the subsystem analyses.

205.2.6.5 The contractor shall describe LOR activities (per para 4.4) activities applicable to the subsystem.

205.2.6.5.1 Reference to more detailed system and subsystem descriptions, including specifications and detailed review documentation, shall be supplied when such documentation is available.

52-4

- Should analysis limitations, such as those introduced by NDIs, be identified?
- Should subsystem input/output data be summarized?

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

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

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

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

~~d. Degradation of a subsystem or the total system.~~

Commented [PDANUAA603]: Was 882E para 204.2.5.a

Commented [PDANUAA604]: Was 882E para 204.2.5.c

Commented [PDANUAA605]: Was 882E para 204.2.5.b Reworded

Commented [PDANUAA606]: 52-4 Was 882E para 204.2.5.a

Commented [PDANUAA607]: FUTURE ACTION: Move to new Task

Commented [PDANUAA608]: Move to 205.2.2

Commented [PDANUAA609]: Moved intent to 205.2.1.7 See 54-10

Commented [PDANUAA610]: FUTURE ACTION: Move to appendix. These are causal factors.

~~e. Design changes that affect subsystems.~~

~~f. Effects of human errors.~~

~~g. Determination:~~

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

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

Commented [PDANUAA611]: Moved to 205.2.1.2

Commented [PDANUAA612]: FUTURE ACTION: Move to appendix. These are causal factors.

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

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

205.2.3 When software to be used within the system is being developed under a separate software development effort, the contractor performing the SHA shall monitor, obtain, and use the output of each phase of the formal software development process in evaluating the software contribution to the SHA. Hazards identified that require mitigation action by the software developer shall be reported to the PM in order to request appropriate direction be provided to the software developers.

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

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

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

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

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

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

a. Imposition of Task 205. (R)

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

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

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

Commented [PDANUAA613]: Moved to 205.2.1.3
See 54-6

Commented [PDANUAA614]: Moved to 205.2.1.4.1 & 205.2.2.2
See 54-11

Commented [PDANUAA615]: Moved to 205.2.1.6 & 205.2.6

Commented [PDANUAA616]: Moved to 205.2.6

Commented [PDANUAA617]: Moved to 205.2.6.1

Commented [PDANUAA618]: Moved to 205.2.6.4

Commented [PDANUAA619]: Moved to 205.2.6.2

Commented [PDANUAA620]: Deleted. See 102.3

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

~~f. Concept of operations.~~

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

205.3 HTS Fields: The following fields shall be incorporated into the HTS. Additional HTS fields may be added as necessary.

a. Unique Hazard Tracking identifier for each hazard
b. Hazard Description
c. Hazard Causal Factors
d. Hazard Effects
e. Hazard Location
f. Hazard Phase
g. Hazard Mode
h. Associated Functions
i. Hazard Probability
j. Hazard Severity
k. Initial HRI
l. Current HRI
m. End-state HRI
n. Potential control measures (aka mitigation or amelioration methods)
o. Hazard Status
p. Hazard control validation/verification
q. Software in or interfacing with the Subsystem (definitive reference to the portion of the software that relates to the hazard)
r. Mode(s) of subsystem operation
s. Interfaces to other subsystems
t. Link to related hazards
u. Control Loop(s) affected

Commented [PDANUAA621]: Each 2XX Tasks has a different set of HTS Fields pertinent to that analyses. As such, required HTS fields include those identified in para 4.3.1.5 (See 46-4; 52-3)

FUTURE ACTION: Review 4.3.1.5 and all 2XX.3 HTS Fields eliminate duplications.

TASK 206
OPERATING AND SUPPORT HAZARD ANALYSIS

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

206.1 Purpose. Task 206 is to perform, document, and maintain an Operating and Support Hazard Analysis (O&SHA) to:

a. Identify hazards introduced by operational and support activities and procedures

57-01: Support activities is usually understood as routine maintenance activities at the local level. This could also be inferred to as "Heavy Maintenance" activities at the depot level. By its nature Heavy Maintenance introduces additional concerns – though limited to the heavy maintenance/depot environment.
This task needs to be revised to clarify the different types of support the O&SHA should cover. This will drive a difference in scope for operational support vs heavy maintenance/depot support. However, the specific task requirements should be the same between these activities.
For example – the TOs used in the operational setting will likely be different than the TOs used in the heavy maintenance/depot setting. However, safety analyses of the respective TOs will look the same for a Task perspective.
Purpose needs to reflect government interest is protecting government resources (i.e. personnel & material).

b. Characterize hazards introduced by operational and support activities and procedures
c. Assess initial/current risks
d. Identify potential control measures
e. Evaluate the adequacy of operational and support procedures, facilities, processes, and equipment ~~used to control risks associated with identified hazards.~~
f. Document hazard analyses in the Hazard Tracking System (HTS)

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

206.2 Task description: The contractor shall perform, document, and maintain an O&SHA to identify hazards, characterize hazards, assess safety risk, identify control measures, and verify implementation of control measures of identified O&SHA hazards. The O&SHA builds on system design hazard analyses focusing on the human-system interface for different modes of operation and maintenance.

Commented [PDANUAA622]: New format to increase readability
Added maintenance of SRHA to keep relevant over life cycle

Commented [PDANUAA623]: 57-01

Commented [PDANUAA624]: 57-02
Delete per redline
Evaluation of these areas is essentially what is being done as part of the hazard identification process. Limiting this evaluation to ONLY those areas associated with controlling risks artificially constrains safety analyses and suggests that certain areas do not have hazards where they may.

Commented [PDANUAA625]: 57-03
Contented adjusted to better align with task

Commented [PDANUAA626]: 57-04
FUUTRE ACTION: Move this thought to the appendix.
It is good information, but is not a direct requirement. As such, it does not belong in the task, but could be included in additional information provided in the appendix..

~~206.2.1 The O&SHA considers the following:~~

~~a. Planned system configuration(s)~~
~~b. Facility/installation interfaces to the system~~
~~c. Planned operation and support environments~~
~~d. Supporting tools or other equipment~~
~~e. Operating and support procedures~~
~~f. Task sequence, concurrent task effects, and limitations~~
~~g. Human factors, regulatory, or contractually specified personnel requirements~~
~~h. Potential for unplanned events, including hazards introduced by human errors~~
~~i. Past evaluations of related legacy systems and their support operations~~

206.2.1 **O&SHA Scope:**

206.2.1.1 This analyses shall include NDI (to incude COTS, GOTS, GFE, etc.).

206.2.1.1.1 NDI shall be treated as "Black Boxes" in the analyses unless (1) sufficient design details are available to analyze appropriately and (2) government approval for analyses on the NDI has been granted. In other words, hazard analyses shall be limited to NDI inputs, outputs, and other interfaces.

206.2.1.1.2 If COTS, GOTS, GFE, and NDI are used in an environment or manner other than originally designed for, and detail analyses has not been accomplished for the expanded environment, then the expanded operating environment shall be documented in the hazard analyses as an "Assumption that such expansion has not introduced additional hazards".

206.2.1.2 Software associated with a subsystem shall be clearly identified so that future references to aspects of the software supporting subsystem are unambiguous.

206.2.1.3 The contractor shall obtain PM approval of hazard analyses techniques to be used before performing the analysis.

206.2.1.4 When software to be used in conjunction with the system, the contractor performing the SSHA shall monitor, obtain, and integrate the output of each phase of the software development process in evaluating the software contribution to the SSHA.

57-8: What about software used in maintenance tools/infrastructure used to support the system? (depot likely to have different set with different concerns than line maintenance) What about organically maintained software (depot environment)?

In maintenance, often parts of the system are removed or disabled. In addition, simulators/emulators may be employed. How does the software function in his partially energized system environment – especially when key inputs may be lacking?

206.2.1.4.1 The contractor shall coordinate with the PM hazard control actions involving software development.

Commented [PDANUAA627]: 57-5
Reformat to align with common format of other 2XX Tasks
a ➔ 206.2.1.7.h
b ➔206.2.1.7.j
c ➔ 206.2.1.7.k
d ➔ 206.2.1.7.r
e ➔206.2.1.7.L
f ➔206.2.1.7.m
g ➔ 206.2.1.7.n, 206.2.1.7.o
h➔ 206.2.1.7.q
i ➔address in appendix

Commented [PDANUAA628]: 57-6
See 51-9
Common language to address NDI in 2XX Tasks

Commented [PDANUAA629]: 57-7
See 52-1

Commented [PDANUAA630]: 57-8

Commented [PDANUAA631]: 57-9
See 51-16
For software needed to sustain the system or software in equipment used to maintain/service the system

206.2.1.5 The contractor shall updated, as necessary, the O&SHA following system design changes and changes to support equipment. This shall include associated software changes.

206.2.1.6 The contractor shall re-evaluate the system and associated support equipment if the respective operating/support environments change.

206.2.1.7 Additional areas to consider include, but not limited to,

a. performance,
b. performance degradation,
c. functional failures,
d. timing errors,
e. design errors,
f. defects,
g. inadvertent functioning,
h. different system configurations or variants,
i. different modes/phases of operation
j. facility/installation interfaces to the system
k. planned operation and support environments
l. operating and support procedures to include warnings, cautions, and special emergency procedures
m. task sequence, concurrent task effects, and limitations
n. human-system interface
o. regulatory or contractually specified personnel requirements
p. system interactions with support equipment.
q. System resiliency to unplanned inputs/events
r. Incorporation of system/facility/installation/tooling/support equipment/test equipment changes/modifications to functional or design requirements
s. PPE requirements and limitations
t. Packaging, handling, storage, transportation and disposal of system, components, materials, etc
u. Training

206.2.1.8 While conducting this analysis, the human shall be considered a component in the maintenance/support of the system, receiving both inputs and initiating outputs.

206.2.2 **Hazard Identification:** The contractor shall apply systematic hazard analyses techniques to identify new safety hazards or impacts to existing hazards to the system, interfaces, control laws, functions, and other software interacting with the system and associated support equipment.

206.2.2.1 The contractor shall obtain government approval of hazard analyses techniques to be used before performing the hazard analyses.

206.2.2.2 As necessary, the contractor shall incorporate supporting subsystem component data for hazard analyses developed by associate contract agreements, government organically developed items, and/or NDI sources.

Commented [PDANUAA632]: 57-10
See 51-17

Commented [PDANUAA633]: 57-11
See 51-18
New requirement to address guidance gap.

Commented [PDANUAA634]: 57-12
See 51-11
Between the 2XX tasks, there needs to be a clear & concise means to summarize what should be considered.
FUTURE ACTION: Scrub this list and move common topics with other 2XX tasks to appendix

Commented [PDANUAA635]: Accounts for distributed development of subsystem components. This can be either HW or SW.
See 51-12

206.2.3 **Hazard Characterization:** The contractor shall use the best available data to characterize each operating and support hazard by applying paragraph 4 methodology to include, but not limited to:

206.2.3.1 Name of subsystem

206.2.3.2 Hazard Description

206.2.3.3 Hazard Causal Factors to include hardware, software, human involvement, and environmental considerations.

206.2.3.4 Hazard Effects

206.2.3.5 Proposed hazard controls (e.g. mitigation or amelioration measures)

206.2.3.6 Identification of where in the system the hazard exists. e.g. hardware components, what "unit" of software, etc.

206.2.3.6.1 Software "units" shall include the corresponding SWCI and AICI levels

206.2.3.6.2 Emergency systems shall focus on preserving the function for when needed during an emergency.

206.2.3.7 Identification of when the hazard asserts itself. e.g. phase of operation or maintenance, mode of operation or maintenance, etc

206.2.3.7.1 Identification of test unique aspects of the hazard.

206.2.3.8 Identification of interfaces between subsystems, hardware, software "units', human, support equipment and SOS where applicable

206.2.3.8.1 Software contributions shall include software developed by other sources.

206.2.3.9 Identification of functions impacted by the hazard

206.2..3.10 Identification of Control Loop impacts

206.2.4 **Assess Hazard risk level:**

206.2.4.1 The contractor shall develop:

206.2.4.1.1 An initial assessment of the subsystem risk of the current system without consideration of additional controls.

206.2.4.1.2 Maintain a current risk assessment of the subsystem risk accounting for all of the hazard controls that have been implemented

206.2.4.1.3 Project an end state risk assessment of the subsystem risk accounting for all planned and implemented hazard controls.

206.2.4.2 The definitions in Table I shall be used to characterize subsystem hazard severity.

206.2.4.3 The definitions in Table II shall be used to characterize subsystem hazard probability.

206.2.4.4 Table III shall be used to derive the respective subsystem HRIs of the hazard**.**

206.2.5 **Identification of Potential Hazard Control Methods:** The contractor shall identify potential operating and support hazard controls and associated requirements to lower the system safety risk to an acceptable level

206.2.5.1 The hazard controls shall be follow the system safety order precedence (paragraph 4.3.4.1) to control system, facility, tooling, etc. related O&SHA hazards.

206.2.5.2 Control methods utilizing Personal Protective Equipment (PPE) shall explicitly document the PPE limitations.

206.2.5.3 Control methods utilizing packaging, handling, storage, and transportation shall be documented.

206.2.5.4 Control methods utilizing packaging, handling, storage, transportation, and disposal of Hazardous Materials (HAZMAT) and hazardous wastes shall be documented.

206.2.6 **Operating & Support Hazard Documentation:** The contractor shall document each subsystem hazard in the Hazard Tracking System (HTS)

206.2.6.1 The contractor shall maintain the currency and correctness of the O&SHA. This would include anomalies, changes to the system impacting the subsystem, changes to the subsystem, etc.

206.2.6.2 Subsystem and system description to address physical and functional characteristics. Reference to more detailed system and subsystem descriptions, specifications, and detailed review documentation, shall be provided when available. (discussion can be documented in a separate location & referenced in the HTS)

206.2.6.3 Subsystem and system descriptions shall account for maintenance modes and activities.

206.2.6.4 The contractor shall account for all hazard analyses methods and techniques employed in conducting the O&SHA. A brief description of each methods and technique employed shall be included in the O&SHA documentation.

206.3 **HTS Fields:** The following fields shall be incorporated into the HTS. Additional HTS fields may be added as necessary.

a. Unique Hazard Tracking identifier for each hazard
b. Hazard Description
c. Hazard Causal Factors
d. Hazard Effects
e. Hazard Phase
f. Hazard Mode
g. Associated Functions
h. Hazard Probability
i. Hazard Severity
j. Initial HRI
k. Current HRI
l. End-state HRI
m. Potential control measures (aka mitigation or amelioration methods)
n. Hazard Status
o. Hazard control validation/verification
p. Software in or interfacing with the Subsystem (definitive reference to the portion of the software that relates to the hazard)
q. Mode(s) of subsystem operation
r. Interfaces to other subsystems
s. Link to related hazards
t. Control Loop(s) affected
u. Applicable warnings, cautions, and procedure references required to control specific hazard

~~206.2.6 At a minimum, the analysis shall identify:~~

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

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

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

Commented [PDANUAA636]: Each 2XX Tasks has a different set of HTS Fields pertinent to that analyses. As such, required HTS fields include those identified in para 4.3.1.5 (See 46-4; 52-3)

FUTURE ACTION: Review 4.3.1.5 and all 2XX.3 HTS Fields eliminate duplications.

Commented [PDANUAA637]: Intent captured in 206.2.3 Hazard characterization & 206.2.5 ID potential hazard control methods

Commented [PDANUAA638]: incorporated into 206.2.5 Task Description. Maintaining O&SHA includes accounting for any changes to the system or maintenance/support methods employed

Commented [PDANUAA639]: intent captured in 206.2.5.ID of potential hazard control methods. ID of these methods drive derived requirements.

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

e. Warnings, cautions, and special emergency procedures.

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

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

h. Training requirements.

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

j. Potentially hazardous system modes under operator control.

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

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

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

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

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

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

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

Commented [PDANUAA640]: Addressed in 206.2.5.2

Commented [PDANUAA641]: 206.2.5 discusses ID potential hazard control methods. Warnings, cautions, and emergency procedures are covered under the design order of precedent as noted in 206.2.5.1.

Commented [PDANUAA642]: Addressed in 206.2.5.3

Commented [PDANUAA643]: Addressed in 206.2.5.4

Commented [PDANUAA644]: 206.2.5 discusses ID potential hazard control methods. Training is covered under the design order of precedent as noted in 206.2.5.1.

Commented [PDANUAA645]: Addressed in 206.2.1.1; 206.2.1.1.1; & 206.2.1.1.2

Commented [PDANUAA646]: Addressed in 206.2.1.7.i

Commented [PDANUAA647]: FUTURE ACTION: Move appendix as it is not a hard requirement.
Note 206.2.1.7 is not an inclusive list; intent is to move common hazard sources to a common discussion in the appendix.

Commented [PDANUAA648]: Addressed in 206.2.2.1

Commented [PDANUAA649]: Addressed in 206.1 & 206.2 – maintenance of the O&SHA

Commented [PDANUAA650]: Addressed in 206.2.6

Commented [PDANUAA651]: Addressed in 206.2.6.2

Commented [PDANUAA652]: Addressed in 206.2.2.1 & 206.2.6.4

Commented [PDANUAA653]: Addressed in 206.2.6.2 & 206.3

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

~~a. Imposition of Task 206. (R)~~
~~b. Identification of functional discipline(s) to be addressed by this task. (R)~~
~~c. Minimum reporting requirements. (R)~~
~~d. Desired analysis methodologies and technique(s) and any special data elements, format, or data reporting requirements (consider Task 106, Hazard Tracking System).~~
~~e. Selected hazards, hazardous areas, or other specific items to be examined or excluded.~~
~~f. COTS, GOTS, NDI, and GFE technical data to enable the contractor to accomplish the defined task.~~
~~g. Legacy and related processes and equipment and associated hazard analyses to be reviewed.~~
~~h. How information reported in this task will be correlated with tasks and analyses that may provide related information, such as Task 207 (Health Hazard Analysis).~~
~~i. Concept of operations.~~
~~j. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.~~

Commented [PDANUAA654]: Deleted. See 102.3

TASK 207
HEALTH HAZARD ~~ANALYSIS~~ ASSESSMENT

60-1 Title change reflects designs are assessed to determine corresponding hazards. Yet, one could also argue analyses of the design is accomplished by applying hazard analyses techniques. Which is title is more correct?

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

207.1 Purpose. Task 207 is to perform, document, and maintain a Health Hazard Assessment (HHA) to

a. identify human health hazards,
b. characterize health hazards
c. assess initial/current risks
d. identify potential corrective actions (aka mitigation & amelioration)
e. document health hazards in the Hazard Tracking System (HTS)

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

207.2 Task Description: The contractor shall perform, document, and maintain an HHA to identify health hazards, characterize health hazards, assess health risk, and identify health hazard control measures~~, and verify implementation of health hazard control measures~~.

60-2 Change **Contractor** to **Assessor?**
Pro: broadened the proponent of the task to "assessor" rather than "contractor" because government (e.g., APHC) also perform HHAs
Con: Construct of MIL-STD-882 is written from the perspective that 882 will be placed on a contract; requirements are written in terms for a contractor to implement.

60-7 Already required (see system safety process Element 6 – para 4.3.6) Move Verification to new task? Is so, FUTURE ACTION

Commented [PDANUAA655]: 60-1

Commented [PDANUAA656]: Reformatted and reworked.

Task split into Task 207 HHA
New Task 211 HAZMATHA

Commented [PDANUAA657]: Added maintenance of SRHA to keep relevant over life cycle

Commented [PDANUAA658]: Reformatted into/rework
207.2.1.1
207.2.1.2.
207.2.1.3
207.2.1.4
207.2.1.5

NOTE: HAZMAT and ergonomic aspects are addressed in Tasks 212 and 211 respectively.

Commented [PDANUAA659]: See 60-2

Commented [PDANUAA660]: Communication of hazards?
Deleted here – see 60.5
(NOTE this would also apply to all of the 2xx tasks)

Commented [PDANUAA661]: 60-7

207.2.1 **HHA Scope:** A health hazard is a condition, inherent to the operation, maintenance, storage, and transportation of material that can cause personnel death, injury, acute or chronic illness, disability, or reduced job performance by exposure to physiological stressors (physical, chemical, or biological).

207.2.1.1 Specific health hazards shall consider:

207.2.1.1.1 Evaluation of hazards for potential acute or chronic health effects.

207.2.1.1.2 Evaluation of the total health impact of all stressors to operators, maintainers, passengers, and other personnel that may be exposed to a hazard.

207.2.1.1.4 Evaluation of physical, chemical, and/or biological material characteristics, quantities, or concentrations for organism or offspring health effects.

207.2.1.1.5 Evaluation of physical, chemical, and/or biological material characteristics quantities, or concentrations for potential to cause substantial present or future danger to the environment.

207.2.1.1.6 Evaluation of potential health effects resulting from exposures to health hazards during normal use.

207.2.1.1.3 Synergetic effects of all agents present.

207.2.1.1.7. Health hazards associated with NDI

207.2.1.1.7.1. NDI shall be treated as "Black Boxes" in the analyses unless (1) sufficient design details are available to analyze appropriately and (2) government approval for analyses on the NDI has been granted.

207.2.1.1.7.2 If NDI are used in an environment or manner other than originally designed for, and detail analyses has not been accomplished for the expanded environment, then the expanded operating environment shall be documented in the hazard analyses as an *"Assumption that such expansion has not introduced additional hazards"*.

207.2.2 System software shall be clearly identified so that future references to aspects of the software supporting subsystem are unambiguous.

207.2.3 Additional areas to consider include, but not limited to, include performance, performance degradation, functional failures, timing errors, design errors, defects, and inadvertent functioning.

207.2.4 While conducting the HHA, the human shall be considered a component within the system, receiving both inputs and initiating outputs.

Commented [PDANUAA662]: Defining what a health hazard is

Commented [PDANUAA663]: NOTE: NDI defined in para 3.2.24 and discussed in 4.5.1 as including COTS, GOTS, GFE, etc.
NDI may impact some health hazard categories but not others. (NDI discussion has been included in each of the hazard analyses tasks for standardization)

207.2.5 HHAs should consider biomedical knowledge and principles to document the total health impact of all operator and maintainer exposures to health hazards during normal use.

Commented [PDANUAA664]: 60-3

Commented [PDANUAA665]: 60-4

60-3 Linking HHA to biomedical knowledge/principles is desirable. Should "Should" be change to "Shall"?
Keep "Should" ➔ allows trained system safety to identify health related issues without formal biomedical training. (Is there a need to define "minimal" biomedical training requirements?)
Change to "Shall" ➔ strengthens HHA hazard credibility by ensuring health hazards are rooted in biomedical knowledge/principles. However, this would introduce additional credential requirements for individuals conducting/reviewing HHAs.

60-4 Agreed health hazards need to address normal use. Should there also be an avenue to investigate health hazards resulting in projected emergency situations? For example, if a system is prone to catching fire, byproducts from the fire could introduce health hazards that need to be considered – especially from a first responder perspective.
How should this aspect be addressed? In a new Task?

60-5 The concept of "Communication of Health Hazards" is an unique aspect/term of Health Hazards. Inferred in this term is the how the hazard is transmitted from the system, workplace, or operational environment to the human.
How should this concept be incorporated without introducing confusion/conflict with existing terminology used?
In essence, this is addressing how a hazard causal factor (e.g. hardware, software, human, or environmental) is transmitted/realized in a system/operator.

207.2.2 **Hazard Identification:** A health hazard is a condition, inherent to the operation, maintenance, storage, transport, use of materiel, or disposal, that can cause death, injury, acute or chronic illness, disability, or reduced job performance of personnel by exposure to physiological stresses.

207.2.2.1 The contractor shall apply systematic hazard analyses techniques to identify new safety hazards or impacts to existing hazards involving health hazard.

207.2.2.2 The contractor shall obtain government approval of hazard analyses techniques to be used before performing the hazard analyses.

207.2.2.3 As necessary, the contractor shall incorporate supporting subsystem component data for hazard analyses through associate contract agreements and/or government organically developed items.

Commented [PDANUAA666]: 60-6

60-6 Intent of para 207.2.2.3: If a different group is developing a portion or impacting a subsystem, the safety analyses needs to account for those relevant details
This can be either HW or SW; in either case, health hazards may be introduced

207.2.2.4 Specific health hazards shall include, but are not limited to:

Commented [PDANUAA667]: Reworded to simplify references in a more structured presentation while being more comprehensive.

HAZMAT references being moved to new Task 211

207.2.2.4.1 Acoustical energy (e.g., steady-state noise, impulse noise, blast overpressure, ultrasonic noise)

207.2.2.4.2 Biological substances (e.g., sanitation, pathogenic microorganisms such as bacteria, viruses, fungi, and mold)

207.2.2.4.3 Chemical hazards (e.g., materials that irritate or are hazardous because of physical properties such as weapon combustion products, fuel combustion products, toxic materials, nanomaterials, ototoxins)

207.2.2.4.5 Mechanical Shock (e.g., acceleration, deceleration, recoil)

207.2.2.4.5 Musculoskeletal Trauma (e.g., ergonomics, muscular exertions, lifting, load carriage, head-supported mass)

207.2.2.4.6 Oxygen deficiency (e.g., ventilation, high altitude, subterranean environments, confined spaces)

207.2.2.4.7 Radiation energy (e.g. ionizing radiation, radio frequency radiation, laser and optical radiation, non-ionizing radiation).

207.2.2.4.8 Temperature Extremes (e.g., heat stress, cold stress, humidity)

207.2.2.4.9 Vibration (e.g., whole-body, segmental, multiple shock)

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

~~207.2.3 A health hazard is a condition, inherent to the operation, maintenance, storage, transport, use of materiel, or disposal, that can cause death, injury, acute or chronic illness, disability, or reduced job performance of personnel by exposure to physiological stresses. Specific health hazards and impacts that shall be considered include:~~

Commented [PDANUAA668]: Moved to 207.2.2

~~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).~~

Commented [PDANUAA669]: Moved to 207.2.2.4.3

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

Commented [PDANUAA670]: Moved to 207.2.2.4.1, 207.2.2.4.5, 207.2.2.4.8, 207.2.2.4.9,

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

Commented [PDANUAA671]: Moved to 207.2.2.4.2

~~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.).~~

Commented [PDANUAA672]: Moved to 207.2.2.4.5

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

Commented [PDANUAA673]: Moved to 207.2.2.4.10

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

Commented [PDANUAA674]: Moved to 207.2.2.4.7, 207.2.2.4.7.1

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

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

~~207.2.2 The HHA shall provide the following categories of information:~~

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

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

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

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

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

207.2.3 **Hazard Characterization:** The contractor shall use the best available data to characterize each health hazard by applying paragraph 4 methodology to include, but not limited to:

207.2.3.1 Where or when in the system does the health hazard exist?

Commented [PDANUAA675]: Moved to 207.2.2.4.6

Commented [PDANUAA676]: Moved to 207.2.3.2

Commented [PDANUAA677]: Moved to 207.2.3.2.1

Commented [PDANUAA678]: Moved to 207.2.3.2.2

Commented [PDANUAA679]: Moved to 207.2.4.4, 207.2.4.5, 207.2.4.6

Commented [PDANUAA680]: Moved to 207.2.5.2

207.2.3.2 Hazard Description. The contractor shall determine the aspect(s) of the operator's/maintainer's health affected by the hazard.

Alternate Wording to 207.2.3.2: The contractor shall anticipate, recognize, and identify the potential health hazards or hazardous conditions inherent to the system, workplace, or operating environment. Identify the sources associated with the health hazards.

207.2.3.2.1 The contractor shall describe the exposure pathway(s) ~~conditions and mode by~~ which a hazardous agent can come in contact with a living organism. Include a description of the means ~~mode~~ by which the agent is transmitted to the organism (e.g., ingestion, inhalation, absorption, or other means ~~mode~~ of contact), as well as evidence of environmental fate and transport. Consider components of the system which may come into contact with users.

Commented [PDANUAA681]: To preclude confusion over the usage of "mode" (aka different operating modes, display modes, etc), verbiage changed to Means

Alternate Wording to 207.2.3.2.1: Exposure description. The contractor shall describe the conditions and pathway by which a health hazard may affect operators or maintainers during normal use. Include qualitative and quantitative information on the presence and magnitude of the health hazards, routes of exposure (e.g., ingestion, inhalation, absorption, or other mode of contact), duration of exposure, frequency of exposure, and population at risk. Describe the purpose of the system and the mission scenarios in which the system will be used. If known, include manpower estimates that will be allocated toward operating and maintaining the system.

207.2.3.2.2 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. -

Alternate Wording to 207.2.3.2.2: Exposure characterization. The contractor shall characterize the exposure using physiological dose-response relationships, potential health effects (acute and chronic), and health protection criteria. As available and deemed practical, use Department of Defense (DOD) and other governmental (Federal, state, and local) criteria and standards to assess health hazards. Provide either a description of the assessment process or the name of the assessment tool or model used.

Commented [PDANUAA682]: This term/concept will need to be defined – or a reference to where it is defined.

207.2.3.3 Hazard Causal Factors to include hardware, software, human involvement, and environmental considerations. Environmental considerations would include, but not limited to, triggers for physical hazards, biological hazards, ergonomic hazards, hazardous material exposure, non-ionizing radiation exposure, and ionizing radiation exposure.

207.2.3.4 Hazard Effects to include immediate effects as well as long term effects.

207.2.3.5 Proposed hazard controls (e.g. mitigation or amelioration measures)

207.2.3.6 Identification of where in the system or when the hazard exists (e.g. hardware components, what "unit" of software, etc.)

207.2.3.6.1 Software "units" shall include the corresponding SWCI and AICI levels

207.2.3.6.2 Emergency systems shall focus on preserving the function for when needed during an emergency.

207.2.3.7 Identification of when the hazard asserts itself. (e.g. phase of operation or maintenance, mode of operation or maintenance, etc.)

207.2.3.7.1 Identification of test unique aspects of the hazard.

207.2.3.8 Identification of interfaces between subsystems, hardware, software "units', human, support equipment and SOS where applicable

207.2.3.8.1 Software contributions shall include software developed by other sources.

207.2.3.9 Identification of functions impacted by the hazard

207.2.3.10 Identification of NDI associated with the hazard.

207.2.3.10.1 Evaluation of NDI to determine if usage is different from what the NTI was originally designed for.

207.2.3.10.2 Unless otherwise approved by the government, hazard analyses shall be limited to NDI inputs, outputs, and other interfaces. Details internal to the NDI shall be treated as a "black box".

207.2.3.11 Hazard Phase: When does the health hazard present itself? Note that different exposure probabilities may exist based on phase of operation.

207.2.3.12 Hazard Mode: When does the health hazard present itself? Note that different exposure probabilities may exist based on mode of operation.

207.2.3.13 Health Hazard Agent: What is the source of the health hazard? This could be chemical, physical, biological, ergonomic, different forms of radiation (e.g. ionizing, non-ionizing)

207.2.3.14 Identification of Control Loop impacts

207.2.3.15 The HHA shall utilize and reference system information, test data, and specifications in order to assess each identified health hazard. Ensure test conditions were established with consideration of all relevant exposure and mission scenario information required in 207.2.2. Specific information and considerations may be required to assess each health hazard, such as:

207.2.3.15.1 Acoustic energy. The contractor shall identify and categorize main noise sources.

207.2.3.15.1.1 As applicable, the contractor shall include steady-state noise, impulse noise, and blast overpressure measurements collected at all occupied positions.

Commented [PDANUAA683]: Added material to focus on the "how" of providing information in the HHA; Laying out the content expectations of what is needed for each type of health hazard

207.2.3.15.1.2 For systems producing steady-state noise, the contractor shall analyze the octave bands, overall sound pressure level, A-weighted decibel level, time-weighted average, and contour distance.

207.2.3.15.1.3 For systems producing impulse noise, the contractor shall analyze the peak pressure level, A-duration, B-duration, and contour distance.

207.2.3.15.1.4 The contractor shall consider the effectiveness and attenuation of hearing protection to prevent auditory injuries.

207.2.3.15.1.5 The contractor shall evaluate the blast overpressure and time-pressure changes associated with weapons firing.

207.2.3.15.2 Biological substances. The contractor shall include design descriptions for systems where biological substances are likely to present a hazard (e.g., food handling, hazardous waste and wastewater, medical/healthcare, ambulatory, mortuary affairs).

207.2.3.15.2.1 The contractor shall identify controls in place (e.g., non-porous materials, work practices, cleaning procedures, personal protective equipment) to eliminate or control occupational exposures to hazardous biological substances.

207.2.3.15.3 Chemical substances. The contractor shall identify the quantity, characteristics, and concentrations of hazardous chemicals created by or routinely used in the system (e.g., fuel and weapon combustion products, toxic materials, nanomaterials).

Commented [PDANUAA684]: HAZMAT to be captured in Tasks 108 and new 211

207.2.3.15.3.1 The contractor shall characterize routine, prolonged exposures and exposures inherent to operations.

207.2.3.15.3.2 The contractor shall use source documents, such as Safety Data Sheets (SDSs), toxicity clearances, and test data measurements.

207.2.3.15.3.3 The contractor shall consider accumulation of substances over time, and compare exposures to all applicable occupational exposure limits (e.g., time-weighted average, ceiling, and short-term exposure).

207.2.3.15.3.4 The contractor shall consider additive effects and effects related to other health hazards (e.g., ototoxins and noise, asphyxiants and oxygen deficient environments).

207.2.3.15.4 Mechanical Shock. The contractor shall evaluate potential sources where mechanical impulses may be transmitted to an individual or body part by the acceleration or deceleration of an inertial force. *Examples include, but are not limited to, recoil from shoulder-fired weapons, deceleration from parachute deployment, and whole-body acceleration/deceleration of occupants of large mobile weapon systems.*

207.2.3.15.4.1 For shoulder-fired weapons, the contractor shall identify the recoil energy, recoil velocity, recoil impulse, force, and/or acceleration.

207.2.3.15.5 Musculoskeletal Trauma. The contractor shall identify the physical properties (e.g., weight, size) of all system components that personnel will manually handle or wear.

207.2.3.15.5.1 The contractor shall include a task analysis listing required non-neutral postures, load carrying, muscular exertions, repetitive motions, etc.

207.2.3.15.5.2 The contractor shall evaluate the possibility of reducing load and force requirements, adding material handling aids or tools, reducing non-neutral postures, reducing frequency of repeated motion, increasing the manpower allocation, or redistributing tasks among personnel manning the system.

207.2.3.15.6 Oxygen deficiency. The contractor shall identify the design and operation of occupied shelters, vehicles, and other enclosures.

207.2.3.15.6.1 The contractor shall evaluate associated ventilation test data (e.g., total fresh and recirculated airflow rates, enclosure volume, maximum number of occupants).

207.2.3.15.6.2 For maintenance-type shelters, the contractor shall ensure local exhaust ventilation requirements are met to eliminate airborne health hazards.

207.2.3.15.6.3 The contractor shall identify confined spaces and permit-required confined spaces.

207.2.3.15.6.4 The contractor shall consider human health effects of operations in high altitude, subterranean environments, and other oxygen deficient environments.

207.2.3.15.7 Radiation energy.

207.2.3.15.7.1 The contractor shall identify all ionizing radiation sources (including isotopes), quantities, and activities.

207.2.3.15.7.2 The contractor shall identify all radio frequency (RF) radiation sources, and evaluate both effects due to absorbed RF energy and RF shock and burn hazards.

207.2.3.15.7.3 The contractor shall include all RF radiation specifications (e.g., frequency, average power, antenna gain, duty factor).

Commented [PDANUAA685]: 61-1

61-1 Add RF Hazard Distance

207.2.3.15.7.4 The contractor shall identify all sources of laser and optical radiation, and evaluate the associated skin and eye hazards.

207.2.3.15.7.5 The contractor shall include all laser specifications (e.g., classification, wavelength, average and/or maximum power or energy, divergence, initial beam diameter, pulse information).

Commented [PDANUAA686]: 61-2

61-2 FUTURE ACTION: Add laser class, hazard distance.
Does "Directed Energy" need to be addressed?

207.2.3.15.8 Temperature Extremes. The contractor shall identify the expected climatic cycles of operational environments and describe the tasks required.

207.2.3.15.8.1 The contractor shall include all measurements associated with the heating and cooling performance of environmental control units (e.g., wet bulb globe temperature at head, chest, and feet locations of all occupant positions, simulated heat loads, time to reach steady-state temperature).

207.2.3.15.8.2 The contractor shall evaluate other sources of heat stress, such as Mission Oriented Protective Posture (MOPP) gear, that raise the internal body temperature.

207.2.3.15.9 Vibration. The contractor shall describe the operational environment conditions affecting whole-body vibration exposure (e.g., speed, terrain conditions, load conditions, seat locations).

207.2.3.15.9.1 The contractor shall identify sources of segmental vibration (e.g., hand-arm) and describe the tasks required.

207.2.3.15.9.2 The contractor shall nclude vibration data for all combinations of conditions.

207.2.4 **Assess Hazard risk level:**

207.2.4.1 The contractor shall develop:

207.2.4.1.1 An initial assessment of the health hazard risk of the current system without consideration of additional mitigations.

207.2.4.1.2 Maintain a current risk assessment of the health hazard risk accounting for all of the hazard controls that have been implemented.

207.2.4.1.3 Project an end state risk assessment of the health hazard risk accounting for all planned and implemented hazard controls.

207.2.4.2 Health hazard risks shall be evaluated in terms of a hazardous exposure producing a specific adverse health outcome.

207.2.4.3 System level health hazard risks should consider the synergistic, additive, and cumulative effects of all hazards present.

207.2.4.4 The definitions in Table I shall be used to characterize subsystem hazard severity.

207.2.4.5 The definitions in Table II shall be used to characterize subsystem hazard probability.

207.2.4.6 Table III shall be used to derive the respective subsystem **HRIs** of the hazard**.**

207.2.4.7 As appropriate for each hazard, describe the potential acute and chronic health risks (e.g., carcinogenicity, flammability, and reactivity).

207.2.5 **Identify Potential Corrective Action(s):** The contractor shall identify potential health hazard controls to lower the system safety risk to an acceptable level

207.2.5.1 The hazard controls shall be follow the system safety order precedence (paragraph 4.x)

207.2.5.2 The contractor shall recommend a mitigation strategy for each hazard.

207.2.5.2.1 The contractor shall identify the degree of risk reduction achievable by the each hazard control.

207.2.6 **HHA Documentation:** The contractor shall document each health hazard in the Hazard Tracking System (HTS)

207.2.6.1 The contractor shall maintain the currency and correctness of the HHA. This would include anomalies, changes to the system impacting the subsystem, changes to the subsystem, etc.

207.2.6.2 Subsystem and system description to address physical and functional characteristics. Reference to more detailed system and subsystem descriptions, sepcifications, and detailed review documentation, shall be provided when available. (discussion can be documented in a separate location & referenced in the HTS)

207.2.6.3 An HHA may include the medical costs avoided as a result of eliminating or controlling health hazards in order to compare to life cycle cost.

207.2.6.4 The contractor shall include a list of all source materials used in conducting the HHA. It may include Government and contractor reports, standards, criteria, test data, technical manuals, and specifications.

207.3 Hazard Tracking System HTS Fields: The following fields shall be incorporated into the HTS. Additional HTS fields may be added as necessary.

a. Unique Hazard Tracking identifier for each hazard
b. Hazard Description
c. Hazard Causal Factors

Commented [PDANUAA687]: Each 2XX Tasks has a different set of HTS Fields pertinent to that analyses. As such, required HTS fields include those identified in para 4.3.1.5 (See 46-4; 52-3)

FUTURE ACTION: Review 4.3.1.5 and all 2XX.3 HTS Fields eliminate duplications.

d. Hazard Effects
e. Hazard Phase:
f. Hazard Mode:
g. Health Hazard Agent:
h. Hazard Probability
i. Hazard Severity
j. Initial HRI
k. Current HRI
l. End-state HRI
m. Potential control measures (aka mitigation or amelioration methods)
n. Hazard Status
o. Hazard control validation/verification
p. Software in or interfacing with the Subsystem (definitive reference to the portion of the software that relates to the hazard)
q. Mode(s) of subsystem operation
r. Interfaces to other subsystems
s. Link to related hazards
t. Control Loop(s) affected
u. Applicable warnings, cautions, and procedure references required to control specific hazard
v. Governing standard/requirement for the health hazard. OSHA, NEPA, ANSI, etc

61-3 Add 207.4 to list pertinent citations (e.g. 207.3.i & subparas).

~~207.2.4 In addition to the information required in 207.2.2 above, the following sections describe the HHA or part of the HHA that provides Hazardous Material (HAZMAT) evaluation, ergonomics evaluation, or describes the operational environment.~~

~~207.2.4.15 The HHA or part of the HHA providing HAZMAT evaluation, in addition to the information required in 207.2.2 above, shall:~~

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

Commented [PDANUAA688]: Reformat; split between new tasks 207 & new 211

Commented [PDANUAA689]: See New Task 211

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

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

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

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

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

Commented [PDANUAA690]: See New Task 212

~~207.2.4.16 In addition to the information required in 207.2.2 above, the HHA or part of the HHA providing ergonomics evaluation shall:~~

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

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

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

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

Commented [PDANUAA691]: 207.2.6.3

a. ~~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~~.

Commented [PDANUAA692]: 207.2.6.4

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

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

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

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

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

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

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

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

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

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

Commented [PDANUAA693]: See Task 211

Commented [PDANUAA694]: The following paras have been incorporated into the revised 207.2 paras above.

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

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

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

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

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

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

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

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

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

d. Sources of information that will be made available and should be utilized.

e. Standards and criteria for acceptable exposures and controls.

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

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

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

(2) 29 CFR 1910.1200, OSHA Hazard Communication.

(3) DODI 6055.08, Occupational Ionizing Radiation Protection Program.

(4) DODI 6055.11, Protection of DOD Personnel from Electromagnetic Fields.

(5) DODI 6055.12, DOD Hearing Conservation Program.

(6) DODI 6055.15, DOD Laser Protection Program.

(7) DOD Handbook 743, Anthropometry of U.S. Military Personnel (Metric).

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

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

(10) MIL-STD-1472, DOD Design Criteria Standard for Human Engineering.

(11) MIL-STD-1474, DOD Design Criteria Limit Noise Limits.

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

(13) MIL-HDBK-828C, Laser Safety on Ranges and in Other Outdoors Areas.

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

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

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

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

Commented [PDANUAA695]: See 61-3

Commented [PDANUAA696]: This, and other "blue" citations were requested to be added.

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

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

(16) U.S. Army Public Health Center, Technical Guide 351, Health Hazard Assessor's Guide.

(17) U.S. Army Human Systems Integration (HSI) Program.

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

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

Commented [PDANUAA697]: Included documents/standards related to HHA, not related to each health hazard (or this list would be ridiculously long). DA Pam 40-501 removed.
This could be removed too since there's a DODI

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

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

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

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

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

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

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

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

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

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

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

(29) ANSI Z136.1-2014, Safe Use of Lasers.

(30) ANSI Z49.1, Safety in Welding, Cutting, and Allied Processes.

(31) International Electrotechnical Commission 60825-1:2014, Safety of laser products – Part 1: Equipment classification and requirements.

(32) Institute of Electrical and Electronics Engineers (IEEE) C95.1 and C95.6 Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 0 KHz to 300 GHz, IEEE Standards Coordinating Committee on Non-Ionizing Radiation Hazards.

Commented [PDANUAA698]: See above comment. There's a DODI for Hearing Conservation Programs.

Commented [PDANUAA699]: See previous comment. There's a DODI for RFR.

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

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

~~g. Concept of operations.~~

~~h. Projected manpower allocation in support of 207.2.2.~~

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

TASK 208
FUNCTIONAL HAZARD ANALYSIS

68-1 Change title to Functional Path Analyses.

Rationale: The output of this task is to provide a "map" of select functions in the design. This map would include both hardware and software contributions.

Documenting hazards are covered in para 4. In addition, other 2xx Tasks provide a more detailed hazard analyses guidance. To repeat the same in 208 would introduce profound confusion.

NOTE: Functional Thread Analyses (FTA) was considered but FTA could be confused with Fault Tree Analyses Therefore, **add a general statement to work any hazard per para 4 (to include logging into HTS).**

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

208.1 Purpose. Task 208 is to perform, document, and maintain a Functional Hazard Analysis (FHA) of an individual system or subsystem(s).

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

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

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

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

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

Commented [PDANUAA700]: 68-1

Commented [PDANUAA701]: Reformat
Realignment of task. See 68-1

Much of what is in the Purpose belongs (in a different form) in the Task Description

SRF term deleted as unneeded. A function may have SCI or SSI items. SCF term historically has been the term used (derived from Joint Services Software Safety Engineering Handbook – JSSSEH).

FUTURE ACTION: Documenting human interface with an SCF needs to be defined. Likewise System of Systems (SoS) interfaces need to be defined.

Commented [PDANUAA702]: Added maintenance of FHA to keep relevant over life cycle

Commented [PDANUAA703]: Reworked in new 208.2;

FUTURE ACTION: some content to be moved to appendix

Commented [PDANUAA704]: An adjustment to describing the task has been made to eliminate confusion and enhance focus of the task

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

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

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

208.2 Task Description: The contractor shall perform, document and maintain a FHA to analyze functions associated with the proposed design. The FHA should be based on the best available data and should include inputs, outputs, critical interfaces, and the consequence of functional failure.

208.2.1 **Function Identification:** The contractor shall identify and obtain government approval for the list of Safety Critical Functions (SCFs) to be analyses/assessed.

208.2.1.1 An SCF is a function within a system that has safety implications. Failure or loss of an SCF may reasonable be expected to result in loss of the system.

208.2.1.2 Each SCF shall have a unique identification assigned to it.

208.2.1.3 The unique SCF identifier shall be used by subsequent analyses.

208.2.1.4 Revisions to the SCF List shall obtain government approval.

208.2.1.5 A description of each SCF shall be developed to document the scope and purpose of the SCF within the design to include interfaces with subsystems, operators, and external sources.

208.2.2 **SCF Mapping:** The contractor shall identify and document all contributing hardware and software items that contribute to each SCF.

68-2 Citing particular portions of software to support this analyses is essential for Task 208 and subsequent 2XX Tasks.
FUTURE ACTION: Develop a means to provide precise software citations.
Perhaps citing the same software "units" that para 4.4 cites when assigning software control categories & corresponding SwCI level is the proper level?

Commented [PDANUAA705]: Task reworked to focus on
(1) ID SCF
(2) Mapping SCF into the design

The product of the task is to produce a listing of SCFs (i.e. which functions to map) and associated SCIs & SSIs.

To de-conflict with other hazard analyses tasks, hazard analyses activities have been moved to other 2XX Tasks. Namely, Task 205, SHA, but potentially other tasks as well.

Commented [PDANUAA706]: Requirements associated with developing a mutually recognized list of SCFs.

Commented [PDANUAA707]: These requirement outline how SCI and SSI items are defined.

68-2

208.2.2.1 An item with the potential for single point failures (SPF) that interrupt/fail an SCF shall be designated a Safety Critical Item (SCI).

68-3 Does the term SCI need to be changed? The important thing for this analyses is NOT the corresponding potential severity of the item, but rather the fact that the SCF could be interrupted.
Yet, there is a relationship that needs to be addressed. That is, failure of a SCF introduces the potential of loss of a system. When viewed from this perspective, SPF drives Safety Critical (**Catastrophic**/Critical) consequence. Focusing only on safety consequence without considering impacts to the function misses the point of Task 208.

208.2.2.2 Any item supporting a SCF other than a SCI shall be designated a Safety Significant Item (SSI).

208.2.2.3 Boundaries around an SCF shall be identified and documented. The SCF boundary defines the extent of where the SCF is mapped to. Examples include, but are not limited to:

a. Operator/maintainer interface with the SCF
b. Within software where no direct meaningful correlation with software unit inputs and the SCF.

208.2.2.4 Each SCI and SSI designation shall correspond to formal configuration nomenclature.

68-4: Early in a program, this is difficult as "names" of parts change. However, once the design baseline has been established, correlation of SCIs and SSIs with the formal part numbers/part names to ensure future traceability becomes possible.

- Is further guidance needed to address SCI and SSI designations BEFORE vs AFTER establishment of the design baseline?

See 68-2 for software, but both hardware and software are affected with this concern.

208.2.2.5 There shall be no "gaps" in the SCF map. In other words, there shall not be any undesignated items between an SCF's SCIs and SSIs.

208.2.2.5.1 A graphical representation depicting how all of a SCF's SCIs and SSIs may be helpful to (1) visually see the relationship between the different items (2) provide a means to check completeness of the list.

208.2.2.6 SCF interfaces, to include control loops, shall be identified.

68-5 FUTURE ACTION: Define the specifics needed to effectively define interfaces (to include control loops)

Commented [PDANUAA708]: 68-3

Commented [PDANUAA709]: This is a frequently overlooked aspect: Where in the design is the SCF map stopped (e.g. SCF boundary)? Unless this is documented, such decisions are quickly lost as the life cycle continues.

Commented [PDANUAA710]: 68-4

Commented [PDANUAA711]: A "gap" in the SCF map represents one or more items that have not been identified. Failure of unidentified SCF items may not be identified or significance understood (from a predictive perspective) and only be identified AFTER a mishap involving such components.

Commented [PDANUAA712]: 68-5

208.2.2.7 The contractor shall provide a pointer/linkage to hazards associated with each SCF. Such hazards involve hardware or software items associated with the SCF. In addition, for each identified hazard, the associated hazard effect degrades or interrupts the corresponding SCF.

208.2.2.8 The contractor shall maintain correctness of the SCF mapping over the contract period.

208.2.2.8.1 The FHA shall account for all changes and modifications.

208.2.2.8.2 The FHA shall account for all system configurations.

208.2.2.9 The FHA may be used to feed other processes, such as helping identify Aviation Critical Safety Items, airworthiness determination, driving hardware and software requirements, etc

208.3 FHA Tracking Fields

Commented [PDANUAA713]: 68-5

68-5 FUTURE ACTION: Define what is needed to track SCFs and associated SCIs/SSIs. Specifically, what fields are needed? (The HTS database is not appropriate since Task 208 is generating an SCF map, not identifying hazards.)

- Name of hardware item or portion of software code for each SCI/SSI
- Description of each SCF
- Boundaries for each SCF
- Interfaces (to include control loops) associated with each SCF

~~(208.2.1.f)~~

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

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

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

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

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

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

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

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

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

~~a. Imposition of Task 208. (R)~~

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

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

~~d. Applicable requirements, specifications, and standards.~~

Commented [PDANUAA714]: Para 4.4 is already invoked. Do not need to invoke a second time again.

Commented [PDANUAA715]: Value added? What will be done with this list (except used as an assurance tool)?

~~e. Concept of operations.~~

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

TASK 209
SYSTEM-OF-SYSTEMS HAZARD ANALYSIS

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

209.1 Purpose. Task 209 is to perform, document and maintain an analysis of the System-of-Systems (SoS) to identify unique SoS hazards.

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

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

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

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

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

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

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

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

209.2 Task description. The contractor shall perform, document and maintain an SoSHA to identify unique SoS hazards, characterize hazards, assess safety risk, identify control measures, and verify implementation of control measures of identified SoSHA hazards.

Commented [PDANUAA716]: Is this the purpose?

Reworked

Commented [PDANUAA717]: Added maintenance of SRHA to keep relevant over life cycle

Commented [PDANUAA718]: Good statement but wrong place. Moved to 209.2.1.7

Commented [PDANUAA719]: 209.2.1.6

Commented [PDANUAA720]: 209.2.5

Commented [PDANUAA721]: 209.2.6

Commented [PDANUAA722]: 209.2.6.1

Commented [PDANUAA723]: 209.2.2.1

Commented [PDANUAA724]: 209.2.6

Different elements of the SoS will likely be under different contracts. How to ensure the element's format/content are compatible with other SoS elements?

209.2.1 **SoSHA Scope:**

209.2.1.1 This analyses shall address how the system interacts within a SoS.

209.2.1.2 The contractor shall obtain government approval for which SoSs the SoSHA will be applied to.

209.2.1.3 This analyses shall include NDI (to include COTs, GOTS, GFE, etc.).

209.2.1.4 NDI shall be treated as "Black Boxes" in the analyses unless (1) sufficient design details are available to analyze appropriately and (2) government approval for analyses on the NDI has been granted.

209.2.1.5 If NDI are used in an environment or manner other than originally designed for, and detail analyses has not been accomplished for the expanded environment, then the expanded operating environment shall be documented in the hazard analyses as an "Assumption that such expansion has not introduced additional hazards".

209.2.1.6 Unique SoS hardware and software architecture elements, locations, interfaces, data, etc shall be clearly identified so that future references

209.2.1.7 The human shall be considered an element of the SoS, receiving both inputs and initiating outputs within the analysis.

209.1.8 SoS stakeholders of elements outside the system shall be identified.

209.2.2 **Hazard Identification:** The contractor shall apply systematic hazard analyses techniques to identify new SoS hazards or SoS impacts to existing hazards.

209.2.2.1 The contractor shall obtain government approval of hazard analyses techniques to be used before performing the SoSHA.

209.2.2.2 As necessary, the contractor shall incorporate supporting system data for hazard analyses through associate contract agreements and/or government organically developed items.

209.2.2.3 The contractor shall …

209.2.3 **Hazard Characterization:** The contractor shall use the best available data to characterize each SoS hazard by applying paragraph 4 methodology to include, but not limited to:

209.2.4.1 Name of SoS element

209.2.4.2 Hazard Description

Commented [PDANUAA725]: A SOSHA can be approached from two different perspectives:
1) The manager of the SOS conducts an analyses of all elements of the SOS
2) Each element of the SOS conducts an analyses of how the SOS element 'fits into" the SOS

Both approaches are valid, but most contracted activity will be (2). Since the expectations are different between (1) and (2), this task is reworked for (2)

Perhaps ADD a discuss in the appendix suggesting language of how to apply the revised task to (1)

Risk acceptance structure will vary. Unless otherwise specified, the risk acceptance for (2) will be assumed. It is left to the program to adjust if the risk acceptance criteria differs.

Commented [PDANUAA726]: Need to reword, but think the general intent is captured. If a different group is developing a portion or impacting a subsystem, the safety analyses needs to account for those relevant details
This can be either HW or SW

Commented [PDANUAA727]: How does the contractor addressing one SOS element communicate/collaborate with the other SoS parties? Associate contractor agreements?

Commented [PDANUAA728]: What field provide a minimal set of data needed for the SoSHA?

209.2.4.3 Hazard Causal Factors to include how the hazard is communicated through the SoS via hardware, software, human involvement, and environmental considerations.

209.2.4.4 System effects of SoS hazards.

209.2.4.5 Identification where in the system the SoS hazard exists. e.g. what hardware component(s), what "unit(s)" of software, etc.

209.2.2.6 Software "units" shall include the corresponding SWCI and AICI levels

209.2.2.7 Emergency systems shall focus on preserving the function for when needed during an emergency.

209.2.2.8 Identification of when the hazard asserts itself. e.g. phase of operation or maintenance, mode of operation or maintenance, etc

209.2.2.9 Identification of test unique aspects of the hazard.

209.2.2.10 Identification of interfaces between SoS elements, subsystems, hardware, software "units', and human.

209.2.2.11 Software contributions shall include software developed by other sources.

209.2.2.12 Identification of functions impacted by the hazard.

209.2.2.13 Identification of NDI (e.g. COTS, GOTS, REUSE Software, GFE, etc.) associated with the hazard. .

209.2.2.13.1 Evaluation of NDI to determine if usage is different from what the NTI was originally designed for.

209.2.2.13.2 Unless otherwise approved by the government, hazard analyses shall be limited to NDI inputs, outputs, and other interfaces. Details internal to the NDI whall be treated as a "black box".

209.2.9 Identification of SoS Control Loop impacts

209.2.4 **Assessing Risk Level:** The contractor shall assess the risk of SoS hazards:

209.2.4.1 An initial assessment of the subsystem risk of the current system without consideration of additional controls.

209.2.4.2 Maintain a current risk assessment of the subsystem risk accounting for all of the hazard controls that have been implemented

209.2.4.3 Project an end state risk assessment of the subsystem risk accounting for all planned and implemented hazard controls.

Commented [PDANUAA729]: From a contractual perspective, the contractor can only really speak for the system(s) they are on contract for. Other SoS element effects should be accounted for the activity overseeing the element in question.

Commented [PDANUAA730]: Interfaces between the system and other SoS elements are key. What are the checks/balances to ensure input data is of the correct format and not corrupted. These "filters" are inherent design features to interrupt SoS hazards.
So, how does one characterize these "filters"? What are they, what are they filtering (or not), etc. Should an aspect of Task 209 specifically analyze these filters?

Also, each SoS Element may be approaching deriving SWCI differently (as SWCI will be derived within each SWCI element; how will the total SoS be reviewed for consistency?)

Commented [PDANUAA731]: Do modes of other SoS elements need to be accounted for?

Commented [PDANUAA732]: How to ensure Table III is consistent across all SoS elements?

209.2.4.4 The definitions in Table I shall be used to characterize subsystem hazard severity.

209.2.4.5 The definitions in Table II shall be used to characterize subsystem hazard probability.

209.2.4.6 Table III shall be used to derive the respective subsystem HRIs of the hazard.

209.2.5 **Identification of Potential Hazard Control Methods:** The contractor shall identify potential SoS hazard controls to lower the system safety risk to an acceptable level

209.2.5.1 The hazard controls shall be follow the system safety order precedence (paragraph 4.x)

209.2.6 ~~**Hazard**~~ **Documentation:** The contractor shall document results of the analysis to include the following:

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

209.2.6.2

209.3 HTS Fields

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

~~a. Imposition of Task 209. (R)~~

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

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

Commented [PDANUAA733]: Need to flesh out

Commented [PDANUAA734]: Each 2XX Tasks has a different set of HTS Fields pertinent to that analyses. As such, required HTS fields include those identified in para 4.3.1.5 (See 46-4; 52-3)

FUTURE ACTION: Review 4.3.1.5 and all 2XX.3 HTS Fields eliminate duplications.

Commented [PDANUAA735]: See 101.3

~~d. Concept of operations.~~

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

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

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

TASK 210
ENVIRONMENTAL HAZARD ANALYSIS

73-1 Why doesn't Task 108 have a Scope and Objectives Section like other Tasks?
➔Addressed in revised task

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

210.1 Purpose. Task 210 is to perform, document and maintain an Environmental Hazard Analysis (EHA) to:

a. Identify hazards to the environment throughout all life-cycle phases and modes
b. Manage environmental hazards using the system safety process described in Section 4
c. Support design development decisions
d. Document environmental hazards

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

210.2 Task description. The contractor shall perform, document, and maintain to identify environmental hazards, characterize environmental hazards, assess risk, identify environmental control measures, and document environmental hazards.

210.2.1 Scope: The contractor shall provide a comprehensive summary of the environmental hazards and impacts of the system throughout the life-cycle.

73-2 How should the EHA be defined? Below subparas parallel other 2XX tasks.

FUTURE ACTION: Refine requirements defining EHA Scope

210.2.1.1. The EHA analyses shall include NDI (to include COTS, GOTS, GFE, etc.).

210.2.1.1.1. NDI shall be treated as "Black Boxes" in the analyses unless (1) sufficient design details are available to analyze appropriately and (2) government approval for analyses on the NDI has been granted.

Commented [PDANUAA736]: Reformat.
HAZMAT related info moved to Task 211

Commented [PDANUAA737]: Added maintenance of SRHA to keep relevant over life cycle
Reordered purposed bullets

Commented [PDANUAA738]: Reformatted & Reworded
Section 4 applies whenever 882 is invoked; it is redundant to repeat here.
Also see 73-2

Commented [PDANUAA739]: 73-2

Commented [PDANUAA740]: Added since NDI components of a system could contribute to environmental issues/consequences
See 51-9

210.2.1.1.2 If and NDI (to include COTS, GOTS, GFE) are used in an environment or manner other than originally designed for, and detail analyses has not been accomplished for the expanded environment, then the expanded operating environment shall be documented in the hazard analyses as an "Assumption that such expansion has not introduced additional hazards".

210.2.1.2 The contractor shall obtain PM approval of environmental hazard/aspect/impact analyses techniques to be used before performing the analysis.

210.2.1.3 System software shall be clearly identified so that future references to aspects of the software supporting the system are unambiguous.

210.2.1.4 The contractor performing the EHA shall monitor, obtain, and integrate the output of each phase of the software development process in evaluating the software contribution to the EHA.

210.2.1.4.1 The contractor shall coordinate with the PM hazard control actions involving software development.

210.2.1.5 The contractor shall update, as necessary, the EHA following system design changes, including software ~~design~~ changes.

210.2.1.6 The contractor shall re-evaluate the system if the system's operating environment changes.

210.2.1.7 Additional areas to consider include, but are not limited to, performance, performance degradation, functional failures, timing errors, design errors, defects, control law failures, and inadvertent functioning.

210.2.1.8 While conducting this analysis, the human shall be considered a component within the system, receiving both inputs and initiating outputs.

210.2.1.9 Environmental impacts from noise generation resulting from operation of the system and subsystems.

210.2.1.10 Environmental aspects and impacts on sea, air, space, and land resources and ecosystems.

210.2.2 **Environmental Hazard/Aspect/Impact Identification**: The contractor shall apply systematical analyses techniques to identify new environmental hazards/aspects/impacts.

73-3
System Safety uses the term Hazard to identify system safety issues that para 4 is built around. Environment Aspect and Environmental Impact are terms used by the environmental community to work/track environmental related issues/concerns. It is not clear if there are Environmental hazards. As such, does para 4 methodology apply to analyzing/controlling environmental aspects/impacts/hazards?
FUTURE ACTION: Standardize Terminology used in Task 210.
FUTURE ACTION: Validate para 4 applicability to environmental aspects/impacts/hazards

Commented [PDANUAA741]: Added to ensure environmental hazard/aspect/impact analyses techniques employed are agreed to be appropriate by the PM (government)
See 52-1

Commented [PDANUAA742]: Added since software within a system could contribute to environmental issues/consequences

Commented [PDANUAA743]: Expanding the operational envelop may introduce new environmental issues/concerns

Commented [PDANUAA744]: Human involvement in the system could contribute to environmental issues/consequences

Commented [PDANUAA745]: Moved from 882E para 210.2.2.a(4).
Added Environmental Impacts to differentiate from noise health hazards covered in Task 207.
Added subsystems for completeness.

Commented [PDANUAA746]: Moved from 882E para 210.2.2.a(8)
Added "aspects" to capture proper scope. EHA is conducted to determine IF there is an "impact". Thus, aspect provides a means to identify analyses areas that do not result in an "impact".

Commented [PDANUAA747]: 73-3
See 74-1

210.2.2.1 As necessary, the contractor shall incorporate supporting system component data for hazard analyses through associate contract agreements, government organically developed items, and/or other NDI sources.

205.2.4**Environmental Hazard/Aspect/Impact Characterization:** The contractor shall use the best available data to characterize each environmental hazard/aspect/impact by applying paragraph 4 methodology to include, but not limited to:

210.2.3.1 Environmental hazard/aspect/impact description.

210.2.3.2 Environmental Hazard/Aspect/Impact Causal Factors to include hardware, software, human involvement, and environmental considerations.

Commented [PDANUAA748]: Generic reference needed as an explicit list will be too burdensome. Also, such a list is common across all 2XX Tasks. FUTURE ACTION ➔ Expand Appendix to discuss specific considerations.

210.2.3.3 Proposed environmental hazard/aspect/impact controls (e.g. mitigation or amelioration measures).

210.2.3.4 Identification of where in the system the environmental hazard/aspect/impact exists. (e.g. subsystem/ components, what "unit" of software, etc.)

210.2.3.4.1 Software "units" shall include the corresponding SWCI and AICI levels.

210.2.3.5 Identification of when the environmental hazard/aspect/impact asserts itself. (e.g. phase of operation or maintenance, mode of operation or maintenance, etc.)

210.2.3.5.1 Identification of test unique aspects of the environmental hazard/aspect/impact.

210.2.3.6 Identification of interfaces between subsystems, hardware, software "units", human, and SOS where applicable.

210.2.3.6.1 Software contributions shall include software developed by other sources.

210.2.3.7 Identification of functions impacted by the environmental hazard/aspect/impact.

210.2.3.8 Identification of NDI (e.g. COTS, GOTS, REUSE Software, GFE, etc.) associated with the environmental hazard/aspect/impact.

210.2.3.8.1 Evaluation of NDI to determine if usage is different from what the NDI was originally designed for.

210.2.3.8.2 Unless otherwise approved by the government, environmental hazard/aspect/impact analyses shall be limited to NDI inputs, outputs, and other interfaces. Details internal to the NDI shall be treated as a "black box".

210.2.3.9 Identification of Control Loop impacts.

210.2.3.10 Possible independent, dependent, and simultaneous events, including system failures, failures of safety devices, common cause failures, and system interactions that could create an environmental hazard/aspect/impact or result in an increase in risk.

210.2.4 **Assess Environmental Hazard/Aspect/Impact Risk Level**:

210.2.4.1 An initial assessment of the environmental risk of the current system without consideration of additional controls.

210.2.4.2 Maintain a current environmental risk assessment of the system risk accounting for all of the hazard controls that have been implemented.

210.2.4.3 Project an end state risk assessment of the environmental risk accounting for all planned and implemented hazard controls.

210.2.4.4 The definitions in Table I shall be used to characterize environmental hazard severity.

210.2.4.5 The definitions in Table II shall be used to characterize environmental hazard probability.

210.2.4.6 Table III shall be used to derive the respective HRIs of the environmental hazard**.**

210.2.5 **Identification of Potential Environmental Hazard/Aspect/Impact Control Methods**: The contractor shall identify potential environmental hazard/aspect/impact controls to lower the environmental risk to an acceptable level.

210.2.5.1 The analysis shall consider the impact of ~~mitigations~~ controls on safety and occupational health, as well as other applicable SE design considerations.

Commented [PDANUAA749]: See ii-2

Commented [PDANUAA750]: Clarification

210.2.5.2 The hazard controls shall follow the system safety order precedence as defined in paragraph 4.3.4.1.

210.2.6 **Environmental Hazard/Aspect/Impact Documentation:** The contractor shall document the EHA.

210.2.6.1 The contractor shall summarize the system's physical and function characteristic.

210.2.6.2 The contractor shall summarize the subsystems, interfaces, control laws, etc. that comprise the system.

210.2.6.3 The contractor shall reference more detailed system and subsystem descriptions, including specifications and detailed review documentation, when such documentation is available.

210.2.6.4 The contractor shall describe all hazard analyses methodologies/techniques used in developing the EHA.

210.2.6.4.1 The contractor shall provide a description of each method and technique used in conduct of the analysis.

210.2.6.4.2The contractor shall include a description of assumptions made for each analysis and the qualitative or quantitative data used.

210.2.6.5 The contractor shall include the EHA results.

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

73-4 This paragraph seems out of place. Some could be merged with the Purpose Section or add a Scope and objectives section.
The thoughts captured are good philosophy are to why an EHA should be accomplished early in the life cycle of a program. However, this discussion does not contain actionable requirements. Such general guidance/knowledge belongs in the appendix.
FUTURE ACTION: Move to appendix.

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

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

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

73-5 Wordy. Use the SE Process to assess hazards and make recommendations to eliminate them and reduce risk.
Response: MIL-STD-882 establishes the System Safety Process. Establishing SE (Systems Engineering) Process requirements is outside the scope of MIL-STD-882.

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

Commented [PDANUAA751]: 73-4

Commented [PDANUAA752]: See ii-2

Commented [PDANUAA753]: This section seems redundant. Could be merged with a Scope or **removed**. See 73-3

Commented [PDANUAA754]: See ii-2

Commented [PDANUAA755]: Moved to 210.2.2.4, 210.2.2.5, 210.2.2.6

Commented [PDANUAA756]: 73-5
Deleted - Redundant with para 4 (which automatically is applicable when MIL-STD-882 placed on contract).

Commented [PDANUAA757]: Moved to 210.2.2

~~(1) Hazardous materials use and generation.~~

~~(2) Demilitarization and disposal requirements.~~

Commented [PDANUAA758]: Moved to New Task 211

Commented [PDANUAA759]: Moved to New Task 211

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

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

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

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

(7) Inadvertent hazardous releases.

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

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

74-1 With other 2XX Tasks, discussion of potential sources for identification of hazards will be moved to appendix. The same logic applies here as well. (1) – (9) are all potential areas to consider when identifying environmental requirements and hazards. Presumably, this list is a non-inclusive list.
What is needed is what are the requirements/rules governing how environmental hazards/aspects/impacts are identified?
FUTURE ACTION: Move (1) – (9) discussion to appendix.
FUTURE ACTION: Define what are the requirements/rules governing how environmental hazards/aspects/impacts are identified?

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

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

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

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

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

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

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

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

Commented [PDANUAA760]: Moved to New Task 211

Commented [PDANUAA761]: Moved to 210.2.1.10

Commented [PDANUAA762]: Moved to New Task 211

Commented [PDANUAA763]: Moved to New Task 211

Commented [PDANUAA764]: Moved to New Task 211

Commented [PDANUAA765]: Moved to 210.2.1.11

Commented [PDANUAA766]: 74-1.
See 210.2.2 for environmental hazard/aspect/impact identification discussion

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

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

Commented [PDANUAA767]: Moved to 210.2.5

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

Commented [PDANUAA768]: Moved to 210.2.6

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

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

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

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

~~a. HAZMAT item or substance name.~~

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

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

~~d. Location of HAZMAT within the system.~~

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

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

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

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

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

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

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

Commented [PDANUAA769]: Moved to 210.2.6.1, 210.2.6.2, 210.2.6.3

Commented [PDANUAA770]: Moved to 210.2.6.4, 210.2.6.4.1, 210.2.6.4.2

Commented [PDANUAA771]: Moved to 210.2.6.5

Commented [PDANUAA772]: Moved to New Task 211

~~b. Sources of emission for each pollutant.~~

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

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

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

~~a. Imposition of Task 210. (R)~~

~~b. Minimum reporting requirements. (R)~~

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

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

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

~~f. Concept of operations.~~

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

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

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

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

210.3 Environmental Tracking System (ETS) Fields: TBD

76-1 Environmental aspects/impacts cannot be tracked in the HTS due to dissimilarities of required information.
FUTURE ACTION: Define fields necessary to track environmental hazards/aspects/impacts.
FUTURE ACTION: Adjust para 4.3.1.5 to account for this different tracking system.

Commented [PDANUAA773]: See 101.3 for rationale why 210.3 is proposed to be deleted.

Commented [PDANUAA774]: New 210.3 to address unique required Task 210 Environmental Hazard/Aspect/Impact Tracking System fields.

Commented [PDANUAA775]: 76-1

TASK 211

HAZMAT HAZARD ANALYSIS

211.1 Purpose. Task 210 is to perform, document and maintain a hazardous materials (HAZMAT) Hazard Analyses (HAZMATHA) to

a. Evaluate proposed HAZMAT usage and processing.

b. Provide the system-specific data to support National Environmental Policy Act (NEPA) and Executive Order (EO) 12114 requirements.

211.2 Task description. The contractor shall perform, document and maintain a HAZMATHA to identify hazards, characterize hazards, assess safety risk, identify control measures, and verify implementation of control measures of identified system hazards.

211.2.1 **HAZMATHA Scope**:

New 211-1 How should the HAZMATHA be defined? Below subparas parallel other 2XX tasks.

FUTURE ACTION: Refine requirements defining HAZMATHA Scope

211.2.1.1. The HAZMATHA analyses shall include NDI (to include COTS, GOTS, GFE, etc.).

211.2.1.1.1. NDI shall be treated as "Black Boxes" in the analyses unless (1) sufficient design details are available to analyze appropriately and (2) government approval for analyses on the NDI has been granted.

211.2.1.1.2 If NDI are used in an environment or manner other than originally designed for, and detail analyses has not been accomplished for the expanded environment, then the expanded operating environment shall be documented in the hazard analyses as an "Assumption that such expansion has not introduced additional hazards".

211.2.1.2 The contractor shall obtain PM approval of HAZMATHA techniques to be used before performing the analysis.

211.2.1.3 System software shall be clearly identified so that future references to aspects of the software supporting the system are unambiguous.

211.2.1.4 The contractor performing the HAZMATHA shall monitor, obtain, and integrate the output of each phase of the software development process in evaluating the software contribution to the HAZMATHA.

211.2.1.4.1 The contractor shall coordinate with the PM hazard control actions involving software development.

Commented [PDANUAA776]: New Tasks to address HAZMAT specific concerns. Activities in Tack 211 are different than those in Task 207 (Health Hazard Analyses) & 210 (Environmental Hazard Analyses)

Commented [PDANUAA777]: Added maintenance of SRHA to keep relevant over life cycle

Commented [PDANUAA778]: Added since NDI components of a system could contribute to HAZMAT issues/consequences
See 51-9

Commented [PDANUAA779]: 54-6
Added to ensure HAZMATHA techniques employed are agreed to be appropriate by the PM (government)See 52-1

Commented [PDANUAA780]: Added since software within a system could contribute to environmental issues/consequences

211.2.1.5 The contractor shall updated, as necessary, the SHA following system design changes, including software ~~design~~ changes.

211.2.1.6 The contractor shall re-evaluate the system if the system's operating environment changes.

211.2.1.7 Additional areas to consider include, but not limited to, include performance, performance degradation, functional failures, timing errors, design errors, defects, control law failures, and inadvertent functioning.

211.2.1.8 While conducting this analysis, the human shall be considered a component within the system, receiving both inputs and initiating outputs.

211.2.1.9 The HAZMATHA shall address hazardous materials use, generation, and associated costs.

211.2.1.10 The HAZMATHA shall address demilitarization and disposal requirements.

211.2.1.10.1 The HAZMATHA shall address quantity, characteristics, concentrations, and exposures to chemical, biological, and other hazards impacting public health such as acute health, chronic health, carcinogenic, contact, flammability, reactivity aspects of the HAZMAT.

211.2.1.11 The HAZMATHA shall address pollutant emissions generation (e.g., air, water, and solid waste).

211.2.1.12 The HAZMATHA shall address release of hazardous substances incidental to the routine maintenance and operation of the system.

211.2.1.13 The HAZMATHA shall address inadvertent hazardous releases.

211.2.1.14 The HAZMATHA shall evaluate alternate materials to identified HAZMATs.

211.2.1.15 The HAZMATHA shall describe processes utilizing HAZMATs.

211.2.2 **HAZMAT Hazard Identification**: The contractor shall apply systematical analyses techniques to identify new environmental hazards/aspects/impacts.

211.2.2.1 As necessary, the contractor shall incorporate supporting system component data for hazard analyses through associate contract agreements government organically developed items, and/or other NDI sources.

211.2.3 **HAZMAT Hazard Characterization**: The contractor shall use the best available data to characterize each environmental hazard/aspect/impact by applying paragraph 4 methodology to include, but not limited to:

Commented [PDANUAA781]: Expanding the operational envelop may introduce new HAZMAT issues/concerns

Commented [PDANUAA782]: Human involvement in the system could contribute to environmental issues/consequences

Commented [PDANUAA783]: Moved from 882E para 210.2.2.a(1)

Commented [PDANUAA784]: Moved from 882E para 210.2.2.a(2)

Commented [PDANUAA785]: Moved from 882E para 210.2.2.a(3)

Commented [PDANUAA786]: Moved from 882E para 210.2.2.a(5)

Commented [PDANUAA787]: Moved from 882E para 210.2.2.a(6)

Commented [PDANUAA788]: Moved from 882E para 210.2.2.a(7)

211.2.3.1 HAZMAT hazard description

211.2.3.2 HAZMAT Hazard Causal Factors to include hardware, software, human involvement, and environmental considerations.

211.2.3.3 Proposed HAZMATHA controls (e.g. mitigation or amelioration measures)

211.2.3.4 Identification of where in the system the HAZMAT hazard exists. (e.g. subsystem/ components, what "unit" of software, etc.)

211.2.3.4.1 Software "units" shall include the corresponding SWCI and AICI levels

211.2.3.5 Identification of when the HAZMAT hazard asserts itself. (e.g. phase of operation or maintenance, mode of operation or maintenance, etc)

211.2.3.5.1 Identification of test unique aspects of the HAZMAT hazard.

211.2.3.6 Identification of interfaces between subsystems, hardware, software "units', human, and SOS where applicable

211.2.3.6.1 Software contributions shall include software developed by other sources.

211.2.3.7 Identification of functions impacted by the HAZMAT hazard.

211.2.3.8 Identification of NDI (e.g. COTS, GOTS, REUSE Software, GFE, etc.) associated with the HAZMAT hazard.

211.2.3.8.1 Evaluation of NDI to determine if usage is different from what the NTI was originally designed for.

211.2.3.8.2 Unless otherwise approved by the government, HAZMAT hazard analyses shall be limited to NDI inputs, outputs, and other interfaces. Details internal to the NDI shall be treated as a "black box".

211.2.3.9 Identification of Control Loop impacts

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

211.2.4 Assess HAZMAT Hazard risk level:

211.2.4.1 An initial assessment of the HAZMAT hazard risk of the current system without consideration of additional controls.

Commented [PDANUAA789]: Generic reference needed as an explicit list will be too burdensome. Also, such a list is common across all 2XX Tasks. FUTURE ACTION ➔ Expand Appendix to discuss specific considerations.

211.2.4.2 Maintain a current HAZMAT hazard risk assessment of the system risk accounting for all of the hazard controls that have been implemented.

211.2.4.3 Project an end state risk assessment of the HAZMAT hazard risk accounting for all planned and implemented hazard controls.

211.2.4.4 The definitions in Table I shall be used to characterize HAZMAT hazard severity.

211.2.4.5 The definitions in Table II shall be used to characterize HAZMAT hazard probability.

211.2.4.6 Table III shall be used to derive the respective HRIs of the HAZMAT hazard**.**

211.2.5 **Identification of Potential HAZMAT Hazard Control Methods**: The contractor shall identify potential HAZMAT hazard controls to lower the system safety risk to an acceptable level.

211.2.5.1 HAZMATHA shall consider the impact of-controls on safety and occupational health, as well as other applicable SE design considerations.

211.2.5.2 The hazard controls shall be follow the system safety order precedence as defined in paragraph 4.3.4.1.

211.2.6 **HAZMATHA Documentation:** The contractor shall document the HAZMATHA.

211.2.6.1 The contractor shall summarized the system's physical and function characteristic.

211.2.6.2 The contractor shall summarize the subsystems, interfaces, control laws, etc that comprise the system.

211.2.6.3 The contractor shall reference more detailed system and subsystem descriptions, including specifications and detailed review documentation, when such documentation is available.

211.2.6.4 The contractor shall describe all hazard analyses methodologies/techniques used in developing the HAZMATHA.

211.2.6.4.1 The contractor shall provide a description of each method and technique used in conduct of the analysis.

211.2.6.4.2 The contractor shall include a description of assumptions made for each analysis and the qualitative or quantitative data used.

211.2.6.5 The contractor shall include the HAZMATHA results.

211.3 HAZMAT Tracking

211.3.1 If the hazards are associated with HAZMAT, they shall include the following minimum data elements:

a. HAZMAT item or substance name.
b. HAZMAT Category (prohibited, restricted, or tracked).
c. Special Material Content Code (SMCC) as designated in DoD 4100.39-M, Volume
d. Location of HAZMAT within the system.
e. Quantity of HAZMAT within the system with traceability to version specific hardware designs.
f. Application, process, or activity whereby quantities of HAZMAT are embedded in the system, or used during operations, and support of the system.
g. Anticipated HAZMAT (whether categorized or not categorized) generated during the system's life-cycle (e.g., installation, Government test and evaluation, normal use, and maintenance or repair of the system).
h. Anticipated HAZMAT (whether categorized or not categorized) generated during mishaps.
i. Special HAZMAT control, training, handling measures, and Personal Protective Equipment (PPE) needed, including provision of required Safety Data Sheets (SDSs).

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

a. Identification of the specific pollutants associated with system operations and maintenance activities.
b. Sources of emission for each pollutant.
c. Quantity and magnitude or rate of pollution generated during normal operation and maintenance as specified by the program office
e. Special emission control, training, handling measures, and personal protective equipment needed.

TASK SECTION 300 – EVALUATION

TASK 301
SAFETY ASSESSMENT REPORT

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

301.1 Purpose. Task 301 is to perform, document and maintain a Safety Assessment Report (SAR) and aHazard Management Report (MHAR) to provide a comprehensive evaluation of the status of safety hazards and their associated risks: Typical events requiring a SAR/MHAR include:

a. prior to test of a system
b. prior to fielding/operation of a system
c. prior to the next contract phase
d. prior to providing the system to another organization/program
e. at contract completion.

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

301.2 Task Description: The contractor shall perform, document, and maintain a system safety assessment of the program to include, at the time of the report, the following:

301.2.1 **Scope:** The contractor shall provide a comprehensive summary of the system safety program to include all system safety products developed to date.

301.2.1.1 Areas not analyzed shall be clearly identified.

301.2.2 **System Safety Process Overview:** The contractor shall provide an overview of all of the system safety processes employed.

301.2.2.1 The contractor shall include all definitions and associated system safety framework from which system safety products are derived from.

301.2.2.2 If applicable, the contractor shall describe how system safety interfaced with model based engineering.

301.2.2.3 The contractor shall summarize the techniques used in developing safety products.

Commented [PDANUAA790]: General Note. This task was largely rewritten/restructured to improve readability, clarity, and account for a means to document additional areas where safety documentation is needed.

Focus is the TASK of developing/gathering data to be documented in the SAR.

The DID provides the content/format details.

Commented [PDANUAA791]: Reformat/edit to provide clearer context

Added "d" to account for (1) programs management responsibility being transferred (2) independent subsystem development being assumed by system

Commented [PDANUAA792]: Reformat/reworked to better capture scope of what is needed to be accounted for in the SAR

Commented [PDANUAA793]: An example of some areas include various forms of NDI. It is important for the record to know what portions of the design were not investigated (aka treated as a "Black Box").

Commented [PDANUAA794]: Recapping the processes followed in accomplishing system safety activities makes the SAR a stand-alone document. It removes potential confusion as to what definitions, processes, decisions, etc are pertinent to correctly interpreting the rest of the report.

Commented [PDANUAA795]: Derived from 882E para 301.2.a
This would cover all of the Tables in para 4 as well as any unique program specific processes.

Commented [PDANUAA796]: Model based engineering will change how system safety accomplishes tasks. Knowing what these process changes are can provide better insights into how the system safety program was executed - & in turn is useful for interpreting system safety products

301.2.2.4 The contractor shall address how vendor and associated contractor safety products have been incorporated.

301.2.3 **System Description**:

301.2.3.1 The contractor shall describe the system to include subsystems and components.

301.2.3.2 The contractor shall describe the software in the system to include the software's general purpose, incorporation of artificial intelligence, and machine learning.

301.2.3.2.1 The software description shall include the computational hardware hosting such software. This would include multicore processing, virtualization, containerization, and other related technologies.

301.2.3.2.2 The contractor shall describe how software is decomposed into smaller partitions/units that are referenced in the safety documentation.

301.2.3.3 The contractor shall describe safety significant control laws.

301.2.3.4 The contractor shall describe interfaces between subsystems, components, other software, and with applicable System of Systems (SoS).

301.2.3.5 The contract shall describe safety significant functions.

301.2.3.5.1 If accomplished, the contractor shall document the results of safety significant function analyses.

301.2.3.6 The contractor shall describe all NDI used in the system during all operations, maintenance, and/or testing.

301.2.3.7 The contractor shall account for all variants and configurations of the system.

301.2.3.8 The contractor shall describe the system environment inclusive of operations, maintenance, and test envelopes.

301.2.3.9 The contractor shall describe modes of operation to include operations, maintenance and test.

301.2.4 **Software Safety Assurance:** The contractor shall summarize software safety compliance (e.g. paragraph 4.4) activities and results.

301.2.4.1 The contractor shall summarize all SWCI LOR and AICI LOR activities.

301.2.4.2 The contractor shall attest to the completion of applicable SWCI LOR and AICI LOR activities for the system.

Commented [PDANUAA797]: As systems become more computerized, a standard description expectation is needed. Understanding the hosting hardware provides the basis of this understanding.

Commented [PDANUAA798]: Laying the foundation of how software units will be referenced in the rest of the system safety documentation. (see 4.4.1.2.1)

Commented [PDANUAA799]: Summarizing Task 208 or similar functional looks

Commented [PDANUAA800]: Broad context here to include COTS, GFE, GFI, etc

Commented [PDANUAA801]: Needed since configuration differences can have a huge impact on how a hazard is realized in a system

Commented [PDANUAA802]: Provided the basis for how/when hazards are realized

Commented [PDANUAA803]: This section provides a means to document LOR activities/results. (gap in 882E does not provide a means for such documentation)

NOTE: Discussion kept at LOR level as the LOR will be uniquely tailored for each program. Thus the requirement is established to account for LOR activities/products while retaining the flexibility for each program to address specific program LOR activities/products.

301.2.5 **Life Cycle:** The contractor shall provide an overview of the program's life cycle to include test, fielding, required safety significant certifications, etc.

301.2.5.1 The contractor shall define the expected operating, maintenance, and testing environments.

301.2.6 **Test/Field Results:** The contractor shall summarize safety significant test results, fielding experience, software anomalies, etc

301.2.7 **Safety Features:** The contractor shall define and summarize safety features in a system.

78-1 **Safety Features** are often cited but not defined. Therefore, from a program perspective, what is a safety feature? What safety features are used in the system?
FUTURE ACTION: Define the term Safety Feature in 3.2.x

301.2.8 **Hazard Tracking System (HTS)**: The contractor shall summarize the most recent status of the HTS.

301.2.8.1 As a minimum, the HTS summary shall include for each hazard a brief description of the issue, the corresponding risk characterize, hazard controls, and hazard resolution status.

301.2.8.2 The contractor shall summarize the effectiveness of hazard controls.

301.2.9 **Environmental/HAZMAT:** The contractor shall summarize the most recent environmental/HAZMAT data.

301.2.9.1 Identification of material type, quantity, and hazards.

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

301.2.9.3 Assessments of why less hazardous materials could not be used.

78-2 FUTURE ACTION: Define expectations of how best to summarize environmental/HAZMAT data.

301.2.10 **Citations:** The contractor shall list all pertinent references, including (but not limited to) hazard analyses, tests reports, reports related to LOR implementation, other program reports, standards, regulations, procedures, manuals, etc.

301.2.10.1 Each reference shall include publication date, title, document number, and other information required to positively cite the document.

78-3 FUTURE ACTION: Will need to update corresponding DID and make sure the DID is in concert with this revision

Commented [PDANUAA804]: Traditionally, overviews would be tied to program milestones. But with new managerial practices (e,g, MTA, Agile software, etc), such a structured timeline is muddled. Therefore, this is written in a more generic manner to be inclusive of all program management approaches

Commented [PDANUAA805]: Catchall for anything the contractor has learned of the system during the reporting period

Commented [PDANUAA806]: 78-1

Commented [PDANUAA807]: HTS includes results of 2XX hazard analyses tasks. As some hazard records can be quite lengthy, what is desired is a summary highlighting how the hazard was characterized

Commented [PDANUAA808]: Was 882E paras 301.2.b, 301.2.c, 301.2.d, 301.2.f, 301.2.g

Commented [PDANUAA809]: Was 882E para 301.2.e 78-2

Commented [PDANUAA810]: Was 882E para 302.2.e(1) See note at beginning of Task 302.

Commented [PDANUAA811]: Was 882E para 302.2.e(2) See note at beginning of Task 302.

Commented [PDANUAA812]: Was 882E para 302.2.e(3) See note at beginning of Task 302.

Commented [PDANUAA813]: Was 882E para 301.2.i This provides a traceable list of sources from which the report was generated from.

301.2.11 **Certification:** The contractor shall include a signed statement certifying the correctness of information and the system's readiness to test, operate, or proceed to the next acquisition phase.

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

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

~~c. Hazard Tracking System (HTS) data.~~

~~d. A summary of risks for each identified hazard.~~

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

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

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

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

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

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

~~• Imposition of Task 301. (R)~~

Commented [PDANUAA814]: Was 882E para 301.2.h Signed Statement is a legal affirmation that all information contained in the report is technically correct and current. It affirms that the contractor believes there are no outstanding issues that will prevent a program from proceeding to the next life cycle phases

Commented [PDANUAA815]: Content moved to 301.2.2.1

Commented [PDANUAA816]: Content moved to 301.2.8.1

Commented [PDANUAA817]: Content moved to 301.2.9

Commented [PDANUAA818]: Content moved to 301.2.8.1

Commented [PDANUAA819]: Content moved to 301.2.11

Commented [PDANUAA820]: Content moved to 301.2.10

Commented [PDANUAA821]: Section being deleted as part of larger MIL-STD restructuring. See corresponding comment to 101.3

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

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

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

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

TASK 302
HAZARD MANAGEMENT ASSESSMENT REPORT

Task 302 duplicates Task 301 with the exception of the yellow highlighted text below.
- Para 302.1 changes the title of the report.
- Para 302.2.e subparas (1) through (3) are new & have been added to 301.2.e.

Proposed deletion of this task for many of the same reasons Task 103 was deleted.
If not deleted, then content of this task needs to be scrubbed to remove material not being used …

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

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

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

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

~~c. Hazard Tracking System (HTS) data.~~

~~d. A summary of risks for each identified hazard.~~

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

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

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

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

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

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

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

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

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

~~a. Imposition of Task 302. (R)~~

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

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

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

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

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

TASK 303
TEST AND EVALUATION PARTICIPATION

82-1 Title Revision needed. Task 303 is part of the "Evaluation" grouping of tasks.

What is the focus of Task 303?

- Ensuring System Safety is involved with the planning of test events?
- Evaluating the safety of a test article prior to the test event?
- Evaluating the execution of test events?
- Other?

(If need be, separate tasks could be constructed to provide better delineation of contracted task activity.)

Focus should be on hazards directly related to the test event. What are the UNIQUE aspects that are introduced through testing that could lead to test issues/concerns/hazards?

NOTE: It is possible to have "life cycles" safety hazards present during a test event but are not UNIQUE/Directly related to the test event. Such "life cycle" hazards are already addressed through 2XX Tasks and should not be duplicated in Task 303.

Example: A hazard exists in a system being used for test (e.g. a hazard associated with landing gear), but the hazard is not related to the functionality of the system to be tested (e.g., evaluation of a communication system). The hazard exists, but is not related to the aspect being tested. Hazards associated with the testing of the communications system would be addressed in this task.

Is government oversight needed with the test event (or do other processes already cover)?

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

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

82-2 **FUTURE ACTION:** Develop new task to address V&V risk mitigation measures

82-3 **FUTURE ACTION:** Formally define (test) event risk. The concept is mentioned, but not defined as to what event risk is or how event risk will be managed (if different from other forms of system safety risks)

82-4 **FUTURE ACTION:** Elaborate on the difference between safety hazards/risks associated with test and those associated with the life cycle. Are test safety risks a subset of life cycle safety risks?

Commented [PDANUAA822]: 82-1
Correctness of Title?

Commented [PDANUAA823]: Revised language to more definitively scope the purpose.

V&V of "Risk mitigation measures" is open ended in context. This could mean risk mitigation measures associated with the test
OR
This could mean risk mitigation measures associated with ANY identified hazard.

NOTE – formal testing is not always accomplished for every possible safety risk mitigation measure. In cases where the test is to develop V& V artifacts to validate such risk mitigation measures, then that would be covered under revised purpose verbiage since such hazards would be directly related to the test event.

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

303.2 Task description. The contractor shall participate in:

a. test and evaluation planning
b. support the preparation of test event Safety Releases
c. conduct post-test event actions
d. maintain a repository of reports

303.2.1 ~~T & E~~ Test and evaluation planning ~~shall include~~, at a minimum, shall include the following:

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

303.2.1.1 Participation in the preparation and updating of the T&E Strategy (TES) and the T&E Master Plan (TEMP).

303.2.1.1.1 TES/TEMP content shall include test hazard considerations and identification of when hazard analyses, risk assessments, and risk acceptances shall be completed in order to support T&E schedules.

82.5 Test (event) planning documentation needs to account for the differences in how risks are addressed via life cycle vs test events. Such clarification is needed since risks are addressed in different ways. For example, risk exposure is much more limited in test vs operational life of most systems.

FUTURE ACTION: Define how life cycle safety hazard/risk constructs are modified to address test event safety hazard/risks.

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

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

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

~~(3) Preparation of the Safety Release.~~

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

Commented [PDANUAA824]: Reformat
Deleted 2nd sentence. This is amply stated in para 4.

Commented [PDANUAA825]: Revised to improve readability

Commented [PDANUAA826]: Reformat

Commented [PDANUAA827]: 82.5

Commented [PDANUAA828]: Reformat

Commented [PDANUAA829]: See revised 303.1
It is outside the scope of 882 to define how testing shall be accomplished and what criteria shall be used to grade such tests.
Not every hazard control (mitigation) is tested. Existing guidance in the test community accomplishes this already.

Commented [PDANUAA830]: Moved to 303.2.1.2.1.1
Analyses changed to evaluation to align with 3xx evaluation tasks

Commented [PDANUAA831]: Moved to 303.2.2

Commented [PDANUAA832]: Moved to 303.2.1.2.1.2
Analyses changed to evaluation to align with 3xx evaluation tasks

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

Commented [PDANUAA833]: Moved to 303.2.2.3

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

Commented [PDANUAA834]: Moved to 303.2.2.2

303.2.1.2 Participation in the development of test plans and procedures

303.2.1.2.1 Test plans and procedures shall include hazard considerations that support:

303.2.1.2.1.1 Evaluation of known system hazards present in a given test event so that test-un unique controls can be developed to manage test event risks.

303.2.1.2.1.2 Evaluation of test equipment and procedures to identify hazards so that test-unique controls can be developed to manage test event risks.

303.2.2 Preparation of the Safety Release shall include:

Commented [PDANUAA835]: 82-6

82-6 The term "Safety Release" has not been defined.

FUTURE ACTION: Formally define "test event Safety Release"

303.2.2.1 Documentation of all system safety hazards and other information related to the test shall be provided to the test community.

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

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

303.2.3 ~~Conduct~~ The following post-test event actions conducted shall include:

Commented [PDANUAA836]: Was 882E 303.2.2 Revised to invoke subpara requirements

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

Commented [PDANUAA837]: Moved to 303.2.3.3

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

Commented [PDANUAA838]: Moved to 303.2.3.1

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

303.2.3.2 Evaluate anomalies and assess new system hazards and to potentially update risk assessments for known hazards.

303.2.3.3 Evaluate test results to assess effectiveness of hazard control measures as tested.

82-7 Clarification is needed distinguish if "hazard control measures" refers to life-cycle hazard control measures (aka 2XX Task hazards) and test safety control measures.

FUTURE ACTION: Include discussion laying out the differences between life-cycle oriented hazards and test oriented hazards. Though both are related, each is asking the question from a different perspective. As such, the management of each category of hazards is different. Life cycle hazards considers implications over the entire life cycle whereas test hazards is focused more on the safe execution of the test event

Commented [PDANUAA839]: Anomalies can include software anomalies (as discussed in para 4.4) as well as anomalies related to the test activity.

Commented [PDANUAA840]: 82-7

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

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

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

83-1 Clarification needed.
Does the HTS track life cycle hazards/risks (e.g. from 2XX Tasks) in the same way Test Safety hazards are tracked?
Or, do life cycle hazards need to be tracked separately than test safety hazards?
FUTURE ACTION: Add discussion regarding tracking requirements for life cycle hazards vs test hazards.

303.2.3.5 Evaluate incident, discrepancy, and anomaly reports generated during test events for information on hazards and control measures.

83-2 Clarification needed. Is this life cycle hazard controls or test hazard controls? See 82-7

303.2.3.5.1 Test hazard control measures shall be incorporated into applicable future test plans.

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

~~a. Hazards identified during test events.~~

~~b. Verification and validation of mitigation measures.~~

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

303.2.4 The contractor shall maintain a repository of test and evaluation results.

83-3 Is this a safety requirement or a system engineering/test requirement? As stated, subpara requirements may be "outside the system safety swim lane"

304.2.4.1 The Government shall be provided access to the test and evaluation repository.

304.2.4.2 The contractor shall provide the government with the test and evaluation repository at the end of the contract.

Commented [PDANUAA841]: Reformat
See 303.2.3.5 & 303.2.3.5.1
Mishap reports changed to anomaly reports since anomaly reports is a broader, more inclusive term. Mishaps would be reported as test anomalies.

Commented [PDANUAA842]: Moved to 303.2.4

Commented [PDANUAA843]: 83-1

Commented [PDANUAA844]: 83-2

Commented [PDANUAA845]: Clarification

Commented [PDANUAA846]: See ii-2
See 82-2

Commented [PDANUAA847]: Reformat
Moved to 303.2.4, 304.2.4.1, 304.2.4.2, 304.2.4.3, 304.2.4.3.1, 304.2.4.3.2, & 304.2.4.3.3

Commented [PDANUAA848]: 83-3

304.2.4.3 The test and evaluation repository shall include the following:

304.2.4.3.1 Hazards identified during test events.

Commented [PDANUAA849]: 83-5

83-5 Clarification needed. Test hazards or applicable life-cycle hazards to the test event?

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

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

Commented [PDANUAA850]: See 102.3 comment (29-2)

~~a. Imposition of Task 303. (R)~~

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a. Imposition of Task 304. (R)

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

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

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

Commented [PDANUAA851]: 44-1 This task has been merged with Task 201, thus deletion here

Commented [PDANUAA852]: See 44.17

TASK SECTION 400 - VERIFICATION

TASK 401
SAFETY VERIFICATION AND VALIDATION

86-1 The terms Verification, Validation, and Compliance are often used interchangeably. In 882E, Verification is used 42 times, Validation 34 times, and Compliance 16 times. While related, each term has a specific meaning, and using them interchangeably introduces a source of confusion – especially when it comes to defining 882 requirement expectations. To paraphrase:

Verification – does the system meet the specification/requirements?
Validation – how well the system meets the specification/requirements?
Compliance – does the system meet applicable governing standard(s)?

FUTURE ACTION: Develop a new task (based on 882C Task 402?) to address compliance.
FUTURE ACTION: Add definitions to para 3 for **Verification**, **Validation**, and **Compliance**.

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

401.1 Purpose. Task 401 is to verify and validate safety requirements and system safety hazard control measures in the system design.

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

401.2 Task description. The contractor shall employ engineering methods to verify and validate safety requirements and safety hazard control measures in the system design.

401.2.1 Scope. Verification and validation shall include requirements, control measures, regulatory standards etc for all aspects of a system to include subsystems, components, operating procedures, maintenance procedures, etc.

401.2.1.1 Verification activities focus on if the system design meets the specification and associated requirements. Such activities may be realized through inspection, analyses, demonstration, and test.

86-2: Should this paragraph cite system engineering configuration management? The intent is not to duplicate these principles in 882F (that would be beyond the scope of system safety), but rather anchor the system safety into the systems engineering process.

Commented [PDANUAA853]: 86-1

Commented [PDANUAA854]: Revised purpose to deconflict with Task 303 (Test)

Commented [PDANUAA855]: Reformat
Content adjusted to more directly address verification and validation activities.
See 401.2 & 401.2.3

Commented [PDANUAA856]: 86-3 Added Scope para

Commented [PDANUAA857]: Verification definition added (see 86-1)
86-2

401.2.1.2 Validation activities focus on how well the specification and associate requirements have been met. In other words, do safety hazard controls measures reduce the safety risk as projected?

401.2.3 Induced or simulated failures shall be considered to demonstrate the acceptable safety performance of the equipment and software.

401.2.4 Safety verification and validation shall include, but not limited to, all life cycle activities such as prototypes, iterative software builds, testing, etc.

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

401.2.5.1 When verification analysis or inspection cannot determine the adequacy (e.g. validation) of safety risk control measures, tests shall be specified and conducted to evaluate the overall effectiveness of the control measures.

401.2.5.1.1 Specific safety tests shall be integrated into appropriate system Test and Evaluation (T&E) plans, including verification and validation plans.

401.2.5.1.2 If these specific safety tests are not conducted, then the non-validated control measure shall not be used to reduce the safety risk probability/severity.

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

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

401.2.6 Documentation

401.2.6.1 The contractor shall document safety verification and validation results ~~and submit a report that~~ to includes the following:

401.2.6.1.1 Artifacts from verification activities showing how specification requirements and safety hazard controls measures have been met (or not).

401.2.6.1.2 Artifacts from validation activities establishing the effectiveness of specification requirements and safety hazard controls measures.

401.2.6.1.3 Applicable HTS citations.

401.2.6.1.4 Applicable safety specification/requirement citations.

Commented [PDANUAA858]: Validation definition added (see 86-1)

Commented [PDANUAA859]: Was 401.2.1
Reformatted.
Verbiage revised for clarification

Commented [PDANUAA860]: Added to address possibility IF validation testing is not conducted.

Commented [PDANUAA861]: Delete
882E para 401.2.1 requires safety tests when analyses or inspections cannot be accomplished; yet this para requires analyses or inspection. This is a circular argument/requirement.

Commented [PDANUAA862]: Delete
Duplicates intent of 401.2.1.1
See 86-1 concerning compliance vs verification

Commented [PDANUAA863]: Was 882E para 401.2.4
Validation added to be consistent with rest of task
"and submit report" deleted as this should be addressed through CDRL/DID.

~~(401.2.4) a. Test procedures conducted to verify or demonstrate compliance with the safety requirements on safety-significant hardware, software, and procedures.~~

~~(401.2.4) b. Results from engineering analyses, analogies, laboratory tests, functional mockups, or models and simulations used.~~

~~(401.2.4) c. T&E reports that contain the results of the safety evaluations, with a summary of the results provided.~~

~~401.1 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:~~

~~a. Imposition of Task 401 (R)~~

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

Commented [PDANUAA864]: Delete
Duplicates 401.2.6.1.1 & 401.2.6.1.2
See 86-1 concerning compliance vs verification

Commented [PDANUAA865]: Delete
Duplicates 401.2.6.1.1 & 401.2.6.1.2

Commented [PDANUAA866]: Delete IAW restructuring of the MIL-STD

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

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

TASK 402
EXPLOSIVES HAZARD CLASSIFICATION DATA

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

402.1 Purpose. Task 402 is to perform analyses and tests, develop data necessary to comply with hazard classification regulations, and prepare hazard classification approval documentation.

402.1.1 Such documentation is required for the development/acquisition of new/modified explosives, the associated packaging, or commodities containing explosives/energetics.

402.1.2 For the purpose of this task explosive materials include all articles containing energetic devices/materials.

88-1 Does this need to be expanded to specifically address insensitive muntions?

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

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

88-2 Are there other references that should be included here – such as from DOT?

402.2.1 Scope: Explosive material classification is required for all new explosive materials and device configuration containing explosive materials.

402.2.1.1 The contractor shall consider employment, storage, and transportation when developing explosive material classifications.

402.2.1.2 Typically, the program developing the new explosive material or a new configuration containing explosive material is responsible for obtaining explosive material classifications.

402.2.2 Pertinent data shall include:

Commented [PDANUAA867]: Reformat for clarity. Too densely written for easy discernment of what the fundamental intent is.

Commented [PDANUAA868]: Rather that have the task continuously refer to explosives/energetics, this para defines to intent so the rest of the task verbiage can be presented in a more straightforward manner.
88-1

Commented [PDANUAA869]: Reformat
See 402.3 & 402.3.2

Commented [PDANUAA870]: Changed to italics for clarity of this citation
88-2

Commented [PDANUAA871]: Scope added to define when this task is needed.

Commented [PDANUAA872]: Edit to make contractually binding

~~402.2.1 Narrative information to include functional descriptions, safety features, and similarities and differences to existing analogous explosive commodities, including packaging.~~

402.2.2.1 Narrative information to include functional descriptions, safety features, and similarities and differences to existing analogous articles containing explosive materials.

402.2.2.2 Narrative packaging information for articles containing explosive materials.

~~402.2.3 Technical data to include Department of Defense Identification Codes (DODICs) and National Stock Numbers (NSNs); part numbers; nomenclatures; lists of explosive compositions and their weights, whereabouts, and purposes; and their weights, volumes, and pressures; technical names; performance or product specifications; engineering drawings; and existing relevant Department of Transportation (DOT) classification of explosives approvals.~~

402.2.2.3 Technical explosive material data to include:

a. Department of Defense Identification Codes (DODICs)
b. National Stock Numbers (NSNs)
c. part numbers
d. nomenclatures
e. lists of explosive compositions and their weights, whereabouts, and purposes
f. lists of other hazardous materials and their weights, volumes, and pressures; technical names
g. performance or product specifications
h. engineering drawings
i. existing relevant Department of Transportation (DOT) classification of explosives approvals

~~402.2.4Storage and shipping configuration data to include packaging details.~~

402.2.2.4 Explosive material storage and shipping configuration data to include packaging details.

~~402.2.3 Test plans.~~

402.2.2.5 Explosive material characterization test plans.

~~402.2.3 Test reports.~~

402.2.2.6 Explosive material characterization test reports.

~~402.2.4 Analyses.~~

402.2.2.7 Analyses required for building explosive material classification analogy if testing is not accomplished.

Commented [PDANUAA873]: Reformat
Added words to provide some clarification of the intent here.

Commented [PDANUAA874]: Added words to provide some clarification of the intent here.

Commented [PDANUAA875]: Added words to provide some clarification of the intent here.

Commented [PDANUAA876]: Added words to provide some clarification of the intent here.

Commented [PDANUAA877]: Clarification of what analyses is being referenced

402.2.2.7.1 Explosive material classification analogy shall be based on a single tested explosive material classified item. In other words, analogies shall not be based on other analogies.

402.2.3 The contractor shall identify safety hazards associated with explosive material design, employment, storage and transportation of explosive materials.

402.2.3.1 The contractor shall characterize safety risk for hazards associated with explosive material design, employment, storage and transportation of explosive materials.

402.2.3.2 The contractor shall assess safety risk for hazards associated with explosive material design, employment, storage and transportation of explosive materials.

402.2.3.3 The contractor shall identify potential control methods for hazards associated with explosive material design, employment, storage and transportation of explosive materials.

402.2.3.4 The contractor shall document safety hazards associated with explosive material design, employment, storage and transportation of explosive materials in the HTS.

88-1 FUTURE ACTION: Define unique HTS fields required to EOD related hazards.

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

~~a. Imposition of Task 402. (R)~~

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

~~c. Hazard classification data from similar legacy systems.~~

~~d. Any special data elements or formatting requirements.~~

Commented [PDANUAA878]: Derived for DOD guidance

Commented [PDANUAA879]: 88-1

Commented [PDANUAA880]: Deleted. See 102.3 rationale.

TASK 403
EXPLOSIVE ORDNANCE DISPOSAL DATA

403.1 Purpose. Task 403 is to provide Explosive Ordnance Disposal (EOD) source data, recommended render-safe procedures, and disposal considerations. Task 403 also includes, but not limited to, the provision of test items for use in new or modified weapons systems, explosive ordnance evaluations, aircraft systems, and unmanned systems.

403.1.1 Such documentation is required for the development/acquisition of new/modified explosives, the associated packaging, or commodities containing explosives/energetics.

403.1.2 For the purpose of this task explosive materials include all articles containing energetic devices/materials.

89-1 Does this need to be expanded to specifically address insensitive muntions?

403.2 Task description. The contractor shall~~:~~ develop explosive ordnance disposal data for new explosive materials.

403.2.1 Scope: Explosive ordnance disposal data is required for all new explosive materials and device configuration containing explosive materials.

403.2.1.1 The contractor shall consider employment, storage, and transportation when developing explosive ordnance disposal data.

403.2.1.2 Typically, the program developing the new explosive material or a new configuration containing explosive material is responsible for obtaining explosive ordnance disposal data.

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

403.2.2 The contractor shall provide detailed source data on explosive ordnance design functioning and safety so that proper EOD tools, equipment, and procedures can be developed, validated and verified.

403.2.3 The contractor shall coordinate explosive ordnance disposal with Naval Explosive Ordnance Disposal Technology Division during design development.

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

403.2.4 The contractor shall recommend courses of action that EOD personnel can take to render safe and dispose of explosive ordnance.

Commented [PDANUAA881]: These are examples and are not an inclusive list.

Commented [PDANUAA882]: Rather that have the task continuously refer to explosives/energetics, this para defines to intent so the rest of the task verbiage can be presented in a more straightforward manner.
89-1

Commented [PDANUAA883]: Scope added to define when this task is needed.

Commented [PDANUAA884]: This is a key aspect of how system safety affects design and has been overlooked

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

403.2.5 The contractor shall provide test ordnance for conducting EOD validation and verification testing. The Naval Explosive Ordnance Disposal Technology Division shall assist in establishing quantities and types of assets required.

403.2.6 The contractor shall identify safety hazards associated with EOD activities.

403.2.6.1 The contractor shall characterize safety risk for hazards associated with EOD activities.

403.2.6.2 The contractor shall assess safety risk for hazards associated with EOD activities.

403.2.6.3 The contractor shall identify potential control methods for hazards associated with EOD activities.

403.2.6.4 The contractor shall document safety hazards associated with EOD activities in the HTS.

Commented [PDANUAA885]: 89-1

89-1 FUTURE ACTION: Define unique HTS fields required to EOD related hazards.

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

Commented [PDANUAA886]: Deleted. See 102.3 rationale.

~~a. Imposition of Task 403. (R)~~

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

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

APPENDIX A

GUIDANCE FOR THE SYSTEM SAFETY EFFORT

Commented [PDANUAA887]: The initial Draft did not directly look at Appendix A or Appendix B as these two appendices are informational only.
Depending on what revisions are included will drive the information presented in Appendices A & B.

The focus of the initial draft was on the content of the requirements in paras 1-6 and subsequent tasks..

A draft Appendix C has been added to provide Level of Rigor (LOR) examples. These examples are deemed necessary due to the persistent confusion concerning exactly what LOR should look like, how it should be documented, and what auditable materials LOR activities generate that can be used to show that LOR activities have been accomplished.

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

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

TABLE A-I. Task application matrix

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

Task Type	***Program Phase***	***Applicability Codes***
ENG – Engineering	*MSA – Materiel Solution Analysis*	*G – Generally Applicable*
MGT – Management	*TD – Technology Development*	*S – Selectively Applicable*
	EMD – Engineering and Manufacturing Development	*GC – Generally Applicable to Design Change*
	P&D – Production and Deployment	*N/A – Not Applicable*
	O&S – Operations and Support	

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

TABLE A-II. Example probability levels

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

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

SOFTWARE SYSTEM SAFETY ENGINEERING AND ANALYSIS

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

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

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

Commented [PDANUAA888]: FUTURE ACTION: Rework Appendix B to reflect para 4.4 revision.

Commented [PDANUAA889]: Note that **(software) system safety risks** are derived via hazard analyses. Hazards identified are based on the realization of system safety risk in the implementation of requirements in the design.

Software development process risks are not the same … they are programmatic risks (e.g. cost, schedule, performance) with safety overtones. Though development process risks may introduce system safety hazards, these development process risks cannot be characterized via design requirement implementation.

LOR activities are used to build assurance that software development processes are not introducing such programmatic risks. Thus, a program needs to define what LOR activities will be applicable. As the program proceeds, each identified criterion is assessed for each unit of software to determine if such software is compliant or not with the LOR criterion.

It is important not to mix these 3 concepts as each is addressing related, but distinctly different purposes.

Commented [PDANUAA890]: FHA not applicable to every program; it is only applicable when the contract requires it.
Therefore, this guidance needs revision

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

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

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

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

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

Commented [PDANUAA891]: FHA not applicable to every program; it is only applicable when the contract requires it.
Therefore, this guidance needs revision

Commented [PDANUAA892]: Insufficient guidance as to what this should entail. See new appendix C

Commented [PDANUAA893]: Very true. But even more to the point is once a SwCI level has been established, there is no mechanism available to reduce the level as is done with Table III and associated hazard controls.

- Ameliorating worst credible potential severity is not the same as ameliorating hazard severity.
- The only way to reduce software control category is to change the underlying software architecture. Even if a program attempted to do so, this approach undermines to underlying reason for using software …

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

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

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

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

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

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

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

Commented [PDANUAA894]: Argument for software safety assurance … to ensure this goal is obtained

Commented [PDANUAA895]: Is the purpose of this para to explain the bottom part of Table V? Many of the topics are covered, but not it a consistent manner.

Commented [PDANUAA896]: What specific activities show this is intent has been met? This comes across as a bunch of "buzz words" without any guidance of how these should be incorporated.
It is the Implementation of these concepts that matters, not that the concept has been considered.
Guidance should be clear enough that different system safety practitioners agree on what this list means and what would be sufficient to prove this intent has been satisfied.

Commented [PDANUAA897]: What specific activities show this is intent has been met? This comes across as a bunch of "buzz words" without any guidance of how these should be incorporated. What specific artifacts are expected?
It is the Implementation of these concepts that matters, not that the concept has been considered. Guidance should be clear enough that different system safety practitioners agree on what this list means and what would be sufficient to prove this intent has been satisfied.

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

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

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

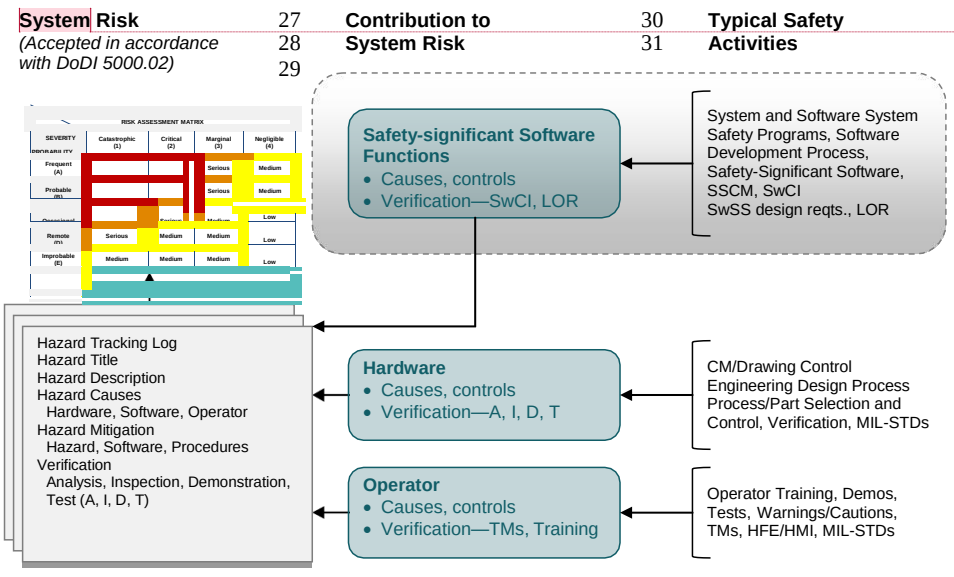


FIGURE B-1. Assessing software's contribution to risk

Commented [PDANUAA898]: What specific activities show this is intent has been met? This comes across as a bunch of "buzz words" without any guidance of how these should be incorporated. What specific artifacts are expected?
It is the Implementation of these concepts that matters, not that the concept has been considered. Guidance should be clear enough that different system safety practitioners agree on what this list means and what would be sufficient to prove this intent has been satisfied.

Commented [PDANUAA899]: Need to rework for standard NDI usage

Commented [PDANUAA900]: ???
This is a circular argument … "after completion of all specific software system safety engineering (hazard?) analyses … information will be integrated into the program hazard analyses"

Commented [PDANUAA901]: There are many issues with this figure.
- It does not address environmental considerations to a hazard.
- Terms not defined in para 3 (CM, HFE, HMI, SwSS, TMs)
- The relationship between the terms is left to the reader to guess at.

Therefore, the figure would need to be reworked.

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

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

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

Commented [PDANUAA902]: Not sure what this table is trying to say. It does not correlate with either Table III or Table VI.
? High risks are ONLY associated with catastrophic or critical hazards???
? Serious risks are ONLY associates with marginal or negligible hazards???
? Reliance on interlocks not adequately addressed. Are these hardware, software, or both?
(There are many more issues here …)

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

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

Appendix C: Examples of Software Level of Rigor Activities

C.1 Overview: This appendix provides a number of examples of Level of Rigor (LOR) activities. These LOR examples are intended to be tailored to meet the needs of the program and, per paragraph 4.4.7.1.4, agreed upon by the following:

a. Procuring Office System Safety
b. Procuring Office Software Development/Testing/Certification Team
c. Contractor System Safety
d. Contractor Software Development/Testing/Certification Team

C.1.1 It is recommended to document the agreed to LOR activities in both the System Safety Program Plan and the Software Development Plan.

C.1.2 The LOR examples are documented in table format with each table dedicated to a program milestone/life cycle phase.

C.1.3 Software is evaluated in units with each unit assigned a software control categories (table IV) that differentiate different complexity levels of software architecture. Likewise, per Figure C1, each unit is assigned AI/Machine Learning categories (TBD table V) that represent different realizations of AI/Machine Learning. From these characterizations, each software unit is assigned a Software Criticality Index (SwCI) per table VI and an TBD AI Criticality Index (AICI) per table VII. The SwCI and AICI, through table VIII, drive corresponding Software LOR and AI/Machine Learning LOR.

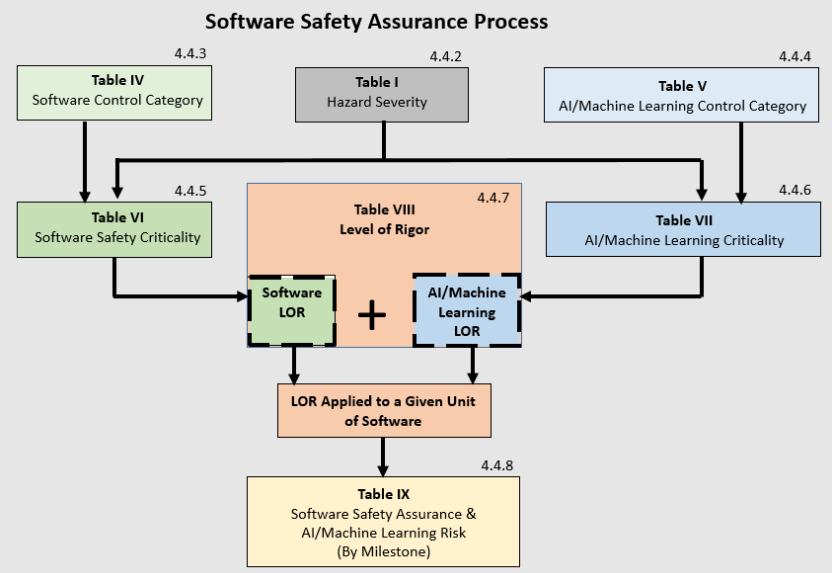


FIGURE C1: Software Safety Assurance Process

Commented [PDANUAA903]: Overview to provide top level perspective of how LOR is derived & context of how it is applied.

Commented [PDANUAA904]: Typically System Program Office (SPO)

Commented [PDANUAA905]: Typically the OEM but could be an organic government capability/office

Commented [PDANUAA906]: Documenting LOR is SSPP provides easy access to the system safety practitioner. Documenting LOR in the SDP provides easy access to the software development/test/certification community

Commented [PDANUAA907]: Summarizing para 4.4 for context

It is important to evaluate each unit of software to derive SwCI/AICI values for that unit. In a sense, these designations drive program costs through identified activities (i.e. required work).
The challenge is to balance the value gained from accomplishing these activities against the cost incurred from doing this work.

Commented [PDANUAA908]: Same as Figure 3 (pg 14b), repeated here for clarity

C.1.4 It is recommended to incorporate LOR compliance assessments into program milestone reviews. This would provide program leadership valuable insight into the health of the software safety assurance effort and allow program leadership to address any shortfalls in LOR compliance.

C.1.5 LOR activities are defined to provide broad, overarching activities derived from best practices and other lessons learned.

C.1.5.1 Defining activities at this level avoids devolving the LOR into the minutia associated with coding standards as coding standards often provide solutions to specific problems. Note this does not prevent a program's coding standards to be stratified against SwCI.

C.1.5.2 The environments the software will be developed in, tested in, and hosted in the final system needs to be established. This "pedigree" (see 4.4.1) permits the system safety practitioner to evaluate changes to the software environment as the program progresses.

C.1.5.3 By definition, after SwCI5/LOR5 has been designated for any software "unit", no further safety requirements are applicable to SwCI5/LOR5 software.

C.1.5.3.1 Exception: Subsequent modifications or hazard analyses may change the identified SwCI & associated LOR and/or AICI & associated LOR, thereby introducing additional LOR activities. In other words, once a hazard has been identified associated with LOR5 software, affected units of software should be revisited and associated LOR revised to LOR1, LOR2, LOR3, or LOR4.

C.1.6 The LOR examples are grouped by program milestones and structured as follows:

a. LOR Activity Title: The activity title and corresponding code. The code is used to link LOR activities across program milestones.

b. LOR Activity Description: A brief explanation of LOR activity. Programs may find it useful to expand this explanation to provide a more detailed explanation of expectations of each LOR activity.

c. LOR Benefits: A brief summary of potential benefits of the LOR activity. This summary provides a basis for system safety and the software development/testing/certification team to evaluate how the activity should be tailored. It is understood that the specific benefits will vary by program. As this entry is included for informational purposes, it is not necessary to include this entry in the tailored LOR listing.

d. LOR Costs/Limitations: A brief summary of potential costs/limitations associated with the LOR activity. This summary provides a basis for system safety and the software development/testing/certification team to evaluate how the activity should be tailored. It is understood that the specific cost/limitations will vary by program. As this entry is included for informational purposes, it is not necessary to include this entry in the tailored LOR listing.

e. LOR Level: Applicable LOR levels are identified for each example.

FUTURE ACTION: Revisit the example LOR activities and reassess LOR levels provided. These LOR levels were based on MIL-STD-882E and need to be revised to reflect the changes in 882F.

Commented [PDANUAA909]: This construct elevates system safety to provide valuable information for program management/decision makers for a program.
Failure to define LOR introduces a programmatic risk that past program software development failures may be repeated.
Failure to complete LOR indicates that the non-complaint LOR activity (derived from past lessons & best practices) – that the program agreed to during planning – introduces a programmatic risk requiring program management/decision maker engagement

Commented [PDANUAA910]: Coding standards are important to develop consistent/ standard code. However, these standards are too far into the weeds to be effectively managed by this construct. Thus, the higher tiered LOR construct highlight critical areas

Commented [PDANUAA911]: Para 4.4.1 lays out the "pedigree" behind the software. This is frequently overlooked – even though it does influence software development. Flaws in the pedigree can result in flawed software.

Commented [PDANUAA912]: SwCI5 ➔ No Safety Impact.
If the unit of software has been determined to be SwCI5, the rationale behind the determination needs to be documented. Issues/Incidents in the future may require revisiting the basis for this determination.
Note: If SwCI5 is changed, then the corresponding LOR activities would then need to be addressed retroactively & thus introduces a programmatic cost/schedule risk to accomplish these previously unplanned activities.

Commented [PDANUAA913]: These Benefits (as well as the corresponding costs/ limitations) are general observations that may or may not be applicable in every case. But it gives the system safety practitioner somewhere to start the dialog with the software development/test/ certification team as to whether or not the example LOR activity is appropriate for the program

Commented [PDANUAA914]: Depending on the system design/architecture and program approach, these levels could be adjusted. The levels indicated in the examples are intended to illustrate how some activities might be assigned to the most critical software while other activities may be needed for (nearly) all software units in question.

NOTE also that in a resource constrained environment, there is a programmatic need to limit LOR activities overall. This is in conflict with the conservative system safety tendency to require more activities to account for potential impacts of unknown. Thus, this level construct provides the basis for balancing/compromising what activities will be incorporated.

C.1.7: LOR content should consider program acquisition strategy, middle tiered acquisition, Agile software, digital engineering, etc.

C.2 Preliminary Design Review (PDR) LOR examples: This section addresses LOR activities that should be completed prior to completion of PDR, corresponding equivalent program event, or when requirements are finalized. The focus is to ensure the foundations of the software safety program are codified and agreed to within the program. Using this framework, software is evaluated in logical "units" and stratified into Software Criticality Index (SwCI). Initial analyses activity of the preliminary design. NOTE that the only mandatory requirement is to assess each unit of software to determine the corresponding SwCI/AICI designation.

Commented [PDANUAA915]: These aspects can alter the baseline acquisition model expectations upon which the following LOR examples have been constructed.
For example, will the LOR activity be accomplished for each Agile software sprint or summarized for the entire Agile software process?

Commented [PDANUAA916]: Included for programs not following the traditional life cycle milestones.

Table C1: PDR Software LOR activities

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[A] FHA	Conduct Functional Hazard Analyses (Task 208) NOTE: Applicable if placed on contract with OEM	• Insight into how safety critical functions are realized in the software • Needed for Airworthiness SCFTA requirement	• Dependent on maturity of requirements • Economical need to limit number of functions • Economical need to bound functions	**1**
[AW] Safety Critical Requirement Review	Review safety critical requirements for completeness	• Establish solid safety requirement foundation • Ensures safety critical requirement gaps are identified and filled • Best Practice	• Manpower • Rework as required due to requirement evolution/ changes	**1, 2**
[B] Safety Requirement/ Hazard Map	Map SCI (Catastrophic/ Critical) requirements to associated hazards	• Positive hazard control requirement transfer to design • Requirement validation easier at end of program	• Manpower • Requires comprehensive SCI requirement listing	**1, 2, 3**
[B1] Safety Requirement/ Function Map	Map safety requirements to functions & into views of system & software architecture	• Positive requirement transfer to design • Requirement validation easier at end of program	• Manpower • Open ended activity unless set of limited functions is defined and agreed to	**1, 2, 3**
[C] Identify NDI Software	Identify proposed NDI (e.g. COTS, GOTS, REUSE, etc) NDI software to be incorporated into the design. Evaluate proposed environment (vs environment NDI software originally designed to operate in)	• Permits early evaluation of NDI software usage in design to ensure further (costly) modifications will not be needed • Screens inappropriate use of NDI software	• Manpower • Effort required counters perception that NDI software is cheaper to procure • Do not have insight into NDI logic, therefore must treat NDI software as a "Black Box"	**1, 2, 3**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[K] Identify Software-Like-Hardware	In the Software Development Plan (SDP), codify how Software-like-Hardware will be addressed. Evaluate hardware devices incorporating Software-like-Hardware logic for safety issues	• Screens inappropriate use • Ensures software or Software-like-Hardware logic implementation is consistent throughout the system	• Pushback not to evaluate Software-like-Hardware (*example: firmware is not "real" software so software safety rules should not apply*)	**1, 2, 3**
[T] Fault Tolerant Design Criteria	Define fault tolerant design requirements/ criteria	• Establishes fault tolerant design requirements	• Adds complexity to code	**1, 2, 3**
[AO] Response to Transient Conditions	Investigates system response to transient conditions	• Ensure robustness in design to address: o Power Transients o Transients between operating modes	• Added complexity to design	**1, 2, 3**
[D] Assess Software Engineering Environment for Appropriateness	Verify software development, test, and certification environments (tools, autocode tools, compilers, linkers, etc) are appropriate and documented for level of software	• Documents safety rationale of why environment/tools are appropriate for SwCI level of software. • Ensures SSE is involved in software development community early • Best Practice	• Manpower/Expertise	**1, 2, 3, 4**
[E] Coding Standards	Verify coding standards are appropriate for each LOR and agreed to by all parties. Verify coding guidelines have been defined and agreed to	• Ensures no disconnects in LOR and standard practices o Fault Tolerant Design o Validated and Controlled Interfaces at all times	• Manpower/Expertise	**1, 2, 3, 4**
[F] SRHA	Conduct System Requirements Hazard Analyses – SRHA (Task 203) NOTE: Applicable if placed on contract with OEM	• Needed for LOR1 software for Airworthiness • Feeds SwCI determination • Can use to prioritize future software builds	• Dependent on maturity of requirements. Completed before requirement solidification results in iterative analyses	**1, 2, 3, 4**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[AL] Design Order of Precedence	Verify Design Order of Precedence (4.3.4.1) integrated into the software development Plan (SDP)/process	• Consistent system safety hazard control philosophy	• Pushback against system safety philosophy as being too restrictive	**1, 2, 3, 4**
[AM] Safety Requirement Peer Review	System Safety participation in software peer reviews, particularly those reviews addressing safety requirements/ features used to control hazards	• System Safety advocacy for coding options that avoid introducing hazards • Software peer reviews provide a means to verify software features have been implemented. This would be evidence for validating the control of hazards	• Manning • Organizational Structure • Time	**1, 2, 3, 4**
[AP] Response to Transient Conditions	Analyze system response to system transients	• Better understanding of system robustness with respect to electrical transients • Better understanding of system robustness with respect to operating mode transients	• Manning	**1, 2, 3, 4**
[AS] Software Partitioning	Partition software for each LOR level as much as practicable from the rest of the software	• Focuses critical code into core modules thereby reducing hazard analyses efforts • Reduces overall LOR requirement flow-down.	• Manning • Configuration control impacts. The lower the LOR, the more partitions requiring configuration tracking	**1, 2, 3, 4**
[G] Assess SwCI for Each Unit of Software *****Mandatory Activity*****	Determine how software will be managed. Assess each "unit" (CSCI, CSC, CSU levels – program needs to specify) against Tables I, IV, & VI to determine SwCI and associated LOR Levels. Severity based on worst credible issue that could be associated with the software. **NOTE:** This is appropriate for all software. Need to document any SwCI5 = LOR 5 "unit"	• Scopes the safety involvement in the software development process • Establishes safety pedigree • Aids in understanding functional threads through the larger software program	• Requires analyses to assess each "unit" of software • Large or complicated architectures may require FHA (Task 208) to provide consistent framework to assess.	**1, 2, 3, 4, 5**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[H] Define and Codify LOR	Define LOR criteria for SwCI/LOR levels and Life Cycle Phases. Codified in the SSPP and SDP. NOTE: Correlate with existing SDP requirements. Take credit for activities already being done.	• Addresses paragraph 4.4 requirement • Answers Table IX, question "Has the Level of Rigor been defined"? • Laying out requirements early can positively influence both design architecture and software process choices	• Manpower/Expertise	**1, 2, 3, 4, 5**
[I] PHL	Conduct PHL (Task 201) NOTE: Applicable if placed on contract with OEM	• Provides early list of potential hazardous areas that involve software • Feeder to SwCI determination • Feeds PHA	• Manpower/Expertise	**1, 2, 3, 4, 5**
[J] PHA	Conduct PHA (Task 202) NOTE: Applicable if placed on contract with OEM	• Generates preliminary list of hazards • Feeds subsequent hazard analyses tasks that involve software • Feeder to SwCI determination	• Initial analysis based on incomplete and evolving design	**1, 2, 3, 4, 5**
[AR] SDP	System Safety formal coordination on SDP requires.	• Ensure LOR activities are codified in SDP (and also in the SSPP) • Baseline expectations	• Manpower/Expertise	**1, 2, 3, 4, 5**

C.3 Critical Design Review (CDR) LOR examples: This section addresses LOR activities that should be completed prior to completion of CDR, corresponding equivalent program event, or when requirements are finalized. Safety analyses of the software in the evolving design is the focus of this life cycle phase. This provides insight into how the software functions within the larger system. Though all of the 2XX tasks are addressed in the PDR & CDR portions of this LOR table, it is recognized that very few programs will have all of these tasks levied on the OEM. It is important to remember that the LOR is focused on the processes associated with software development, testing, and certification, whereas Task 2XX hazard analyses are focused on how the software functions within the system architecture.

Commented [PDANUAA917]: Included for programs not following the traditional life cycle milestones.

NOTE that the only mandatory requirement is to assess each unit of software to determine the corresponding SwCI/AICI designation.

Table C2: CDR Software LOR activities

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[A1] Revise FHA	Revise Functional Hazard Analyses (Task 208)	• Needed for Airworthiness SCFTA requirement • Revision keeps safety product current and correct with design evolution	• Dependent on maturity of requirements • Economic need to limit number of activities • Economic need to bound functions • Revisions may drive additional cost if LOR increases	**1**
[L] SCFTA	Develop Safety Critical Functional Thread Analysis (SCFTA) for SCFs	• MIL-HNBK-516C Airworthiness activity • Functional logic map is useful for subsequent analyses • Ensures all safety critical logic is identified	• Time/Resource intense • SCFTA must be in limited number of threads and bounded as to how far each thread is mapped to keep this activity economical • Derived from FHA	**1**
[M] Voting Logic	Assess Multi-Channel Cross-Voting Logic	• Ensures voting logic correct; leads to correct system actions	• Detailed logic analysis takes time and resources.	**1, 2**
[AW1] Revised Safety Critical Requirement Review	Review changes to safety critical requirements for completeness.	• Maintains solid safety foundation • Ensures safety critical requirement gaps are identified and filled • Best Practice	• Manpower • Rework as required due to requirement evolution/ changes	**1, 2**
[B1] Revise Safety Requirement/ Function Map	Revise safety requirements map to functions and into views of system and software architecture	• Positive requirement transfer to design • Requirement validation easier at end of program	• Manpower • Open ended activity unless set of limited functions is defined and agreed to	**1, 2, 3**
[B2] Revise Safety Requirement/ Hazard Map	Revise SCI (Catastrophic/ Critical) requirements map to associated hazards as needed	• Positive hazard control requirement transfer to design • Requirement validation easier at end of program	• Manpower • Requires comprehensive SCI requirement listing	**1, 2, 3**
[B4] Safety Requirement/ Design Component Map	Map safety-critical requirements to design components to	• Ensure safety critical requirements properly flow down to the component level of the design	• Manpower	**1, 2, 3**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[C1] Identify NDI SW from Changes to the System	Identify proposed COTS, GOTS, REUSE, and other NDI software changes to be incorporated into the design. Evaluate proposed environment (vs environment NDI software originally designed to operate in)	• Permits early evaluation of COTS/GOTS/REUSE/NDI software to ensure further (costly) modifications will not be needed • Screens inappropriate use	• Manpower • Effort required counters perception that NDI software is cheaper to procure • Do not have insight into NDI logic, therefore must treat NDI software as a "Black Box" • May not have access to what environment NDI software was originally designed to operate in	**1, 2, 3**
[K1] Identify New Software-like-Hardware Introduced from Changes to the System	Evaluate changes to the system to determine if hardware devices incorporating Software-like-Hardware logic have introduced safety issues	• Screens inappropriate use • Ensures software or Software-like-Hardware logic implementation is consistent throughout the system	• Pushback not to evaluate Software-like-Hardware (*example: firmware is not "real" software so software safety rules should not apply*)	**1, 2, 3**
(T1) Fault Identification and Response	Assess fault identification and response scheme.	• Ensures planned fault response & reconfiguration is proper and does not introduce additional safety issues • Identification of fault conditions without prescribed response • Details how is the operator notified of a fault • Assessment of how the identification/response scheme meets fault tolerant design criteria	• Added complexity to code	**1, 2, 3**
[U] Assess Interface Design	Assess Interface design for correctness and completeness	• Ensures Interfaces are correct and do not harbor safety hazards	• Manpower	**1, 2, 3**
[AQ] Faulty Data	Assess software design handling for inappropriate, missing, or unexpected data	• Ensure software is robust enough to properly handle incorrect data	• Manpower	**1, 2, 3**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[D1] **Assess Changes to Software Engineering Environment for Appropriateness**	Assess changes to software development, test, and certification environments (tools, auto-code tools, compilers, linkers, etc) are appropriate and documented for level of software	• Documents safety rationale of why environment/tools are appropriate for SwCI level of software. • Ensures SSE is involved in software development community early • Best Practice	• Manpower/Expertise	**1, 2, 3, 4**
[E1] **Revised Coding Standards**	Verify compliance of revisions to coding standards. Verify coding standards remain appropriate for each LOR and agreement has be renewed	• Validate safety pedigree • Ensures no disconnects in LOR and standard practices o Fault Tolerant Design o Validated and Controlled Interfaces at all times •	• Manpower	**1, 2, 3, 4**
[F1] **Revised SRHA**	Evaluate requirements changes for SRHA revision (Task 203)	• Needed for LOR1 software for Airworthiness • Feeds SwCI determination • Can use to prioritize future builds	• Dependent on maturity of requirements	**1, 2, 3, 4**
[G1] **Assess Hardware/ Software Changes to SwCI designations**	Verify changes to coding guidelines have been defined and agreed to. In addition, verify changes to code has not changed the associated SwCI level of that code	• Scopes the safety involvement in the software development process • Establishes/maintains safety pedigree • Aids in understanding functional threads through the larger software program	• Requires analyses to assess each "unit" of software • Large or complicated architectures may require FHA (Task 208) to provide consistent framework to assess.	**1, 2, 3, 4**
[N] **SSHA**	Conduct Subsystem Hazard Analyses (Task 204) NOTE: Applicable if placed on contract with OEM	• Develop SW related hazards at the subsystem level. • Control options identified.	• Time • Resources	**1, 2, 3, 4**

LOR Activity Title	LOR Activity Description	• LOR Benefits	• LOR Costs/Limitations	LOR Level
[O] SHA	Conduct System Hazard Analysis (Task 205) NOTE: Applicable if placed on contract with OEM	• Develop SW related hazards at the system level. • Control options identified.	• Time • Resources	**1, 2, 3, 4**
[P] O&SHA	Conduct Operating & Support Hazard Analyses (Task 206) NOTE: Applicable if placed on contract with OEM	• Develop SW related hazards from the system level operational and maintenance perspective. • Control options identified.	• Time • Resources	**1, 2, 3, 4**
[Q] HHA	Conduct Health Hazard Analyses (Task 207) NOTE: Applicable if placed on contract with OEM	• Integrates how SW is involved with heal related hazards. • Control options identified	• Time • Resources • Generally applied only when significant health issues are suspected in a system	**1, 2, 3, 4**
[R] SOSHA	Conduct System of System Level Hazard Analysis (Task 209) NOTE: Applicable if placed on contract with OEM	• Provides safety insight into highly complex interacts with many different systems	• Time • Resources • Integrates multiple systems and would generally be beyond scope of a single program office	**1, 2, 3, 4**
[S] EHA	Conduct Environmental Hazard Analyses (Task 210) NOTE: Applicable if placed on contract with OEM	• Investigates how software may influence environmental concerns	• Time • Resources • Scope of activity falls within the environmental domain; therefore generally not levied by system safety	**1, 2, 3, 4**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[V] Review Draft Test Plans to Ensure LOR is Properly Incorporated	Review draft Test Plan to verify LOR 1, 2, 3, & 4 requirements are incorporated	• Verification that testing will incorporate LOR criteria • Test Cases for: o Stress Testing o Stability Testing o Disaster Testing o Exception handling correctness o Interface correctness o Boundary handling correctness (How does the software respond to approaching boundary conditions, landing on the boundary, or operating beyond the boundary?) o Proper Events o Proper Sequencing of Events • Proper Timing	• Resources • Time	**1, 2, 3, 4**
[AK] Mode Mismatch	Evaluation command modes are implemented and identify any mode mismatch	• Ensure seamless transitions between modes of operation • Allows cues to be developed for operator/maintainer to positively know which mode is active at any given time	• Adds code complexity	**1, 2, 3, 4**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[AS1] Software Partitioning	Assess changes to software partitioning for each LOR level as much as practicable from the rest of the software	• Focuses critical code into core modules thereby reducing hazard analyses efforts • Reduces overall LOR requirement flow-down. • Focus is on changes to the software since last phase	• Manning • Configuration control impacts. The lower the LOR, the more partitions requiring configuration tracking	**1, 2, 3, 4**
[H1] Revisions to LOR Definition and Codification	Revisions to LOR criteria defined for SwCI/LOR levels and Life Cycle Phases. Codified in the SSPP and SDP. Note: Correlate with existing SDP requirements. Take credit for activities already being done.	• Addresses 882E para 4.4 requirement • Answers 882E Table 6, question #1 • Laying out requirements early can positively influence design architecture choices	• Manpower/Expertise	**1, 2, 3, 4, 5**
[AR1] SDP Changes	Any change to the approved SDP required System Safety formal coordination	• Maintains agreement of LOR content per para 4.4.7.1.4	• Manpower/Expertise	**1, 2, 3, 4, 5**

C.4 LOR examples prior to formal testing: This section addresses LOR activities that should be completed prior to the beginning of formalized test or equivalent program activity. The activities are focused on ensuring build-up activities leading to formal testing have been completed. Prior phase hazard analyses should be complete. Software test plans should be finalized. It is likely that the design has matured and changed since previous phase LOR activities were accomplished. As such, associated software safety products need to be revised.

Table C3: Software LOR activities prior to formal testing

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[A2] Revise FHA	Revise Functional Hazard Analyses (Task 208)	• Needed for Airworthiness SCFTA requirement • Revision keeps safety product current and correct with design evolution	• Dependent on maturity of requirements • Economical need to limit number of functions • Economical need to bound activities • Revisions may drive additional cost if LOR increases	**1**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[L1] Revise SCFTA	Revise Safety Critical Functional Thread Analysis (SCFTA) for SCFs. Derived from FHA	• MIL-HNBK-516C Airworthiness activity • Functional logic map is useful for subsequent analyses • Ensures all safety critical logic is identified	• Time/Resource intense • Economic need to limit number of SCFTA threads and establish SCFTA boundaries	**1**
[M1] Revised Voting Logic	Assess Revisions to Multi-Channel Cross-Voting Logic	• Ensures revised voting logic correct; leads to correct system actions	• Detailed logic analysis takes time and resources.	**1, 2**
[W] Detailed Code Walkthrough	Perform detailed inspections of code for compliance with LOR, SDP, coding standards, and other program guidelines	• Peer review to ensure software meets intended function • Provides confidence that logic is correct before entering test	• Resources • Time	**1, 2**
[AF] Test Case Review	Review each LOR1 & LOR2 test case	• Ensures critical test points for SwCI 1 & 2 software have been identified and proposed tested will screen characteristics of interest	• Manpower • Time • Additional testing	**1, 2**
[AG] FMET	Review STP incorporates failure modes and effects testing (FMET)	• Ensures FMET coverage is adequately addressed in the STP	• Manpower • Time • Additional testing	**1, 2**
[AG1] FMET Regression Testing	Review STP incorporates regression failure modes and effects testing (FMET)	• Ensures FMET regression coverage is adequately addressed in the STP	• Manpower • Time • Additional testing	**1, 2**
[AH] Marking Code	Within code, mark LOR1 & LOR2 code with the appropriate LOR	• Clear concise comments in the source code makes sustainment & trouble shooting easier	• Manpower	**1, 2**
[AI] Hardware Failure Sensitivity Review	Evaluation/testing of ensure hardware failure sensitivities	• Ensures hardware/system failure modes are understood and accounted for in the design	• Manpower • Additional testing	**1, 2**
[AW2] Revised Safety Critical Requirement Review	Review changes to safety critical requirements for completeness.	• Maintains solid safety foundation • Ensures safety critical requirement gaps are identified and filled • Best Practice	• Manpower • Rework as required due to requirement evolution/ changes	**1, 2**

LOR Activity Title	LOR Activity Description	• LOR Benefits	• LOR Costs/Limitations	LOR Level
[B5] Revised Safety Requirement/ Function Map	Revise safety requirements to functions map & into views of system/software architecture	• Positive requirement transfer to design • Requirement validation easier at end of program • Maintain currency of safety product	• Manpower • Open ended activity unless set of limited functions is defined and agreed to	**1, 2, 3**
[B6] Revised Safety Requirement/ Hazard Map	Revise SCI (Catastrophic/ Critical) requirements map to associated hazards	• Positive hazard control requirement transfer to design • Requirement validation easier at end of program • Maintain currency of safety product	• Manpower • Requires comprehensive SCI requirement listing	**1, 2, 3**
[B7] Revised Safety Requirement/ Design Component Map	Revise safety-critical requirements to design components map	• Ensure safety critical requirements properly flow down to the component level of the design • Maintain currency of safety product	• Manpower	**1, 2, 3**
[B8] Safety Requirements/ Code Map	Map safety-critical-requirements to code	• Ensures safety critical requirement traceability at code level	• Manpower	**1, 2, 3**
[B9] Safety Requirement/ Test Case Map	Map safety-critical requirements & safety-critical test cases	• Aligns safety requirements to safety critical test cases	• Manpower	**1, 2, 3**
[C2] Identify NDI SW from Changes to the System	Identify proposed NDI software changes to be incorporated into the design. Evaluate proposed environment (vs environment NDI software originally designed to operate in)	• Permits early evaluation of NDI software to ensure further (costly) modifications will not be needed • Screens inappropriate use	• Manpower • Effort required counters perception that NDI software is cheaper to procure • Do not have insight into NDI logic, therefore must treat NDI software as a "Black Box"	**1, 2, 3**
[K2] Identify New Software-like-Hardware Introduced from Changes to the System	• HW devices incorporating SW-like-HW logic need to be evaluated to ensure no safety issues are introduced Does SDP specifically address how SW-like-HW will be addressed?	• Ensures logic implementation is consistent	• Pushback not to evaluate (*ex: firmware is not real software so software rules should not apply*)	**1, 2, 3**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[T2] Revised Fault Identification and Response	Assess fault identification and response scheme.	• Ensures planned fault response & reconfiguration is proper and does not introduce additional safety issues • Identification of fault conditions without prescribed response • Details how is the operator notified of a fault • Assessment of how the identification/response scheme meets fault tolerant design criteria	• Added Complexity to the code	**1, 2, 3**
[U1] Assess Revised Interface Design	Assess Revisions to Interface design to ensure correctness and completeness.	• Ensures Revised Interfaces are correct and do not harbor safety hazards • Ensures Test Plans account for functional (software), physical, and human interfaces are under continuous control	• Manpower	**1, 2, 3**
[AC] Fault Contribution Inspection	Perform detailed code inspections for fault contributions	• Rigorous review to identify fault causal factors so that controls can control these causal factors • Verifies redundant fault tolerance features are working correctly	• Resources • Time	**1, 2, 3**
[AJ] Environment Sensitivity Review	Evaluate the system to determine what stressful events need to be tested	• Ensure software is robust within intended environment	• Additional testing	**1, 2, 3**
[AQ1] Faulty Data	Review/revised assessed software design handling of inappropriate, missing, or unexpected data as the result of changes	• Ensure software is robust enough to properly handle incorrect data • Identify test case specifics	• Manpower • Additional Testing	**1, 2, 3**
[AV]	Review problem reporting/defect tracking, change control, and change review activities for safety impact and compliance	• Ensures positive screening of anomalies for safety impacts	• Manpower • Expertise	**1, 2, 3**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[D2] Assess Changes to Software Engineering Environment for Appropriateness	Assess changes to software development, test, and certification environments (tools, auto-code tools, compilers, linkers, etc) are appropriate and documented for level of software	• Documents safety rationale of why environment/tools are appropriate for SwCI level of software. • Ensures SSE is involved in software development community early • Best Practice	• Manpower/Expertise	**1, 2, 3, 4**
[E2] Revised Coding Standards	Verify compliance of revisions to coding standards. Verify coding standards remain appropriate for each LOR and agreement has be renewed	• Ensures no disconnects in LOR and standard practices	• Manpower	**1, 2, 3, 4**
[F2] Revised SRHA	Evaluate requirement changes for SRHA revision (Task 203)	• Needed for LOR1 software for Airworthiness • Feeds SwCI determination • Can use to prioritize future builds •	• Dependent on maturity of requirements	**1, 2, 3, 4**
[N1] Revise SSHA	Revise Subsystem Hazard Analyses (Task 204) NOTE: Applicable if task placed on contract with OEM	• Mature SW related hazards • Verify control implementation •	• Time • Resources	**1, 2, 3, 4**
[O1] Revise SHA	Revise System Hazard Analysis (Task 205) NOTE: Applicable if task placed on contract with OEM	• Mature SW related hazards • Verify control implementation •	• Time • Resources	**1, 2, 3, 4**
[P1] O&SHA	Revise Operating & Support Hazard Analyses (Task 206) NOTE: Applicable if task placed on contract with OEM	• Mature SW related hazards • Verify control implementation •	• Time • Resources	**1, 2, 3, 4**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[Q1] HHA	Revise Health Hazard Analyses (Task 207) NOTE: Applicable if task placed on contract with OEM	• Mature SW related hazards • Verify control implementation	• Time • Resources	**1, 2, 3, 4**
[R1] SOSHA	Revise System of System Level Hazard Analysis (Task 209) NOTE: Applicable if task placed on contract with OEM	• Provides safety insight into highly complex interacts with many different systems • Mature SW related hazards • Verify control implementation	• Time • Resources • Integrates multiple systems and would generally be beyond scope of a single program office	**1, 2, 3, 4**
[S1] EHA	Revise Environmental Hazard Analyses (Task 210) NOTE: Applicable if task placed on contract with OEM	• Investigates how software may influence environmental concerns • Mature SW related hazards • Verify control implementation	• Time • Resources • Scope of activity falls within the environmental domain; therefore generally not levied by system safety	**1, 2, 3, 4**
[V1] Test Plan LOR Input	Review Test Plan to verify LOR 1, 2, 3, & 4 requirements are incorporated into the software test plan	• Verification that testing will incorporate LOR criteria • Test Cases for: o Stress Testing o Stability Testing o Disaster Testing o Exception handling correctness o Interface correctness o Boundary handling correctness (How does the software respond to approaching boundary conditions, landing on the boundary, or operating beyond the boundary?) o Proper Events o Proper Sequencing of Events • Proper Timing	• Resources • Time	**1, 2, 3, 4**
[X] Label Test Cases with LOR	Ensure test cases within the STP are marked with the appropriate LOR they support	• Provides traceability between LOR and STP	• Manning	**1, 2, 3, 4**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[Y] System Safety Risk Acceptance	System Safety risk (after control) acceptance accomplished prior to formal test or first use … and if safety risks are not accepted?	• Active safety management or emerging software related issues	• Tight timeline from when an issue is first validated to when risk acceptance package needs to be formally accepted. May result in "out of cycle" safety risk acceptance actions. • Identification of a safety issue resulting from an anomaly held hostage to anomaly correction prioritization	**1, 2, 3, 4**
[AE] Fault Injection Testing	Add fault injection test cases to formal test plans.	• Stress tests software to ensure proper execution when faults are present.	• Resources • Time	**1, 2, 3, 4**
[AK1] Revise Mode Mismatch	Evaluation changes to ensure proper command modes are implemented. Any mode mismatch identified	• Ensure seamless transitions between modes of operation • Allows cues to be developed for operator/maintainer to positively know which mode is active at any given time	• Adds code complexity	**1, 2, 3, 4**
[AN] Information Latency & Inadvertent/ Failure to Properly Display Information	Evaluate system to determine if latent data issues exist. Likewise, Inadvertent/Failure to properly display information shall be evaluated.	• Better Understanding of code execution • Identification of potential hazards/safety concerns	• Manpower	**1, 2, 3, 4**
[AS2] Software Partitioning Revisions	Assess changes to software partitioning for each LOR level as much as practicable from the rest of the software	• Focuses critical code into core modules thereby reducing hazard analyses efforts • Reduces overall LOR requirement flow-down. • Focus is on changes to the software since last phase	• Manning • Configuration control impacts. The lower the LOR, the more partitions requiring configuration tracking	**1, 2, 3, 4**
[AT] SW Only Preforms Intended Functions	Verify no extraneous functions are incorporated into the SW	• Ensures coded functions meet requirements	• Manpower	**1, 2, 3, 4**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[AU] Extraneous or Dead (or Intentionally Deactivated) Code	Analyze code for extraneous or Dead Code	• Ensures deterministic execution. Extraneous/Dead Code, if present and mistakenly executed, would result in non-deterministic execution	• Manpower/Expertise	**1, 2, 3, 4**
[G2] Assess HW/SW Changes to SwCI Designations *****Mandatory Activity*****	Review HW and SW changes to determine if there are impacts to previous SwCI designations NOTE: This is appropriate for all changes. Need to document any SwCI5 = LOR 5 criteria.	• Scopes the safety involvement in the software development process • Establishes safety pedigree • Aids in understanding functional threads through the larger software program	• Requires analyses to assess changes to each "unit" of software • Large or complicated architectures may require FHA (Task 208) to provide consistent framework to assess.	**1, 2, 3, 4, 5**
[H2] Revisions to LOR Definition and Codification	Revisions to LOR criteria defined for SwCI/LOR levels and Life Cycle Phases. Codified in the SSPP and SDP. Note: Correlate with existing SDP requirements. Take credit for activities already being done.	• Addresses 882E para 4.4 requirement • Answers 882E Table 6, question #1 • Laying out requirements early can positively influence design architecture choices	• Manpower/Expertise	**1, 2, 3, 4, 5**
[AR2] SDP Changes	Any change to the approved SDP required System Safety formal coordination	• Ensure LOR activities are codified in SDP (and also in the SSPP) • Baseline expectations	• Manpower/Expertise	**1, 2, 3, 4, 5**

C.5 LOR examples prior to fielding: This section addresses LOR activities that should be completed prior to fielding or corresponding equivalent program event. The focus is on ensuring formal testing and IV&V activities required to be completed. In addition, ensuring build-up activities leading to fielding have been completed. Prior phase hazard analyses should be complete. It is likely that the design has matured and changed since previous phase LOR activities were accomplished. As such, associated software safety products need to be revised.

Commented [PDANUAA918]: Included for programs not following the traditional life cycle milestones.

Table C4: Software LOR activities prior to Fielding

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[A3] Revise FHA	Revise Functional Hazard Analyses (Task 208)	• Needed for Airworthiness SCFTA requirement • Revision keeps safety product current and correct with design evolution	• Dependent on maturity of requirements • Economical need to limit number of activities • Economic need to bound activities • Revisions may drive additional cost if LOR increases	**1**
[L2] Revise SCFTA	Revise Safety Critical Functional Thread Analysis (SCFTA) for SCFs. Derived from FHA	• MIL-HNBK-516C Airworthiness activities • Functional logic map is useful for subsequent analyses • Ensures all safety critical logic is identified	• Time/Resource intense • Economic need to limit number of SCFTA threads and establish SCFTA boundaries	**1**
[AA] 100% Regression Testing	Perform 100% regression testing on all LOR-1 software that is changed	• Builds confidence of deterministic execution • Verifies execution of each change to the software	• Resources • SIL resources • Time	**1**
[M2] Revised Voting Logic	Assess Revisions to Multi-Channel Cross-Voting Logic	• Ensures revised voting logic correct; leads to correct system actions	• Detailed logic analysis takes time and resources.	**1, 2**
[Z] 100% Branch Code Testing	Ensure every possible software branch is executed at least once during testing NOTE: This does not mean every combination of branches are tested	• Builds confidence of deterministic execution • Verifies execution of complete decision coverage of code. • Identifies code not tested as DEAD code	• Resources • SIL resources • Time	**1, 2**
[AG2] FMET Results	Review results from STP to failure modes and effects testing (FMET)	• Verification of proper response to software failure modes	• Manpower	**1, 2**
[AG3] FMET Regression Results	Review results from the STP from regression FMET	• Verification of proper response to software failure modes	• Manpower	**1, 2**
[AH-1] Marking Code Revisions	Within code, mark changes to LOR1 and LOR2 code with the appropriate LOR	• Clear concise comments in the source code makes sustainment & trouble shooting easier	• Manpower	**1, 2**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[AI-1] Hardware Failure Sensitivity Review	Review hardware failure sensitivities for safety issues	• Ensures hardware/system failure modes are understood and accounted for in the design	• Manpower • Additional testing	**1, 2**
[AW3] Revised Safety Critical Requirement Review	Review changes to safety critical requirements for completeness.	• Maintains solid safety foundation • Ensures safety critical requirement gaps are identified and filled • Best Practice	• Manpower • Rework as required due to requirement evolution/ changes	**1, 2**
[AX] Witness Test Execution	Independently witness the execution of Safety-Critical unit tests	• Witnessing critical tests provides independent confirmation of proper test execution.	• Resources • Time	**1, 2**
[B11] Review Safety Mapping	Review previously developed traceability maps for coverage and completeness. Update as required	• Reviews maps and test results • Maintains currency of safety products	• Manpower	**1, 2, 3**
[C3] Identify NDI SW	Identify proposed NDI software changes to be incorporated into the design. Evaluate proposed environment (vs environment software originally designed to operate in)	• Permits early evaluation of NDI software to ensure further (costly) modifications will not be needed • Screens inappropriate use	• Manpower • Effort required counters perception that NDI software is cheaper to procure • Do not have insight into NDI logic, therefore must treat NDI software as a "Black Box"	**1, 2, 3**
[K3] Identify Software-like-Hardware	• HW devices incorporating SW-like-HW logic need to be evaluated to ensure no safety issues are introduced Does SDP specifically address how SW-like-HW will be addressed?	• Ensures logic implementation is consistent throughout the system	• Pushback not to evaluate (*ex: firmware is not real software so software rules should not apply*)	**1, 2, 3**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[T3] Revised Fault Identification and Response	Assess fault identification and response scheme.	• Ensures planned fault response & reconfiguration is proper and does not introduce additional safety issues • Identification of fault conditions without prescribed response • Details how is the operator notified of a fault • Assessment of how the identification/response scheme meets fault tolerant design criteria	• Added Complexity to the code	**1, 2, 3**
[U2] Assess Revised Interface Design	Assess Revised Interface design to ensure correctness & completeness	• Ensures Revised Interfaces are correct & do not harbor safety hazards	• Manpower	**1, 2, 3**
[AB] Software Certification	Participate in post-test acceptance review/ certification of safety-critical code	• Ensures Safety criterion has been met before software is certified	• Manpower	**1, 2, 3**
[AJ1] Adverse Environment Sensitivity Review	Evaluate testing to ensure software in the system is responding properly to events. *Any improper or wrong events noted requires additional hazard analyses and testing to ensure no safety hazards result.*	• Evaluate the system to determine what stressful events need to be tested	• Software may not be robust within intended environment • Additional testing	**1, 2, 3**
[AQ2] Faulty Data	Review/revised assessed software design handling of inappropriate, missing, or unexpected data	• Ensure software is robust enough to properly handle incorrect data to add test cases	• Manpower • Additional Testing	**1, 2, 3**
[AV1] Defect Tracking	Review problem reporting/defect tracking, change control, & change review activities for safety impact and compliance	• Identifies emerging safety issues associated with software	• Manning	**1, 2, 3**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[D3] Assess Changes to Software Environment for Appropriateness	Ensure changes to software development, test, and certification environments (tools, autocode tools, compilers, linkers, etc) are appropriate and documented for level of software	• Documents safety rationale of why environment/tools are appropriate for SwCI level of software. • Ensures SSE is involved in software development community early • Best Practice	• Manpower/Expertise	**1, 2, 3, 4**
[E3] Revised Coding Standards	Ensure coding standards are appropriate for each LOR & agreed to by all parties	• Ensures no disconnects in LOR and standard practices	• Manpower	**1, 2, 3, 4**
[F3] Revised SRHA	Evaluate requirements changes for SRHA revision (Task 203) NOTE: Applicable if task placed on contract with OEM	• Needed for LOR1 software for Airworthiness • Feeds SwCI determination • Can use to prioritize future builds	• Dependent on maturity of requirements	**1, 2, 3, 4**
[N2] Revise SSHA	Revise Subsystem Hazard Analyses (Task 204) NOTE: Applicable if task placed on contract with OEM	• Mature SW related hazards • Verify control implementation	• Time • Resources	**1, 2, 3, 4**
[O2] Revise SHA	Revise System Hazard Analysis (Task 205) NOTE: Applicable if task placed on contract with OEM	• Mature SW related hazards • Verify control implementation	• Time • Resources	**1, 2, 3, 4**
[P2] Revise O&SHA	Revise Operating & Support Hazard Analyses (Task 206) NOTE: Applicable if task placed on contract with OEM	• Mature SW related hazards • Verify control implementation	• Time • Resources	**1, 2, 3, 4**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[Q2] Revise HHA	Revise Environmental Hazard Analyses (Task 210) NOTE: Applicable if task placed on contract	• Mature SW related hazards • Verify control implementation	• Time • Resources Verification of proper response to software failure modes • Manpower contract with OEM	**1, 2, 3, 4**
[R2] SOSHA	Revise System of System Level Hazard Analysis (Task 209) NOTE: Applicable if task placed on contract with OEM	• Provides safety insight into highly complex interacts with many different systems • Mature SW related hazards • Verify control implementation	• Time • Resources • Integrates multiple systems and would generally be beyond scope of a single program office	**1, 2, 3, 4**
[S2] EHA	Revise Environmental Hazard Analyses (Task 210) NOTE: Applicable if task placed on contract with OEM	• Investigates how software may influence environmental concerns • Mature SW related hazards • Verify control implementation •	• Time • Resources • Scope of activity falls within the environmental domain; therefore generally not levied by system safety	**1, 2, 3, 4**
[V2] Test Report Review	Review/approve tests results and verify that the tests provide the required LOR test coverage and were executed in compliance with the test plan. Safety Critical features validated.	• Formal artifact to be used with Airworthiness • Validate planned test coverage completed. • Test failure and/or anomalies identified for further evaluation	• Resources	**1, 2, 3, 4**
[Y] System Safety Risk Acceptance	MIL-STD-882E System Safety risk (after control) acceptance accomplished prior to formal test or first use … and if safety risks are not accepted?	• Active safety management or emerging software related issues	• Tight timeline from when an issue is first validated to when risk acceptance package needs to be formally accepted. May result in "out of cycle" safety risk acceptance actions. • Identification of a safety issue resulting from an anomaly held hostage to anomaly correction prioritization	**1, 2, 3, 4**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[Z] Tailored Branch Code Testing Results	Verify select software branches are executed at least once during testing NOTE: This does not mean every combination of branches are tested	• Builds confidence of deterministic execution • Verifies execution of complete decision coverage of code. • Identifies code not tested as DEAD code	• Resources • SIL resources • Time	**1, 2, 3, 4**
[AC1] Software Anomaly Evaluation	Safety evaluation of software anomalies and defects during testing & fielding NOTE: SW anomalies can be noted prior to formalized (vs informal desktop testing) test activities	• Safety better integrated into software development process • Safety can promptly engage in software anomalies with safety impact to determine other system impacts as well as define control strategies. Results may drive additional Safety Analyses • Best Practice	• Safety needs to dedicate time to routinely evaluate software anomalies	**1, 2, 3, 4**
[AD] Tailored Regression Testing	Made against changes to a "chuck" of software. Policy needs to define which tests are required to be repeated for any change in the software. Policy needs to be formally coordinated with System Safety and codified in STP (1) Establish policy before testing begins Assess Each change	• Builds confidence of deterministic execution • Verifies execution of each change to the software	• Resources • SIL resources • Time	**1, 2, 3, 4**
[AE1] Fault Injection Testing Results	Review test results for fault injection test cases. Did software behave as expected?	• Stress tests software to ensure proper execution when faults are present.	• Resources • Time	**1, 2, 3, 4**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[AK2] Mode Mismatch	Evaluate testing to ensure proper command modes are implemented. Any mode mismatch identified	• Ensure seamless transitions between modes of operation • Allows cues to be developed for operator/maintainer to positively know which mode is active at any given time	• Adds code complexity	**1, 2, 3, 4**
[AN1] Information Latency & Inadvertent/ Failure to Properly Display Information	Evaluate system to determine if latent data issues exist. Likewise, Inadvertent/Failure to properly display information shall be evaluated.	• Ensures proper data displayed to operator/maintainer • Identification of hazards	• Manpower/Resources	**1, 2, 3, 4**
[AS3] Software Partitioning	Each LOR level SW shall be partitioned as much as practicable for the rest of the SW	• Focuses critical code into core modules thereby reducing hazard analyses efforts • Reduces overall LOR requirement flow-down. • Focus is on changes to the software since last phase	• Manning • Configuration control impacts. The lower the LOR, the more partitions requiring configuration tracking •	**1, 2, 3, 4**
[AT1] SW only Preforms Intended Functions	No extraneous functions incorporated into the SW as the result of a change	• Ensures coded functions meet requirements	• Manpower	**1, 2, 3, 4**
[AU2] Extraneous or Dead (or Intentionally Deactivated) Code	Analyze changes to code for extraneous or Dead Code	• Ensures deterministic execution. Extraneous/Dead Code, if present and mistakenly executed, would result in non-deterministic execution	• Manpower/Expertise	**1, 2, 3, 4**
[G3] Assess Hardware/ Software Changes to SwCI Designations *****Mandatory Activity*****	Review HW and SW changes to determine if there are impacts to previous SwCI designations NOTE: This is appropriate for all changes. Need to document any SwCI5 = LOR 5 criteria.	• Identifies changes in scope of safety involvement in the software development process • Maintains currency and correctness of SwCI documentation	• Requires analyses to assess changes to each "unit" of software • Large or complicated architectures may require FHA (Task 208) to provide consistent framework to assess.	**1, 2, 3, 4, 5**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[G3] **Assess HW/SW Changes to SwCI Designations** *****Mandatory Activity*****	Review HW and SW changes to determine if there are impacts to previous SwCI designations NOTE: This is appropriate for all changes. Need to document any SwCI5 = LOR 5 criteria.	• Scopes the safety involvement in the software development process • Establishes safety pedigree • Aids in understanding functional threads through the larger software program	• Requires analyses to assess changes to each "unit" of software • Large or complicated architectures may require FHA (Task 208) to provide consistent framework to assess.	**1, 2, 3, 4, 5**
[H3] **Revisions to LOR Definition and Codification**	Revisions to LOR criteria defined for SwCI/LOR levels and Life Cycle Phases. Codified in the SSPP and SDP. NOTE: Correlate with existing SDP requirements. Take credit for activities already being done.	• Addresses 882E para 4.4 requirement • Answers 882E Table 6, question #1 • Laying out requirements early can positively influence design architecture choices	• Manpower/Expertise	**1, 2, 3, 4, 5**
[AR3] **SDP Changes**	Any change to the approved SDP required System Safety formal coordination	• Ensure LOR activities are codified in SDP (and also in the SSPP) • Baseline expectations	• Manpower/Expertise	**1, 2, 3, 4, 5**

C.6 LOR examples in sustainment.

By definition, the following activities are to be periodically (every 5 years) completed during Sustainment.

Table C5: Software LOR activities during Sustainment

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[A4] **Revise FHA**	Revise Functional Hazard Analyses (Task 208)	• Needed for Airworthiness SCFTA requirement • Revision keeps safety product current and correct with design evolution	• Dependent on maturity of requirements • Economical need to limit number of activities • Economic need to bound activities • Revisions may drive additional cost if LOR increases	**1**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[L3] Revise SCFTA	Revise Safety Critical Functional Thread Analysis (SCFTA) for SCFs. Derived from FHA	• MIL-HNBK-516C Airworthiness activities • Functional logic map is useful for subsequent analyses • Ensures all safety critical logic is identified	• Time/Resource intense • SCFTA must be in limited number of threads and bounded as to how far each thread is mapped to keep this activity economical	**1**
[M3] Revised Voting Logic	Assess Revisions to Multi-Channel Cross-Voting Logic	• Ensures revised voting logic correct; leads to correct system actions	• Detailed logic analysis takes time and resources.	**1, 2**
[AW4] Revised Safety Critical Requirement Review	Review changes to safety critical requirements for completeness.	• Maintains solid safety foundation • Ensures safety critical requirement gaps are identified and filled • Best Practice	• Manpower • Rework as required due to requirement evolution/ changes	**1, 2**
[B11] Review Safety Mapping	Review previously developed traceability maps for coverage and completeness. Update as required	• Reviews maps and test results • Maintains currency of safety products	• Manpower	**1, 2, 3**
[C4] Identify NDI SW	Identify proposed NDI software changes to be incorporated into the design. Evaluate proposed environment (vs environment software originally designed to operate in)	• Permits early evaluation of NDI software to ensure further (costly) modifications will not be needed • Screens inappropriate use	• Manpower • Effort required counters perception that NDI software is cheaper to procure • Do not have insight into NDI logic, therefore must treat NDI software as a "Black Box"	**1, 2, 3**
[K4] Identify Software-like-Hardware	• HW devices incorporating SW-like-HW logic need to be evaluated to ensure no safety issues are introduced • Does SDP specifically address how SW-like-HW will be addressed?	• Ensures logic implementation is consistent	• Pushback not to evaluate (*ex: firmware is not real software so software rules should not apply*)	**1, 2, 3**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[T4] Revised Fault Identification and Response	Assess fault identification and response scheme.	• Ensures planned fault response & reconfiguration is proper and does not introduce additional safety issues • Identification of fault conditions without prescribed response • Details how is the operator notified of a fault • Assessment of how the identification/response scheme meets fault tolerant design criteria	• Added Complexity to the code	**1, 2, 3**
[U3] Assess Revised Interface Design	Assess Revised Interface design to ensure correctness and completeness	• Ensures Revised Interfaces are correct and do not harbor safety hazards	• Manpower	**1, 2, 3**
[AB1] Software Certification Revisions	Participate in revisions to software certifications or previously certified software	• Ensures Safety criterion has been met before software is certified	• Manpower	**1, 2, 3**
[AJ2] Adverse Environment Sensitivity Review	Field surveillance of environmental sensitivity	• Review software performance with respect to (severe) environmental conditions	• Ensure software is robust within intended environment	**1, 2, 3**
[AV-2] Defect Tracking	Review problem reporting/defect tracking, change control, and change review activities for safety impact and compliance	• Identifies emerging safety issues associated with software	• Manning	**1, 2, 3**
[D4] Assess changes to software environment for appropriateness	Ensure changes to software development, test, and certification environments (tools, autocode tools, compilers, linkers, etc) are appropriate and documented for level of software	• Documents safety rationale of why environment/tools are appropriate for SwCI level of software. • Ensures SSE is involved in software development community early • Best Practice	• Manpower/Expertise	**1, 2, 3, 4**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[E4] **Revised Coding Standards**	If coding standards are revised, ensure coding standards are appropriate for each LOR and agreed to by all parties	• Ensures no disconnects in LOR and standard practices o Fault Tolerant Design o Validated and Controlled Interfaces at all times	• Manpower/Expertise	**1, 2, 3, 4**
[F4] **Revised SRHA**	Evaluate requirements changes for SRHA revision (Task 203) NOTE: Applicable is placed on contract with OEM	• Needed for LOR1 software for Airworthiness • Feeds SwCI determination • Can use to prioritize future builds	• Dependent on maturity of requirements	**1, 2, 3, 4**
[N3] **Revise SSHA**	Revise Subsystem Hazard Analyses (Task 204) NOTE: Applicable when placed on contract with OEM	• Mature SW related hazards • Verify control implementation	• Time • Resources	**1, 2, 3, 4**
[O3] **Revise SHA**	Revise System Hazard Analysis (Task 205) NOTE: Applicable when placed on contract with OEM	• Mature SW related hazards • Verify control implementation	• Time • Resources	**1, 2, 3, 4**
[P3] **O&SHA**	Revise Operating & Support Hazard Analyses (Task 206) NOTE: Applicable when placed on contract with OEM	• Mature SW related hazards • Verify control implementation	• Time • Resources	**1, 2, 3, 4**
[Q3] **HHA**	Revise Environmental Hazard Analyses (Task 210) NOTE: Applicable when placed on c•	• Mature SW related hazards • Verify control implementation	• Time • Resources Verification of proper response to software failure modes Manpower contract with OEM	**1, 2, 3, 4**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[R3] SOSHA	Revise System of System Level Hazard Analysis (Task 209) NOTE: Applicable when placed on contract with OEM	• Mature SW related hazards • Verify control implementation	• Time • Resources	**1, 2, 3, 4**
[S2] EHA	Revise Environmental Hazard Analyses (Task 210) NOTE: Applicable when placed on contract with OEM	• Investigates how software may influence environmental concerns • Mature SW related hazards • Verify control implementation	• Time • Resources • Scope of activity falls within the environmental domain; therefore generally not levied by system safety	**1, 2, 3, 4**
[AC2] Software Anomaly Evaluation	Safety evaluation of software anomalies and defects during testing & fielding	• Safety better integrated into software development process • Safety can promptly engage in software anomalies with safety impact to determine other system impacts as well as define control strategies. Results may drive additional Safety Analyses • Best Practice	• Safety needs to dedicate time to routinely evaluate software anomalies	**1, 2, 3, 4**
[AK3] Mode Mismatch	Evaluate testing to ensure proper command modes are implemented. Any mode mismatch identified	• Ensure seamless transitions between modes of operation • Allows cues to be developed for operator/maintainer to positively know which mode is active at any given time	• Adds code complexity	**1, 2, 3, 4**
[AN2] Information Latency & Inadvertent/ Failure to Properly Display Information	Evaluate system to determine if latent data issues exist. Likewise, Inadvertent/Failure to properly display information shall be evaluated.	• Ensures proper data displayed to operator/maintainer • Identification of hazards	• Manpower/Resourses	**1, 2, 3, 4**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[AS4] Software Partitioning	Each LOR level SW shall be partitioned as much as practicable for the rest of the SW	• Focuses critical code into core modules thereby reducing hazard analyses efforts • Reduces overall LOR requirement flow-down. • Focus is on changes to the software since last phase	• Manning • Configuration control impacts. The lower the LOR, the more partitions requiring configuration tracking •	**1, 2, 3, 4**
[AT1] SW only Preforms Intended Functions	No extraneous functions incorporated into the SW as the result of a change	• Ensures coded functions meet requirements	• Manpower	**1, 2, 3, 4**
[AU3] Extraneous or Dead (or Intentionally Deactivated) Code	Extraneous or Dead Code not present in LOR1 or LOR2 designated code	• Ensures deterministic execution. Extraneous/Dead Code, if present and mistakenly executed, would result in non-deterministic execution	• Manpower/Expertise	**1, 2, 3, 4**
[G4] Assess HW/SW Changes to SwCI Designations	Review HW and SW changes to determine if there are impacts to previous SwCI designations NOTE: This is appropriate for all changes. Need to document any SwCI5 = LOR 5 criteria.	• Identifies changes in scope of safety involvement in the software development process • Maintains currency and correctness of SwCI documentation	• Requires analyses to assess changes to each "unit" of software • Large or complicated architectures may require FHA (Task 208) to provide consistent framework to assess.	**1, 2, 3, 4, 5**
[H4] Revisions to LOR Definition and Codification	Revisions to LOR criteria defined for SwCI/LOR levels and Life Cycle Phases. Codified in the SSPP and SDP. NOTE: Correlate with existing SDP requirements. Take credit for activities already being done.	• Addresses 882E para 4.4 requirement • Answers 882E Table 6, question #1 • Laying out requirements early can positively influence design architecture choices	• Manpower/Expertise	**1, 2, 3, 4, 5**
[AR4] SDP Changes	Any change to the approved SDP required System Safety formal coordination	• Ensure LOR activities are codified in SDP (and also in the SSPP) • Baseline expectations	• Manpower/Expertise	**1, 2, 3, 4, 5**

LOR Activity Title	LOR Activity Description	LOR Benefits	LOR Costs/Limitations	LOR Level
[H4] Revisions to LOR Definition and Codification	Revisions to LOR criteria defined for SwCI/LOR levels and Life Cycle Phases. Codified in the SSPP and SDP. Note: Correlate with existing SDP requirements. Take credit for activities already being done.	• Addresses 882E para 4.4 requirement • Answers 882E Table 6, question #1 • Laying out requirements early can positively influence design architecture choices	• Manpower/Expertise	**1, 2, 3, 4, 5**
[AR2] SDP Changes	Any change to the approved SDP required System Safety formal coordination	• Ensure LOR activities are codified in SDP (and also in the SSPP) • Baseline expectations	• Manpower/Expertise	**1, 2, 3, 4, 5**

C.7 PDR AI LOR examples

FUTURE ACTION:
Develop PDR AI LOR examples
Develop Table C6: PDR AI LOR activities

C.8 CDR AI LOR examples

FUTURE ACTION:
Develop CDR AI LOR examples
Develop Table C7: CDR AI LOR activities

C.9 AI LOR examples prior to formal testing

FUTURE ACTION:
Develop formal testing AI LOR examples
Develop Table C8: AI LOR activities prior to formal testing

C.10 AI LOR examples prior to fielding

FUTURE ACTION:
Develop fielding AI LOR examples
Develop Table C9: AI LOR activities prior to Fielding

C.11 AI LOR examples in sustainment

FUTURE ACTION:
Develop sustainment AI LOR examples
Develop Table C10: AI LOR activities during Sustainment

C.12 LOR Activities Summary over the Life Cycle

A. Functional Hazard Analyses (FHA) [also includes A1, A2, A3, & A4]: Conduct FHA per Task 208 (if placed on contract). This analytical activity involved identifying functional threads with safety interest and "mapping" all of the thread components into the system architecture. This is generally accomplished early in the life cycle and often will drive LOR/design requirements. Focus of the FHA is on LOR 1 software. Updates to the FHA **[A1, A2, A3, A4]** are warranted to maintain currency and correctness with the evolving design.

An FHA needs to be accomplished to support Airworthiness Safety Critical Function Thread Analyses (SCFTA) per MIL-HNBK-516C. Significant drawbacks include (1) maintaining a disciplined systematic approach, (2) bounding the number of functions to investigate, (3) bounding the extent of how far each SCF will be mapped.

B. Safety Requirement/Hazard Map [See also B2, B5, B11]: This activity develops traceability between Safety Critical Item (SCI) requirements and identified hazards. This traceability is used by safety, software development/testing/certification team, and airworthiness to ensure positive hazard control requirements have been transferred into the design. This traceability needs to be maintained as additional hazards are identified in the system. This activity is typically accomplished prior to PDR and revised as needed.

B1. Safety Requirement/Functional Map [See also B3, B6, B11]: This activity builds traceability between safety requirements and the system architecture. This is typically accomplished before PDR and revised as needed.

B4. Safety Requirement/Design Component Map: This activity builds traceability between safety requirements and the system architecture. Typically accomplished prior to CDR.

B7. Revise Safety Requirement/Design Component Map: This activity maintains the traceability between safety requirements and the system architecture.

B8. Safety Requirement/Code Map: This activity extend the traceability from prior maps to build traceability between safety requirements and the code.

B9. Safety Requirement/Test Case Map: This activity builds traceability between safety requirements and the test cases.

B10. Review/Revise Safety Mapping [See also B11]: This activity reviews all prior developed safety maps for completeness and correctness before to fielding and revise these maps as necessary.

This activity addresses the *Design* per Tables VI & VII.

C. Safety Requirement/Hazard Map [See also C1, C2, C3, C4]: Any NDI software, such as COTS, GOTS, REUSE, and other NDI software, introduces limitations and complexities into how hazard analyses can be accomplished on that software. Namely, the safety analysist does not have insight into the specific logic employed in NDI software, and as such, is forced to treat NDI software as a "black box" in the analysis.

Often, NDI software is "sold" as a cost avoidance approach. However, such savings can quickly be consumed by additional specialty engineering activities. These savings could also be consumed if modifications to the NDI software are required.

Furthermore, system safety needs to ensure NDI software is used within the same "safety environment" that is was developed. Using NDI in a more critical safety usage would drive a reevaluation of thee software. If the NDI software is modified, it will need to be reevaluated. Also, software changes may affect interfaces with NDI and would also need to be evaluated.

This activity is dependent upon the system complexity, the operating environment the NDI will be used in, and the amount of NDI proposed to be used. As such, this activity is recommended for LOR 1, 2, & 3. In addition, NID would need to be revisited throughout the lifecycle if software changes introduce into the design affect the NDI implementation.

This activity addresses the *Analyses of Requirements* per Tables VI & VII.

D. Assess Software Environment for Appropriateness: Knowledge of the proposed operating environment to ensure the software development/testing/certification environments are appropriate for each level of software. Tools, autocode tools, compilers, linkers, etc are evaluated to ensure safety issues cannot be inserted into the software. Documentation thereof captures the rationale why the environment/tools are appropriate for the SwCI level of the software. Establishing the software development/testing/certification environment (aka pedigree) early provides a foundation the rest of the system safety programs can build upon. Note, it is important that tool settings be documented as well to preserve the deterministic nature of compiled code. This will also help troubleshooting

D1. Assess Changes to Software Environment for Appropriateness [see also D2, D3, D4]: Ensures changes to the software environment are assessed as a program progresses through the life cycle. This review screens for disconnects between LOR and standard practices.

E. Coding Standards: It is acknowledged that each software development organization has their own set of coding standards which governs how that software organization develops software. Review of coding standards to identify which coding standards apply to each LOR level. Verify coding guidelines have been defined and agreed to. This ensures there are no disconnects between the coding standards, LOR, and SDP. Examples include guidance in fault tolerant designs & interfaces requiring validations control at all times.

E1. Revised Coding Standards [See also E2, E3, E4]: Over the course of a program, coding standards may change. Any such changes need to be assessed by safety and findings documented. This maintains a baseline understanding.

F. System Requirements Hazard Analyses (SRHA): Conducted SRHA per Task 203 (if placed on contract). Activity is usually accomplished early in a program life cycle. Requirements are reviewed for safety implications. Results could adjust SwCI and can be used to prioritize future iterations of the software. Needed for LOR1 software. Dependent on requirement maturity.

F1. SRHA Revision [see also F2, F3, F4]: Whenever requirements change throughout the program lifecycle, such changes need to be assessed by safety and findings documented.

G. Assess Software Criticality Index (SwCI) for each portion of software: THIS IS A MANDATORY ACTIVITY. Assess the lowest "unit" (e.g. CSCI, CSC, CSU) of software that will be managed by configuration management. This will provide a ready reference where safety issues reside in the larger software unit. For every such "unit" of software, that software is evaluated against the Software Critical Index (SwCI) criteria as defined in Tables I (hazard severity), IV (software control category), V (AI control category), VI (software criticality), and VII (AI criticality) in. Severity is based on worst credible hazard that could be associated with the software. The SwCI levels drive corresponding LOR levels and associated set of LOR activities. This activity becomes more involved the larger and more complicated as system is. In addition, it is important to have defined how Safety Critical Function boundaries will be addressed and codified.

G1. Assess SwCI for each revised portion of software [See also G2, G3, G4]: As this analysis is initially accomplished on a notional software architecture, revisions to the software architecture require a reassessment to ensure the SwCI for the "unit" of software has not changed.

H. Define and Codify LOR: This corresponds to the first question of Table IX. Establishing the LOR early aids program management in planning. Drawback is understanding the software development process with available expertise early in a program. Suggestion- align existing software development practices to correlate with the LOR.

H1: Revised LOR [See also H2, H3, H4]: Revisions to LOR criteria need to be codified. Safety and the software development/testing/certification community need to agree on such revisions.

I. Preliminary Hazard List (PHL): Conduct PHL per Task 201 (if placed on contract). This activity generates a brainstorming list early in the program life cycle that identifies potential safety issues. This list feeds the SwCI determination. The drawback is it may be more cost effective to start with the Preliminary Hazard Analyses (PHA) Task 202.

J. Preliminary Hazard Analysis (PHA): Conduct PHA per Task 202 (if placed on contract). This activity generates a systematic list of hazards early in the program life cycle

K. Identify Software-Like-Hardware [see also K1, K2, K3, K4]: There are many varieties of hardware-based logical computing devices. Since these devices are hardware-based, many argue that software rules do not apply. Yet, these devices conduct logical operations. Furthermore, debates ensue about how the differences between firmware, programmable logic devices (PLCs), field programmable gate arrays (FPGAs), to a name a few. Therefore, to ensure all logical devices comply with common requirements, the term Software-like-Hardware has been adopted to encompass all hardware-based logical computing devices.

L. Safety Critical Function Thread Analyses (SCFTA) [also includes L1, L2, L3]: This activity is derived from Airworthiness, MIL-HNBK-516C, Section 15. Safety Critical Functions developed in the FHA [see A] are mapped through the system design in the SCFTA. The focus is on LOR 1 software. This functional logic map is useful for subsequent analytical activities. Updates to the SCFTA **[L1, L2, L3]** are warranted to maintain currency and correctness with the evolving design. SCFTAs are time consuming to construct and maintain. As such, SCFTAs are focused only on functions residing in the most critical SwCI.

This activity addresses the *Analyses of Requirements* per Tables VI & VII.

M. Voting Logic: Assesses multi-channel cross-voting logic for correctness in all operating and maintenance conditions. Incorrect voting logic may lead to mishaps. Detailed assessments take time and personnel.

M1: Revised Voting Logic [also includes M2, M3]: If voting logic has been revised or characteristics of the design have changed that affect the validity of the voting logic, then the voting logic needs to be reassessed.

This activity addresses the Arc*hitecture* per Tables VI & VII.

N. Subsystem Hazard Analyses (SSHA) [see also N1, N2, N3]: Conduct the SSHA per Task 204 (if placed on contract). The SSHA considers how software contributes to hazards within subsystems.

This activity addresses the *Analyses* per Tables VI & VII.

O. System Hazard Analyses (SHA) [see also O1, O2, O3]: Conduct the SHA per Task 205 (if placed on contract). The SHA considers how software contributes to hazards in a system.

This activity addresses the *Analyses* per Tables VI & VII.

P. Operating & Support Hazard Analyses (O&SHA) [see also P1, P2, P3]: Conduct the O&SHA per Task 206 (if placed on contract). The SSHA considers how software contributes to hazards associates with how the system is used and related maintenance.

This activity addresses the *Analyses* per Tables VI & VII.

Q. Health Hazard Analyses (HHA) [see also Q1, Q2, Q3]: Conduct the HHA per Task 207 (if placed on contract). The HHA considers how software contributes to hazards affecting the health of operators, maintainers, and general public.

This activity addresses the *Analyses* per Tables VI & VII.

R. System of Systems Hazard Analyses (SoSHA) [see also R1, R2, R3]: Conduct the SoSHA per Task 209 (if placed on contract). The SoSHA considers how software contributes to hazards in a system of subsystems environment.

This activity addresses the *Analyses* per Tables VI & VII.

S. Environmental Hazard Analyses (EHA) [see also S1, S2, S3]: Conduct the EHA per Task 210 (if placed on contract). The EHA considers how software contributes to hazards associated with the environment.

This activity addresses the *Analyses* per Tables VI & VII.

T. Fault Tolerant Design Criteria: Establish fault tolerant design requirements and associated criteria early in a program. This provides the basis for how fault tolerant design criteria need to be applied to the system architecture. Design criteria may be changes, but this runs the risk of altering design requirements which in turn may lead to additional costs.

T1. Fault Identification and Response [T2, T3, T4]: As the software design matures, this task provides an understanding of how faults are identified and how software responds in a safe, deterministic manner. Fault insertion testing criteria are identified. In addition, software response should include operator/maintainer notification that a fault was detected in the interface.

This activity addresses the *Analyses* per Tables VI & VII.

U. Assess Interface Design [see also U1, U2, U3]: Interfaces have historically been an area prone to have hazards. This activity assesses interfaces to make sure each is interface if fully understood and the system design properly incorporated.

V. Review Draft Test Plan to Ensure LOR Implemented: Activity ensures LOR requirements addressed in the draft STP(s).

V1. Test Plan LOR Input:

V2. Test Report Review:

W. Detailed Code Walkthrough: Peer review to conduct a detailed inspection of the code for compliance with the LOR, SDP, coding standards, and other program guidance. The goal of the review is to ensure the software meets the intended function(s). Walkthroughs take time and experienced personnel. Such walkthroughs typically occur prior to formal testing.

This activity addresses the *Code* per Tables VI & VII.

X. Lable Test Cases within LOR:

Y. System Safety Risk Acceptance: Formal risk acceptance of all hazards required by AFI 91-202.

Z. 100% Branch Code Testing: By testing every logical branch screens for Dead Code (code not able to be executed). It also builds confidence in deterministic execution of the code. Costs include testing, time and resources.

Z1: Results of testing reviewed for safety impacts.

This activity addresses the *In Depth Testing* per Tables VI & VII.

AA. 100% Regression Testing: This activities builds confidence that modified software has deterministic execution and that safety issues have not been introduced through changes since the previous certification of the unit of software. Complete coverage takes time and consumes program resources, such as a software integration laboratory. This activity is focused on LOR-1 software.

This activity addresses the *In Depth Testing* per Tables VI & VII.

AB. Software Certification [see also AB-1]: The safety community needs to have a vote concerning the certification of software with safety impacts. The safety community's concerns shall be based on no adverse safety impacts associated with any LOR criteria.

AC. Fault Contribution Inspection [AC1, AC2]

AD. Tailored Regression Testing

AE. Fault Injection Testing [AE1]: Codify how desired faults will be introduced into software test protocols.

AF. Test Case Review: Review of the test cases ensures that test coverage is planned for all SwCI-2 software. Typically, this is accomplished prior to formal test. Costs include the manpower required for this review.

This activity addresses the *In Depth Testing* per Tables VI & VII.

AG. Failure Modes & Effects Testing (FMET): FMET testing exercises the software through testing identified failure modes. The results should align with the planned failure responses. The Software Test Plan (STP) must lay out the details with respect to the FMET tests. These tests should replicate real-world failure mechanisms.

AG-1 FMET Regression Testing: The purpose of these tests are to exercise the software through testing of identified failure modes associed with the architecture's regression scheme. These tests should replicate real-world failure mechanisms.

AG-2 Review FMET Test Results: The purpose of this activity is to review FMET test results to ensure these results align with the expected software responses.

AG-3 Review FMET Regression Test Results: The purpose of this activity is to review FMET regression test results to ensure these results align with the expected software responses.

This activity addresses the *In Depth Testing* per Tables VI & VII.

AH. Marking Code: Clear and concise comments embedded in source code and associated documentation makes sustainment and troubleshooting easier.

AH-1: As SwCI 1-2 code is revised, comments need to be revised as applicable.
This activity addresses the *Code* per Tables VI & VII.

AI. Hardware/Software Sensitivity Review: Hardware/software failures must be understood before software code can be written to account for these failure modes. This may drive additional testing.

AI-1. Revised Hardware/Software Sensitivity Review: Review test results to ensure they align with the hardware/software sensitivity review. Revise where needed. May drive adjustments to code.

AJ. Environmental Sensitivity Review: Assess which environmental conditions will stress the system design, develop applicable test cases, and incorporate into system test plans.

AJ-1. Review Environmental Sensitivity Results: Review these result to determine if any environmental impacts exist.

AJ-2: Environmental Field Surveillance: Field surveillance of the system functioning in the field.

AK. Mode Mismatch [AK1, AK2, AK3]

AL. Design Order of Precedence: This activity ensure design order of precedence has been integrated into the software development process/SDP when resolving safety issues.

AM. Safety Requirement Peer Review: Advocate software featured to preclude hazards from being introduced into the software design. Identifies logic discrepancies. Verification helps validate hazard closure.

AN. Information Latency & Inadvertent Failure to Properly Display Status Data

AO. Response to Transient Conditions: This activity explores how the system responds to transient conditions such as:
Power: As a result of electrical anomalies/failures or other non-graceful means of removing electrical power.
Operating Modes: Transitions while changing from one mode to another

AP. Reserved

AQ. Faulty Data [see also AQ1, AQ2, AQ3]: Assess the robustness of the design to address a variety of data related issues. Does the software continue to function in a deterministic manner despite such bad data?

AR. Software Development Plan (SDP) [AR1, AR2, AR3, AR4]: Formal safety coordination of the SDP establishes the baseline of how software will be developed/tested/certified. Safety needs to coordinate on every revision to the SDP.

AS. Software Partitioning [AS1, AS2, AS3, AS4]:

AT. Software Only Performs Intended Function [AT1, AT2]: Ensure no extraneous functions have been incorporated into the software.

AU. Extraneous/Dead Code [AU1, AU2, AU3]:

AV. Defect Tracking [AV-1, AV-2]: Safety needs to evaluate every problem report/defect/anomaly/etc associated with software to determine if safety impacts exist.

AW. Safety Critical Requirement Review [AW1; AW2; AW3; AW4]: Review safety critical requirements to ensure correctness and completeness. Assessments take time and experienced personnel. Revisions to Safety Critical Requirements require subsequent reviews.

AX. Witness Test Execution: For safety critical tests, safety witnessing test execution provides independent confirmation of proper test execution.

This activity addresses the *In Depth Testing* per Tables VI & VII.

CONCLUDING MATERIAL

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

Preparing activity:
Air Force – 40

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

SD-4 project:
SAFT -2006-002

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

Commented [PDANUAA919]: The following codes listed are managed via ASSIST. These will be updated as required