

System Safety Management Plan
for
Unmanned Aircraft Systems

JANUARY 2018



Approved By: _____

COURTNEY P. COTE
COL, AV

Project Manager, Unmanned Aircraft Systems

Distribution Statement D:

Distribution authorized to the Department of Defense and U.S. DoD contractors only; Administrative or Operational Use, 30 Sept 2013. Other requests shall be referred to the Program Executive Office (PEO) Aviation, Unmanned Aircraft Systems Project Management Office (UAS PMO), Technical Management, SFAE-AV-UAS-TM, Redstone Arsenal, AL 35898-5000.

Table of Contents

1.0 INTRODUCTION	1
1.1 Purpose	1
1.2 References	1
1.3 Scope	2
1.4 System Safety Program (SSP) Goal	2
1.5 Policy	2
2.0 ORGANIZATION AND RESPONSIBILITIES	3
2.1 General	3
2.2 Integration of Associated Disciplines	3
2.3 Responsibilities	4
2.3.1 Project Manager (PM)	4
2.3.2 UAS Safety Manager	4
2.3.3 Product Manager (PdM)	4
2.3.4 Product Safety Manager (PdSM)	6
2.3.5 AMCOM Safety Office	7
2.3.6 Aviation & Missile Research, Development, and Engineering Center (AMRDEC)	7
2.3.7 Training and Doctrine Command (TRADOC)	8
2.3.8 Program Executive Officer, Aviation (PEO AVN) Safety	8
2.3.9 Contractor System Safety Support	8
3.0 RISK MANAGEMENT	8
3.1 Hazard Identification	9
3.1.1 System Safety Analysis Tasks and Products	9
3.2. Risk Assessment	10
3.2.1 Hazard Severity Categories	10
3.2.2 Hazard Probability Levels	11
3.2.3. Risk Assessment Code (RAC)	12
3.3 Risk Resolution	13
3.4 Risk Acceptance	14
3.4.1 Materiel Developer Risk Acceptance	14
3.4.2 Interface with User Mission Risk Assessment (and Acceptance) Actions	14
3.5 Hazard Tracking	14

3.6 Risk Management for Test	16
4.0 SOFTWARE SYSTEM SAFETY (SwSS).....	16
4.1 Software Safety	17
4.2 Software Safety Analysis	17
4.3 Software Safety Assessment.....	18
4.4 Software Verification and Validation	21
4.5 Software Updates	21
4.6 Role of Software System Safety Working Group (SwSSWG).....	21
4.7 Role of SSSTRP.....	21
4.7.1 Software System Safety Technical Review Panel (SSSTRP) Reviews.....	23
4.8 Contracting for Software Requirements	23
4.8 COTS Validation.....	23
5.0 System Safety Working Group (SSWG).....	23
6.0 Safety and Maintenance Notification Messages.....	24
7.0 Definitions	24
8.0 Acronyms.....	26
APPENDIX A - Product Manager System Safety Working Group (SSWG) Charter	29
APPENDIX B - PM UAS Software Safety Minimum Level of Rigor (LOR) Table	33
APPENDIX C - Safety and Maintenance Notification System (UAS Workflow Diagram)	52
APPENDIX D – System Safety Risk Assessment (Example Format)	53
APPENDIX E - SSSTRP Finding/Assessment Response (Template)	54

1.0 INTRODUCTION

The Project Manager (PM) for Unmanned Aircraft Systems (UAS) has overall responsibility for the life cycle of Army UAS and related systems, which includes ensuring System Safety, as required by Army Regulation (AR) 385-10. These responsibilities include implementing a tailored System Safety Program (SSP) encompassing all systems and development, implementation, and maintenance of a System Safety Management Plan (SSMP) as part of the acquisition strategy for products in PM UAS.

1.1 Purpose

This SSMP establishes management policies, objectives, and responsibilities for developing and executing a SSP for the life cycle of all, current and emerging, UAS Project Office (PO) managed systems. This plan provides procedures to identify and control or eliminate hazards associated with these systems. This SSMP describes the methodology for accepting residual risks. It also establishes a hazard tracking system (HazTrak) for all UAS PO managed systems.

1.2 References

- a. AMCOM Regulation 385-17, Software System Safety, 15 Mar 08.
- b. AR 25-50, Preparing and Managing Correspondence, 2 Nov 12.
- c. AR 385-10, The Army Safety Program, 24 Feb 17.
- d. AR 40-10, Health Hazard Assessment Program, 27 July 2007.
- e. AR 750-6, Army Equipment Safety and Maintenance Notification System, 3 Feb 09.
- f. ASA (ALT) Memorandum, Subject: Environmental, Safety and Occupational Health (ESOH) Risk Review, 15 Nov 13.
- g. DA PAM 385-16, System Safety Management Guide, 13 Aug 13.
- h. JSSEH, Joint Software Systems Safety Engineering Handbook, 1 Apr 16.
- i. MIL-STD-882E, System Safety Program Requirements, 11 May 12.
- j. PEO AVN 13-08, System Safety Risk Management Process, 27 Sep 13.
- k. RTCA DO-178C, Software Considerations in Airborne Systems and Equipment Certification, 5 Jan 2012.

1.3 Scope

This SSMP will be executed by the UAS Project Management Office (PMO), who will ensure requirements are appropriately levied on supporting government organizations and on Prime Contractors via contractual statements of work (SOW). The SSMP defines the relationship between the PMO and the U.S. Army Aviation and Missile Command (AMCOM), other governmental agencies, major contractors. It establishes System Safety management responsibilities. The SSMP establishes the methods by which each Product Manager (PdM) monitors, evaluates and ensures the execution of the SSP. This SSMP will be reviewed and updated annually.

1.4 System Safety Program (SSP) Goal

The UAS SSP goal is to identify, assess, and mitigate or eliminate hazards in a timely manner and obtain risk acceptance of residual risks at appropriate levels for hazards associated with system operation, maintenance, and support as defined in approved operational requirements and system specifications.

1.5 Policy

It is the PMO Policy to conduct the following at the PdM level:

- a. Search continuously and systematically for potential system hazards and assess their risk in terms of credible severity and probability.
- b. Utilize this SSMP, add a product annex, or create a Product SSMP to document significant deviations in the System Safety approach for managing hazards, including hardware and software contributions and controls. Product Annex (es) or SSMP should be staffed via PM-UAS-TM Safety.
- c. Use a System Safety Working Group (SSWG) team approach to risk management with particular emphasis on including all stakeholders when assessing universal products (those items common/interoperable across multiple platforms) and how their hazards integrate with other systems.
- d. Resolve hazards in a time frame commensurate with the level of risk and program resources.
- e. Whenever possible, engineering controls will be used to eliminate hazards, procedure and administrative controls will only be used whenever engineering controls are not feasible (for example, affordability, availability, lack of training resource and/or trained personnel, and so forth).
- f. Identify and document hazards and resultant actions in a tracking system through final resolution.
- g. Exercise residual risk acceptance in accordance with (IAW) PEO Policy, reference (f).
- h. Assist the User in defining materiel and operational constraints, and risks associated with proposed local mission or material changes as an interface with their mission risk assessment process.

2.0 ORGANIZATION AND RESPONSIBILITIES

2.1 General

The PM has overall responsibility for ensuring System Safety throughout all UAS system life cycles. A formal System Safety Working Group (SSWG) will be established by each PdM using the Charter in Appendix A. The SSWG will convene periodically (at least twice per annum) during the life of the system to ensure appropriate coordination of the System Safety concerns and to assist in identification, coordination, tracking, and correction of the System Safety hazards. The SSWG will consist of primary and associate members selected to represent their respective activities. The voting members of the SSWG consist of a representative from Army Engineering Directorate (AED), AMCOM Safety, TCM, Program Executive Office (PEO) AVN and the PM (normally represented by the PM).

The PM (or PdM) Safety Manager facilitates the SSWG and when multiple PdMs are involved, a Safety Manager from each product will be in attendance. In the event of a tie vote, the PM will make the final decision. The SSWG facilitator will enter the voting results into the SSWG minutes along with any supporting information requested to be included by one of the voting members. SSWG meeting minutes will be provided in draft form for the voting members' concurrence before final signature. Findings and conclusions of the SSWG will be provided as recommendations to PM-UAS for approval.

2.2 Integration of Associated Disciplines

- a. UAS Human Systems Integration (HSI) - System Safety will maintain independence from the HSI domain for day-to-day operations. However, System Safety, through the AMCOM Safety Office, will participate fully as a primary member of the HSI Joint Working Group and will receive and provide input to the HSI program.
- b. Test and Evaluation (T&E) Integrated Product Team (IPT) - System Safety specific testing issues and test data will be exchanged to ensure hazards are identified and resolutions verified. The general safety of the test effort will also be reviewed IAW para 3.6. The PdM Test Coordinator is responsible for providing System Safety documentation required by test activities.
- c. U.S. Army Human Research and Engineering Directorate (HRED) - System Safety will utilize the HRED expertise to identify hazards caused or compounded by human performance constraints.
- d. U.S. Army Public Health Center (PHC) and the Army Material Command (AMC) Surgeon - System Safety will use medical and occupational health expertise to identify health hazards and to obtain recommendations for their elimination or mitigation. The AMC Command Surgeon is the central point of contact within AMC regarding Health Hazard Assessment (HHA) information, and will coordinate with PHC to establish an Independent Medical Assessor (IMA). System Safety may then coordinate directly with the IMA.
- e. Environmental - The SSP may identify environmental issues during the hazard analysis and resolution process. System Safety will coordinate environmental issues with the proper agencies.

2.3 Responsibilities

Individual and organizational responsibilities to implement this SSMP are described in the following paragraphs.

2.3.1 Project Manager (PM)

The PM UAS has overall responsibility for System Safety management of assigned systems. The PM will review the PdM's System Safety products and staff safety documents for external coordination. The PM will assign a UAS Safety Manager (at the project level to function as a Safety Team Lead) to ensure PdM Safety Manager coordinate activities, cross-level knowledge and support integrated products such as universal UAS products. The PM or designated representative will represent the PM at UAS SSWGs and Co-chair with the AMCOM Safety Representative. In the absence of the PM, the succession of UAS representation at UAS SSWGs is the Chief, Technical Management Division (TMD); Chief, UAS Engineering Operations, or UAS Safety Manager.

The PM will coordinate actions with external agencies and ensure PdM System Safety efforts are conducted proactively within program limitations. The PM Safety Manager will act as the primary POC for execution of this SSMP.

The PM is the risk acceptance authority for Low and Medium level hazards.

2.3.2 UAS Safety Manager

The PM will designate a Project Safety Manager who acts as the focal point for all safety actions. A formal SSWG will be established and convened every 6 months to coordinate system safety concerns as defined in Para 5.0 within. The Project Safety Manager assists in identification, coordination, tracking, and correction of all hazards opened by the SSWG Charter Members as defined in Appendix A.

2.3.3 Product Manager (PdM)

The PdM will:

- a. Designate a Product Safety Manager (PdSM) and delineate or delegate appropriate SSP implementation authority.
- b. Establish and Charter the SSWG (Appendix A).
- c. Ensure that applicable System Safety engineering and management instructions, regulations, specifications, and standards are implemented with contract Statements of Work (SoW) and system specifications.
- d. Ensure that specific SSP objectives, requirements and funding are incorporated into planning and execution documents.
- e. Assign budget and manpower resources to accomplish System Safety management tasks required by Army regulation, PEO AVN 13-08, and this SSMP.

- f. Ensure that Hazard Analyses are performed, documented, and reviewed IAW Army Regulation (AR) and PEO AVN 13-08.
- g. Ensure that hazard risk management and residual risk acceptance is accomplished IAW AR and PEO AVN 13-08.
- h. Maintain a documentation system, hazard tracking and/or System Safety Risk Assessment (SSRA) files, for risk acceptance decisions. HazTrak (<https://avnhaztrak.peoavn.army.mil>) has been established for this purpose.
- i. At each milestone, review the hazards, residual risks, risk acceptance recommendations, and provide Hazard Resolution Plans and status.
- j. Establish government and contractor relationships and interactions that will ensure positive contributions to, and an understanding of, contractual System Safety requirements.
- k. Establish procedures to evaluate Material Change Programs, and any other configuration change for conformity to System Safety standards.
- l. Establish procedures for tracking System Safety performance.
- m. Develop procedures for incorporating integrated human factors and health safety data identified by the cognizant disciplines throughout the product lifecycle.
- n. Establish relationships with the CBTDEV and the User to ensure that the actual system use environment is known, and make recommendations to the CBTDEV when hazardous differences are identified.
- o. Ensure that a safety assessment is conducted for all change proposals to confirm that new hazards are not introduced by design changes.
- p. Ensure that Software System Safety (SwSS) is managed IAW PEO AVN 13-08 and this SSMP.
- q. Request issuance of Safety and Maintenance Notification by the AMCOM Safety Office in accordance with AR 750-6 (reference c.).
- r. Request a HHA from the U.S. Army PHC at each major milestone and provide the most recent version to U.S. Army Test and Evaluation Command (ATEC) 60 days prior to the start of all testing. The most recent HHA shall be provided to the AMCOM Safety Office when requesting a safety and health assessment in support of a Materiel Release.
- s. Monitor the Contractor's SSPP.

2.3.4 Product Safety Manager (PdSM)

The PdSM will:

- a. Support and execute safety tasks for the PdM.
- b. Use the PEO HazTrak for tracking hazards, findings, supporting information and recommendations to final resolution; the final resolution being an appropriate program decision based on the findings as they relate to program constraints, and/or risk acceptance at the appropriate level.
- c. Ensure that HHAs are requested from the AMC Office of the Surgeon in accordance with AR 40-10 and that resulting issues are presented to the SSWG to be adjudicated as required.
- d. Prepare and present appropriate documentation for accepting residual risks IAW PEO AVN 13-08.
- e. Review all relevant reports including (but not limited to): Abbreviated Aviation Accident Reports (AAAR), Failure Reporting, Analysis and Corrective Action System (FRACAS) Reports, and Preliminary Reports of Aviation Mishaps (PRAM) to identify safety concerns.
- f. Convene pre-coordination meetings and/or facilitate the SSWG (Appendix A).
- g. Develop a SSWG meeting schedule, record meeting notes, voting member votes, position papers from voting members (if supplied) and distribute SSWG minutes once signed by the PM.
- h. Maintain all relevant archival documents including, but not limited to, hazard tracking, deliverable safety reports, and meeting minutes.
- i. Ensure all development, sustainment and integration contracts and applicable delivery orders contain the optimum System Safety requirements in accordance with the philosophy of this Plan.
- j. Coordinate CBTDEV requests for System Safety assistance in reducing risks identified in their Risk Management Process.
- k. Ensure that System Safety documents required for Milestone Decision Reviews (MDR) are generated and provided for use in the review package.
- l. Ensure that Hazard Tracking Records are reviewed prior to each SSWG meeting to determine any change in hazard status, and provide resulting conclusions and recommendations to the group.
- m. Prepare a Hazard Executive Summary (EXSUM) to alert the Army Safety Action Team (ASAT) Chairman when a hazard is identified that has a potentially significant impact on training or operations, IAW PEO Aviation Policy.
- n. Respond to accident board findings and recommendations submitted by the U.S. Army Combat Readiness Center (CRC) IAW PEO Aviation Policy.

- o. Prepare Risk Determinations to document, but not accept, risk (e.g. to support safety messages).
- p. Prepare and staff Risk Decision Memorandum (RDM) for interim risk pending SSRA staffing, or accept risk where a SSRA is not applicable (such as for test) IAW PEO AVN 13-08.
- q. Prepare SSRA Part I (per Appendix D), staff and track through to acceptance of risk per Appendix B.
- r. Submit Commander's Critical Information Requirements (CCIR) relating to mishaps or other safety related events.
- s. Provide an initial and mitigated risk determination to AMCOM Safety Office for all ASAM and AMAM Messages along with a recommendation for the type of message to be requested IAW the PEO AVN 13-08 and AR 750-6.

2.3.5 AMCOM Safety Office

The AMCOM Safety Office will:

- a. Advise PdM on System Safety requirements.
- b. Participate as the SSWG Co-Chairperson.
- c. Coordinate on PMO documents relating to System Safety, including recommendations for changes to MIL-Specs and Standards.
- d. Assist in maintaining active/working files of all safety related documentation.
- e. Track accident findings and recommendations received from the U.S. Army CRC from notification to resolution.
- f. Perform System Safety analyses to define specific issues for SSWG.
- g. Perform other System Safety support tasks as identified in the matrix support agreement.
- h. Coordinate and Issue Safety and Maintenance Notifications IAW AR 750-6 by request from the PM.

2.3.6 Aviation & Missile Research, Development, and Engineering Center (AMRDEC)

The AED, TMD, SED, and others, as applicable, will provide a description of safety issues identified during design, development, production, and fielding, and contractor quality program and materials evaluations. This includes requests from the field for materiel or operational deviations or waivers presenting a serious or high level risk. They will also apply their expertise toward resolution action identification and implementation.

2.3.7 Training and Doctrine Command (TRADOC)

The TRADOC Capabilities Manager (TCM) will be the system point of contact, unless otherwise directed, for official user coordination on hazard resolution actions. The TCM will also be the point of contact for operational requirements issues.

2.3.8 Program Executive Officer, Aviation (PEO AVN) Safety

PEO AVN Safety Officer has overall responsibility for System Safety management of assigned systems. The PEO reviews the PM's SSMP and staff safety documents for external coordination.

2.3.9 Contractor System Safety Support

The Prime Contractor will execute the contracted statement of work, which includes participation as a SSWG member.

3.0 RISK MANAGEMENT

Risk Management (RM) is the process of identifying, assessing, and controlling hazards or risks and making decisions that balance risk costs with mission benefits. All hazards associated with PM-UAS Products will be documented and managed in the PEO HazTrak (<https://avnhaztrak.peoavn.army.mil>).

The basic steps in the RM cycle are:

- a. Perform a systematic analysis using a defined, repeatable process.
- b. For each identified issue, determine the most serious credible outcome in terms of severity and probability and assign a Risk Assessment Code (RAC).
- c. Based upon the assessed risk, assign a resolution priority and eliminate or control the hazard accordingly.
- d. For hazards that cannot be completely eliminated, for whatever reason, perform risk acceptance procedures commensurate with the residual risk level IAW PEO AVN 13-08.
- e. Monitor the hazard. All hazards associated with PM-UAS Products will be documented in the PEO HazTrak.

NOTE: Software embedded in systems presents unique challenges for risk analysis and hazard identification. These challenges are greater for developed, fielded systems. Hazard identification and risk acceptance must be conducted within the landscape of operational requirements, patch updates and information assurance needs. Software hazard analysis for UAS will adhere to the spirit of AMCOM Regulation 385-17 and the criticality matrix of MIL-STD 882E. Software Risk Management is addressed in Section 4.0 within.

3.1 Hazard Identification

The purpose of risk analysis/safety analysis is to identify hazards to personnel, equipment, and or the environment, and generate safety requirements. Hazard identification and tracking will include the entire UAS. Ground Control Station (GCS) or aircraft hazards will be addressed by the cognizant Product Office with PM oversight (as SSWG Chair) to ensure equitable hazard management across product lines. Whenever possible, the PdSM should attend sister-product SSWGs.

A systematic analysis processes will be used to identify potential hazardous conditions. Analyses are not restricted to MIL-STD-882E processes but will also include reliability, human factors and environmental methods. All means will be used to proactively identify hazards before related mishaps occur in the field. Priority will be given to identification before a design is finalized.

- (1) Potential hazards identified during analysis will be tracked as issues until the SSWG adjudicates them.
- (2) Each Issue will be expressed using the “Source, Mechanism, Outcome” method to allow for consistent management of risk by the PdM.
- (3) Issues can be proposed by any involved party, but must be adjudicated by the SSWG to become a hazard. Issues determined to be “not a credible hazard” will be recorded in the SSWG minutes and, if time and workload permit, recorded in the hazard log and closed.
- (4) Software failure is not a stand-alone hazard, rather a source for an eventual outcome (usually with a related hardware mechanism). Refer to Section 4.0 within for management of software hazards.

3.1.1 System Safety Analysis Tasks and Products

System Safety analysis will be conducted early and often in the product lifecycle. Each change in design or function will include a safety analysis to limit the injection of new hazards into the system. The majority of this analysis will be based on vendor documentation, test results and field experience. The safety analysis tasks to be performed by the developer and documented in support of the program shall consist of but are not limited to the following:

- a. SSPP IAW Task 102 of MIL-STD-882E
- b. Preliminary Hazard List IAW Task 201 of MIL-STD-882E
- c. Functional Hazard Analysis (FHA); Analysis must also include failure effects on the aircraft
- d. NOTE: The Family of Systems (FoS) FHA database will be provided and shall be used by the developer as the baseline.
- e. Preliminary Hazard Analysis (PHA) IAW Task 202 of MIL-STD-882E
- f. Failure Modes and Effects Analysis (FMEA)
- g. Quantitative Fault Tree Analysis (FTA)

- h. Operating & Support Hazard Analysis (O&SHA)
- i. Hazard Tracking Reports
- j. Safety Assessment Report (SAR) IAW Task 301 of MIL-STD-882E

When issues are presented that relate to non-PM UAS developed or managed hardware or software, the issue will be logged in HazTrak as “Not a UAS Hazard” and transmitted to the cognizant material developer via memorandum. This issue will be closed in HazTrak with a copy of the transmittal memorandum and, whenever possible, a reference to the underlying standard attached.

An example of an issue is a vehicle’s roll-over limits that are not exceeded by addition of UAS equipment during vehicle integration with the UAS system.

Issues that relate to Operational Health standards, such as lifting weight/height, tripping hazards, etc., the appropriate army guidance shall be used to develop labeling and technical manual documentation necessary to meet Army requirements. The issue will be logged in HazTrak as a closed hazard when labeling and Technical Manual™ changes are complete. Risk acceptance documentation will be completed and managed IAW PEO AVN 13-08. A memorandum from the PdM that references the appropriate Army guidance and certifies completion of the labeling requirement will be uploaded as a supporting document in the HazTrak record and the issue will be closed with a Risk Assessment Code (RAC) of OS (zero-S as defined in Section 3.5) without further voting from the SSWG.

3.2. Risk Assessment

For each issue identified by analysis, the PdSM shall determine the most credible outcome in terms of severity and probability. The Hazard Severity and Hazard Probability Categories described in the following subparagraphs will be used to assign a RAC.

- (1) Care must be taken to separate “possible” outcomes from credible outcomes.
- (2) Issues and their outcome(s) shall be expressed at the system level to allow a common frame of reference for the SSWG, the PdM and their staff. (i.e. the “fuel starvation” Outcome will not be expressed as “engine failure” when the engine failure would credibly lead to an outcome of “loss of air vehicle” – the system level event).
- (3) Expression of risk at the system level is not synonymous with combining multiple sources into a single issue or hazard. In rare cases, with SSWG concurrence, multiple hazards (with multiple sources) may be combined within a single component hazard acceptance document with the focus being elimination of the hazard at the appropriate component, sub-system or system level. For example, multiple alternator failure sources may be combined into a single risk acceptance document if the material solution involves sourcing a replacement alternator.

3.2.1 Hazard Severity Categories

The PEO AVN hazard severity categories assess the consequences of the hazard outcome. Mishap severity categories provide a quantitative and/or qualitative measure of loss that could result from environmental conditions, design inadequacies, procedural deficiencies, or component

failure/malfunction. The term “aircraft loss” in PEO AVN 13-08 does not directly correlate to UAS due to the intentionally disparate nature of UAS vs manned systems. The most unique UAS feature is the separation of the flight crew and many of the system components from the air vehicle. UAS severity will be assessed using dollar values as the primary determinant.

Assessments will be conducted on standard basis of issue configuration. If a non-standard configuration change causes a system to exceed the dollar-value threshold for a given risk severity (e.g. a \$7M UAS carrying a \$5M non-standard payload presents a potential loss greater than \$10M), the associated hazards must be re-evaluated and will require separate hazard acceptance(s) for the higher risk configurations. Specific situations must be analyzed by the PdM, the PM UAS and other stakeholders. Configuration limitations posed by dollar values must be documented as part of the SSRA and/or AWR.

- a. Category 1 – Catastrophic: Death or permanent total disability; irreversible significant environmental damage; or monetary loss exceeding \$10M.
- b. Category 2 – Critical: Severe injury or severe occupational illness (permanent partial disability) or hospitalization of three or more personnel, reversible significant environmental damage or monetary loss exceeding \$1M but less than or equal to \$10M.
- c. Category 3 – Marginal: Minor injury or minor occupational illness (no permanent effect/1 or more lost work days), reversible moderate environmental damage, or monetary loss exceeding \$100K but less than or equal to \$1M.
- d. Category 4 – Negligible: Less than minor injury or occupational illness (less than one lost workday), minimal environmental damage or monetary loss less than or equal to \$100K.

3.2.2 Hazard Probability Levels

The hazard probability will reflect the quantitative and/or qualitative expectation that the potential mishap, at the credible severity, will occur during operation.

NOTE: There will be times when an additional probability should be referenced to show a high risk in relation to a specific phase or environment. This can be done in the hazard narrative with an explanation of the specific condition. Probability must be framed in an appropriate exposure interval. For example, a specific maintenance hazard may have a very low hazard probability due to very infrequent performance. However, if the activity is required, there is a more increased probability of injury. Without an additional condition specific reference point, the actual high-risk activity would be missed.

TABLE 3-1. MISHAP PROBABILITY LEVELS

Level	Description	Individual Item (qualitative)	Probability (mishaps per 100,000 flight hours)
A	Frequent	Likely to occur often in the life of an item.	Greater than 100
B	Probable	Will occur several times in the life of an item.	Less than or equal to 100 and greater than 10
C	Occasional	Likely to occur sometime in the life of an item.	Less than or equal to 10 and greater than 1
D	Remote	Unlikely but possible to occur in the life of an item.	Less than or equal to 1 and greater than 0.1
E	Improbable	So unlikely, it can be assumed occurrence may not be experienced.	Less than or equal to 0.1 and greater than 0.01
F	Very Improbable	So unlikely that occurrence may be a complete surprise.	Less than or equal to 0.01 but greater than zero

3.2.3. Risk Assessment Code (RAC)

The RAC is the combination of the hazard severity category and the hazard probability level, written as a number and a letter. An initial RAC is assigned upon hazard identification and may change as the hazard is better defined or mitigation actions are taken. The change must be justified and documented in the Hazard Log, or suitable supporting document. The goal is to complete the mitigation action by bringing the probability to zero. RACs for hazards with no residual risk requiring acceptance are described in paragraph 3.5.h.

TABLE 3-2. RISK MANAGEMENT MATRIX

Severity Probability		Catastrophic	Critical	Marginal	Negligible
		1	2	3	4
Frequent >100	A	High AAE	High AAE	Serious PEO	Medium PM
Probable >10 and <=100	B	High AAE	High AAE	Serious PEO	Medium PM
Occasional >1 and <=10	C	High AAE	Serious PEO	Serious PEO	Medium PM
Remote >0.1 and <=1	D	Serious PEO	Serious PEO	Medium PM	Medium PM
Improbable >0.01 and <=0.1	E	Serious PEO	Medium PM	Medium PM	Low PM
Very Improbable >Zero and <0.01	F	Medium PM	Low PM	Low PM	Low PM

RISK ASSESSMENT CODE

1A – 1C; 2A – 2B

1D – 1E; 2C – 2D; 3A – 3C

2E; 3D – 3E; 4A – 4D

1F; 2F; 3F; 4E-4F

RISK LEVEL

HIGH

SERIOUS

MEDIUM

LOW

PRIORITY

URGENT

CRITICAL

ELEVATED

ROUTINE

AUTHORITY

AAE

PEO

PM*

PM*

*Per PEO AVN 13-08, PM system level medium and low risk acceptance authority may not be delegated.

3.3 Risk Resolution

Once the appropriate RAC is determined, the PdM will assign a resolution priority within the overall scope of program efforts and eliminate or control the hazard accordingly. Hazards will be addressed according to the priority of Table 3-2. Potential mitigations should be developed to eliminate or lower the risk to an acceptable level. The SSWG will evaluate potential methods for controlling or eliminating a hazard and estimate the expected effectiveness of each method. The SSWG will provide a report/meeting minutes to the PM and PdM setting forth the risk assessment results based on the hazard control recommendations. All hazards will be annotated and managed in the HazTrak until resolved. Hazards eliminated by design or architecture changes will be re-adjudicated and closed by the SSWG.

- The PdM team will eliminate or control hazards as part of the overall product management effort.
- The total system is evaluated in the PdM systems engineering (and other) efforts, providing a “top down” and “bottom up” look at safety, reliability, suitability, and supportability within the constraints of cost, schedule and performance.

3.4 Risk Acceptance

3.4.1 Materiel Developer Risk Acceptance

For hazards that cannot be completely eliminated, for any reason, mitigate the risk to the lowest possible level consistent with Operational requirements and resource constraints and perform risk acceptance procedures commensurate with the residual risk level IAW PEO AVN 13-08. Hazard/Risk resolution recommendations should serve as the initial documentation for a risk-acceptance decision. Table 3-2 defines the Command level decision authority for accepting the risk associated with each hazard.

The consequences of risk acceptance of the proposed configuration and alternative actions should be stated quantitatively when practical. The decision to accept the risk shall also consider impact on schedule, operational effectiveness, and other factors and should be included in the overall program risk assessment. In accordance with AR 385-10, the responsible CBTDEV will make recommendations on risk assessments, and include their recommendations for alternative or supplemental actions.

Risk will be accepted by the appropriate authority IAW PEO AVN 13-08.

The SSRA will be drafted for all serious and higher level risks for which available controls cannot reduce the residual risk to a medium or low level in less than one year. The SSRA will include mitigation plans and an expiration date with the intent of reducing risk. The SSRA will be staffed through the AMCOM Safety Office, to the Commander, AMCOM; Commander, U.S. Army Aviation Center of Excellence (USAACE), prior to forwarding to the PEO for signature or other action.

If a risk is mitigated to the lowest possible level, but not completely eliminated, it may be incorporated into the underlying risk of the system by execution of a memorandum for record which will serve to document that the risk has been reduced to the lowest possible level within the constraints of the program.

3.4.2 Interface with User Mission Risk Assessment (and Acceptance) Actions

User/Operator Risk Assessments are encouraged. When the User requests a deviation from established configuration or procedures, the PdM will address the request, coordinating directly with the requester and the Risk Acceptance Authority.

3.5 Hazard Tracking

IAW PEO AVN Directive, HazTrak will be utilized by the PdM to track all identified hazards at <https://avnhaztrak.peoavn.army.mil/>.

- a. The status of a hazard or issue will be listed as “Proposed” when it is submitted from any source and until opened or dismissed as not a hazard by the SSWG or PdM.
- b. A hazard is in the “Open” status when the SSWG or PdM formally acknowledges it.
- c. The “Monitor” status identifies a category of open hazards that is assigned by the SSWG or PdM to hazards which are awaiting test completion for better definition of the hazard, hazards

awaiting test for substantiation of corrective action, hazards which are based on isolated events and more data is needed to justify corrective action/hazard closure, or hazards for which corrective action has been defined and is in progress.

- d. The “Accepted” status applies to hazards if the decision authority (Table 3-2) has given written approval of the final risk category. “Accepted” risks will generally have a periodic review date and, potentially, an expiration date for the acceptance (if set by the acceptance authority). Open-ended hazard acceptance will be reserved for the very few hazards which have no foreseeable potential for elimination or further mitigation. These hazards should be considered for closure by the Milestone Decision Authority (MDA).
- e. Hazards within the PM risk acceptance authority may be accepted without a formal SSRA. The SSWG will recommend closure to the PM as part of the SSWG briefing and/or minutes. PM signature on the minutes shall constitute interim risk acceptance. The SSWG recommendation and reference to the signed minutes shall be noted in the HazTrak Record.
- f. The “Recommended Closed” status applies to hazards which the SSWG or PM has deemed to be impractical to reduce and that further tracking will impair the ability of the SSWG to conduct its chartered tasks.
- g. The status of a hazard will be listed as “closed” under normal circumstances if the risk has been eliminated, is determined by the SSWG to be not a credible hazard. Closed hazards may be reopened if circumstances warrant.
- h. In the HazTrak Database, hazards closed with no residual risk are defined below. Previously accepted or closed hazards will be reviewed by the PM/PdM Safety Managers and AMCOM Safety prior to SSWG meetings, or at least twice annually for changes in risk. The SSWG will approve recoding and the PM will be notified through the meeting minutes. “Open” or “Monitor” hazards may be recommended for zero residual risk closure with SSWG and PM approval. The HazTrak details will be updated to show the date of the review, the justification for RAC assignment, the action taken by the PM, and the final severity and probability. RACs for hazards with no residual risk will be assigned as follows:

0A (zero A) – Hazards which are no longer valid due to errors, superseded by other hazards and/or similar actions will be administratively coded 0A and the action taken section appropriately annotated.

0R (zero-R) – Hazards eliminated by a materiel/design change, to include a life or overhaul change.

0S (zero-S) – Hazards with no residual risk requiring acceptance by virtue of the design meeting or exceeding all applicable consensus and/or military standards and being operated in an environment consistent with those standards, i.e., being operated with published procedures that may include operating limitations, field inspections, and maintenance procedures.

3.6 Risk Management for Test

The processes discussed in the preceding paragraphs are used for material risks of the UAS fleet. For UAS products involved in testing, hazards shall be assessed by the Test Flight Authority (typically the PdM) and the associated risks will be accepted at an appropriate level.

A Test Flight Authorization (TFA) Memorandum will be developed for each test prior to execution. The format is standard AR 25-50 memorandum format. The TFA will describe the test to be conducted to include a description of the components/functions being tested and success/fail criteria. Other contents at the discretion of the PdM with minimum topics of:

- a. Test risk assessments with hazards and mitigations with responsible parties, and Program risk assessment with hazards, mitigations and responsible parties. Also required is an explicit statement of the residual test risk and residual program risk.
- b. Test risk analysis and assessment will be included in the TFA along with a program risk analysis and assessment relating to the test activity (e.g. if the test involves the only capital asset in the program, the severity of loss of the test asset increases program risk).

The test risk is accepted when the TFA is signed by the appropriate Risk Acceptance Authority. Low test risk may be accepted at the PdM level with a copy furnished to the PM.

Medium test risk will be accepted by the PM. Acceptance authority for serious (and higher) test risk will be determined on a case-by-case basis at the PM's discretion.

The TFA will be addressed to the party responsible for execution of the test and a complete copy will be furnished to the PM UAS. The TFA will be signed by the PdM or their delegate (and endorsed by the risk acceptance authority if risk level exceeds the PdM level).

The TFA is not mission risk acceptance. Responsibility for the operational/mission risk assessment for any flight (including test) rests with the appropriate mission risk acceptance authority and shall be conducted IAW AR 385-10 and local Statement of Procedures (SOP).

Test risk will not be adjudicated by the SSWG nor entered into the hazard log. The PdM responsible for the test will assess and record test risk IAW this SSMP. Record keeping after test is at the discretion of the PdM.

4.0 SOFTWARE SYSTEM SAFETY (SwSS)

Within the System Safety organization, SwSS provides the interface between System Safety Engineering and Software Development (SD). Software System Safety is the application of System Safety principles, criteria and techniques to software. The Software Development lifecycle initiates at concept refinement and results in a software release, this lifecycle is executed multiple times during the product acquisition lifecycle. Throughout the SD lifecycle, emphasis should be placed on the system and how software contributes to or mitigates failures. Development of Safety Critical SW should be part of the overall Software Development Plan (SDP). Sound analysis, rigorous testing, and proper verification and validation methods will ensure that safety requirements are met. This process will provide confidence that the software will perform as specified and allow for successful certification.

The PdM will ensure UAS software is developed with the goal of achieving an airworthiness approval recommendation from the SED's JS-SSA JSSEH Implementation Guide and the SEDs PM Handbook for Aviation Software Airworthiness (PMHASA) provide detailed guidance to ensure software safety and to support the flight software airworthiness approval. While the documents were developed to address new system acquisition, the analysis and activities should be applied to enhancements and modifications of PM UAS legacy systems.

Software hazard analysis has unique challenges. These challenges are greater for developed, fielded systems. Hazard identification and risk acceptance must be conducted within the landscape of operational requirements, patch updates and information assurance needs. Software hazard analysis for UAS will adhere closely to the guidance in AMCOM Regulation 385-17, MIL-STD 882E, JSSEH Implementation Guide, and SED's PM Handbook for Aviation Software Airworthiness.

4.1 Software Safety

Software Safety success is dependent on a safety-significant software development process, sound hazard assessment process, and accomplishment of the depth and breadth of software analysis validations and verification activities necessary to provide a sufficient level of confidence that a safety-critical or safety-related software function will perform as required. These activities are described as a Level of Rigor (LOR) have been codified and included here as Appendix B. The table in Appendix B contains the PM UAS base Level of Rigor required tasks and minimum standard for LOR artifacts expected in all developments. The LOR artifacts generated as a result of this stringent process will be available for a SSSTRP review, software certification efforts, and ultimately evidence to support a favorable Software Safety Statement for Material Release.

4.2 Software Safety Analysis

Software faults may contribute to hazards, in either control of, or interface with, the supported system. Software contributions to hazards arise through defects, errors, and omissions, leading to a failure of the system to operate correctly. In depth hazard analysis will be conducted to identify potential or existing software contributions to hazards and requirements developed to either eliminate those hazards or reduce them to an acceptable level. The software safety analysis tasks to be performed by the developer and documented in support of this effort shall consist of but are not limited to the following:

- a. Software contributions to identified system hazards and documented in the Preliminary Hazard Analysis (PHA) IAW MIL-STD-882E Task 202.
- b. Identification and documentation of System Software Critical Safety Functions (SCSFs) in the FHA IAW MIL-STD-882E Task 208.
- c. Safety Requirements Hazard Analysis IAW Task 203 of MIL-STD-882E, or equivalent in AMCOM 385-17.
- d. Software Test Description, Software Test Plans and subsequent Software Test Reports.
- e. System Hazard Analysis (SHA) IAW Task 205 of MIL-STD-882E, or equivalent in AMCOM 385-17.

- f. Subsystem Hazard Analysis (SSHS) IAW Task 204 of MIL-STD-882E, or equivalent in AMCOM 385-17.
- g. Software Hazard Analysis Reports.
- h. Change Impact Analysis, if applicable.
- i. Demonstrated LOR Compliance.

NOTE: A list of required Software Development Artifacts is available in SED's PMHASA, Appendix B, Table 19.

4.3 Software Safety Assessment

Unlike material risks, the assessment of risk due to software cannot rely solely on severity and probability.

Software risk considers the Degree of Control that software exercises over the hardware and the Potential Risk Severity to determine the criticality of the hazard. Finally, software risk, more appropriately, the Software Contribution to System Risk, is quantified by using the tables within MIL-STD 882E.

- a. The degree of software control is defined using the Software Control Categories (SCC) listed on MIL-STD 882E, Table IV.

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. <i>(This definition includes complex system/software functionality with multiple subsystems, interacting parallel processors, multiple interfaces, and safety-critical functions that are time critical.)</i>
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. <i>(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.)</i> - 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. <i>(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.)</i>

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. <i>(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.)</i> - 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.

- b. The potential risk severity of the hazard combines with the degree of control in MIL-STD 882E, Table V to determine the Software Criticality Index.

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

c. The Software Criticality Index (SwCI) is used to define the required LOR tasks.

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.

d. LOR tasks are 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. 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 MIL-STD 882E, Table VI. Table VI depicts the relationship between SwCI, risk levels, completion of LOR tasks, and risk assessment. All software developed will maintain current LOR status in development of all affected functions. Affected functions must be tested with regression test of the highest assessed SwCI level for that function.

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

If developing software to satisfy Army Software Airworthiness in accordance with civil certification standards, i.e. DO-178C, the developer shall perform a cross walk between the LOR table in Appendix B of this document and those tasks required to meet the applicable Development Assurance Level (DAL). Appendix C of the SED's PMHASA and Appendix B of this SSMP contain objectives maps that can be used to aid in the comparison. The developer shall gain concurrence from the government that those tasks required to meet the civil standard meet or exceed those tasks identified in the LOR table. The developer shall document the process used during software development in the SSSPP, and provide artifacts to satisfy the requirements of the SSSTRP and Material Release Authority.

4.4 Software Verification and Validation

If an Independent Verification/Validation (IV&V) is required to satisfy the software review and Material Release process for software suitability, the developer shall provide the necessary documents/artifacts for review and allow the assigned independent reviewer access to those documents at their facility.

4.5 Software Updates

Subsequent software releases shall require additional safety analysis to determine the effect of changes on the existing system. Updates to existing artifacts may be acceptable depending on the nature of the software update. Participation in the SSSTRP shall be required if changes to the software introduce a change in capability such as the implementation of new requirements.

Software Hazard mitigations and/or solutions must adhere to the current software development requirements (i.e. AMCOM 385-17) unless the PdM determines (i.e. the SSWG indicates) otherwise based on urgency of need and available resources.

4.6 Role of Software System Safety Working Group (SwSSWG)

Products may utilize a SwSSWG. The SwSSWG plays a critical role in bridging the gap between the software development process and the safety organization. Moreover the SwSSWG serves as the mechanism for communicating any credible potential hazards, either experienced or uncovered, during the legacy, current, or in-development program. The SwSSWG should function under the authority of the SSWG and under their Charter. The function of the SwSSWG will as be to assist the PM and Project Safety Manager on Software Safety issues. The goal of the SwSSWG is to analyze proposed and outstanding software hazards and SSSTRP findings/recommendations. The SwSSWG shall provide input and recommendations to the program SSWG for adjudication. Ideally, the SwSSWG will meet twice a year in conjunction with a SSWG but not less than once a year.

4.7 Role of SSSTRP

The AMCOM SSSTRP plays a critical role in UAS Software Safety in that it is the principle guide to the PM regarding the focus for software development resources. The SSSTRP advises the SSSPP Managers and provides guidance and suggested approaches on SwSS issues and compliance with the SwSS Policy. The SSWG involvement in Software Safety is supportive of the SSSTRP efforts when specific functions are

identified that are a source for a credible outcome [using the Server Management Objects (SMO) model of hazard identification] that is not otherwise related to an existing material hazard.

In legacy systems (developed prior to the implementation of AMCOM 385-17), a lack of system level testing is not necessarily a hazard nor is a lack of LOR testing (or alternative artifacts) automatically assessed as a credible hazard. Per Chapter 1 of AMCOM 385-17, UAS legacy systems work with the SSSTRP to identify compliance gaps and work toward resolution/closure of these gaps. The level of effort is ultimately determined within the program resources and requirements with particular focus (for fielded systems) on reliability analysis, FMECA and other real world performance indicators. Remaining items are addressed following the appropriate adjudication processes.

However in new and significantly modified legacy systems, lack of LOR compliance will result in risk assessment as discussed in Section 4.3 within.

When specific software functions are identified as sources to hazards, or when an existing hazard has a credible software source, the hazard log will indicate the software component of the hazard.

The SSSTRP and SwSSWG focus on software allows the SSWG to avoid becoming overwhelmed by analysis at the function level of the software intensive UAS. The PdM's and their associated SSWGs are not resourced to conduct an independent, comprehensive assessment of every potential software issue in UAS. Due to the potential for an unsupportable burden caused by recording potential hazards based on a list of software functions, when no other indicator exists beyond FHA/LOR analysis, software hazards will not be individually adjudicated by the SSWG, but rather analyzed and communicated via the SwSSWG. Thus, as discussed in AMCOM 385-17, the SwSSWG is used to adjudicate credible software related hazards and then upon adjudication voice those to the SSWG appropriately.

Software hazards may be independently addressed as a hazard by the SwSSWG/SSWG when that body determines the SSSTRP reports, IV&V efforts and other software development oversight is inadequate to inform the PdM and PM of the software issues inherent in the system. To be adjudicated as a hazard, the software safety issue must meet the following guidelines:

- a. Must have a credible root concern [e.g. Software Integration Laboratory (SIL) or other test failures/concerns, field experience, detailed analysis validated by PdM, source code, design artifact, etc.].
- b. Specific function identified as a source which leads to a credible outcome (e.g., for AV2181 Mishap baro-metric altimeter zero data was used by the mission processor, PPT4 Hellfire shot flew toward the equator, tanks slope was inverted in SW implementation, etc.) [Inadequate example is, "Software failure may lead to..."].
- c. The source-mechanism-outcome of the issue must be well defined and have an actionable measurable solution within the functional requirements of the system (e.g., mission processor reject baro zero, upon Manned-Unmanned Teaming (MUM-T) handover reset stores control computer software, fix Tactical Automated Landing System (TALS) survey code, etc.).

4.7.1 Software System Safety Technical Review Panel (SSSTRP) Reviews

All SSP activities and milestones will be aligned with the scheduled program reviews. Coordination with the AMCOM Safety Office will identify appropriate times for the SSSTRP to conduct periodic reviews and provide Software Safety Program reviews. Documents will be updated as necessary at each milestone review. Safety program status shall be provided during the System Requirements Review (SRR), Preliminary Design Review (PDR), Critical Design Review (CDR), and Test Readiness Review (TRR). A SSSTRP review will be requested after conclusion of testing to evaluate and provide recommendations for the Software Safety Statement.

4.8 Contracting for Software Requirements

The PMHASA contains an Appendix which is to be used as a guide for acquisition managers when procuring systems with flight software requirements. The Appendix A, Recommended Generic Software SOW, is to be consulted during Technical Management review of all PM-UAS Contracts.

NOTE: PMHASA does not include DO-178C supplement objectives, so if Model Based Development (MBD), Object Oriented (OO), or Tool Qualification are necessary, additions are needed to the guidance provided in PMHSAS.

Due to the incremental approach to integrating current requirements, the SOW and/or Request for Proposal (RFP) will clearly define what analyses and activities are required at the PdM's discretion.

When considering changes to existing systems, PdM's are encouraged to go heavy on regression testing and off-nominal messaging at interface junctions (e.g. UGCS communicates to Hunter. Test valid packets with invalid commands).

4.8 COTS Validation

When considering a COTS solution, PdM's must consider Section 4.4 (Software V&V) within and other applicable portions of this document in order to satisfy the software review and certification efforts, and ultimately produce evidence to support a favorable Software Safety Statement for a Material Release.

5.0 System Safety Working Group (SSWG)

The SSWG/SwSSWG is chartered by the PM to actively identify and assess hazards, monitor System Safety task accomplishment, identify System Safety requirements, organize and coordinate interfacing functions, and provide timely and effective recommendations to the Product Director (see Appendix A). The SSWG will be Co-chaired by the PM or his/her designee (usually the UAS Safety Manager or a designated government PdM representative) and the AMCOM Safety Office representative. A representative from AED, PEO AVN, and TCM will also serve as primary members of the SSWG. Each primary member will be a voting member and the PM will have the final authority. The PdM Software & Test Branch will participate in the PdM SSWG as necessary on all software related hazards. Additional members may include but are not limited to safety or engineer team representatives from participating developers. SSWG meetings will be held to work on individual issues and will usually include in-depth informational discussions of relevant System Safety issues and advancements. Tasking will be recorded on Action Item sheets and managed by the Product Office to completion.

Primary SSWG member meetings shall also be held at the request of the PM to assist in identification, definition, assessment, and resolution of immediate System Safety issues. These meetings may be conducted telephonically or at a designated location. SSWG meetings will be held at least every six months but may convene more frequently if the need should arise. Agenda items may be proposed by any organization and reviewed by the Safety Manager. Minutes will be prepared, coordinated with the primary members, and distributed for all formal SSWG meetings. A System Safety IPT will be established by non-Program of Record (POR) Offices within PM UAS, and a representative will attend the PdM SSWG to ensure information is shared with applicable stakeholders.

6.0 Safety and Maintenance Notification Messages

Staffing of Safety messages will be executed by AMCOM Safety Office IAW AR 750-6.

7.0 Definitions

The following definitions are consistent with MIL-STD-882E and AR 385-10, and are tailored to fit the needs of the UAS SSP:

- a. Combat Developer (CBTDEV) – Command or agency that formulates doctrine, concepts, organization, training, materiel requirements, and objectives. Represents the user community over the life cycle of the system.
- b. Depot – A central facility for conduct of heavy maintenance on Army systems. For UAS, depot may include the vendor’s production and repair facility (due to a lack of established army depot activities for UAS systems). Post-mishap tear down, investigation and repair may occur at vendor depot facilities and may, at the discretion of the responsible Army authority, be witnessed by the Defense Contract Management Agency (DCMA), Corpus Christi Army Depot (CCAD) Mishap Investigators, or other qualified agencies.
- c. Hazard – Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment. Hazards are defined primarily through three key elements: Source, Mechanism, and Outcome.
- d. Hazardous Material – Any substance that, due to its chemical, physical, or biological nature, causes safety, public health, or environmental concerns that would require an elevated level of effort to manage.
- e. Life Cycle – All phases of the system’s life including design, research and development, test and evaluation, production, deployment (inventory), operations and support, and disposal.
- f. Level of Rigor (LOR) – Software development efforts required to minimize risk of software failures by focusing resources based on criticality of functions.
- g. Materiel Developer (MATDEV) – Command or agency responsible for research, development, and production of a system in response to approved requirements. Parties include the program/project/product manager or product director.

- h. Mechanism – The second part of the Source, Mechanism, Outcome model for defining hazards. That process or sequence of events that allows or enables the source to cause harm.
- i. Mishap – An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.
- j. Mishap Risk – An expression of the impact and possibility of a mishap in terms of potential severity and probability of occurrence.
- k. Outcome – The third part of the Source, Mechanism, Outcome model for defining hazards. That harm which the source brings about through the mechanism.
- l. Residual Mishap Risk – The remaining mishap risk that exists after all mitigation techniques have been implemented or exhausted, in accordance with the System Safety design order of precedence.
- m. Safety – Absence of those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.
- n. Product Management System Safety Team – A generic term used in this plan to identify the Product Manager’s core, matrix and contractor personnel commonly working together to resolve an identified program issue.
- o. Safety Message – Safety related information transmitted to field users through any number of army messaging systems, the purpose of which is to provide timely information to prevent mishaps while allowing traceability of receipt and, when necessary, compliance with directives. For UAS, Safety Messages may include contractor communications with field repair activities such as Tactical Field Notices (TFN), Alert Bulletins (AB) or others. These internal communications do not replace the official Army messaging system, but may be used in conjunction with an Army Safety Action Message (ASAM), Army Safety Maintenance Action Message (AMAM), Safety of Flight (SOF) Message, etc. Where compliance is mandatory, standard Army Messages are required.
- p. Source – The first part of the Source, Mechanism, Outcome model for defining Hazards. An activity, condition or circumstance that has the potential to do harm to an asset.
- q. System Capability (and Loss of System Capability) – The ability of a UAS system to perform a given mission. Where a manned aircraft becomes non-mission capable when unable to fly, a UAS system has multiple aircraft to overcome a single AV loss and maintain system capability. System Capability is lost when the UAS system cannot launch, control and recover an unmanned aircraft, or the system cannot use a payload to conduct missions.
- r. System Safety – The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk throughout all phases of the system life cycle.
- s. System Safety Engineering – An engineering discipline that employs specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated mishap risk.

- t. System Safety Management – An element of program management that establishes the SPP requirements and ensures the planning, implementation, and accomplishment of tasks and activities to achieve System Safety consistent with the overall program requirements and constraints.
- u. System Safety Program (SSP) – The combined tasks and activities of System Safety Management and System Safety Engineering that enhance operational effectiveness throughout the entire system life cycle.
- v. System Safety Program Plan (SSPP) – A formal document prepared by the contractor that describes the planned safety tasks required to meet contractual System Safety requirements. It includes organizational responsibilities, methods of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems.
- w. 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, Commercial Off The Shelf (COTS), Government Off The Shelf (GOTS), re-used, Government Furnished Equipment (GFE), and Government-developed software used in the system.
- x. Software System Safety Technical Review Panel (SSSTRP) - The AMCOM SSSTRP functions as the vehicle for evaluating safety-critical software and providing endorsements to the Materiel Release Review Board.
- y. System Safety Working Group (SSWG) – An assembly of primary and associate members organized and chartered to assist the PM/PdM in achieving System Safety objectives.
- z. Software System Safety Working Group (SwSSWG) – A twice a year, or as necessary, gathering of SSWG member and software stakeholders to specifically cover software items pertaining to Safety Objectives.

NOTE: Typically held as a sidebar with the SSWG.

8.0 Acronyms

AAAR	Abbreviated Aviation Accident Report
AAE	Army Acquisition Executive
AB	Alert Bulletins
AED	Aviation Engineering Directorate
ALC	AMCOM Logistics Center
AMAM	Army Maintenance Action Message
AMC	Army Materiel Command
AMCOM	Aviation and Missile Command
AMRDEC	Aviation and Missile Research Development and Engineering Center
ASAM	Army Safety Action Message

ASAT	Army Safety Action Team
ATEC	Army Test and Evaluation Command
AVN	Aviation
CBTDEV	Combat Developer
CCAD	Corpus Christi Army Depot
CCIR	Commanders Critical Information Requirements
CECOM	Communications-Electronics Command
CDR	Critical Design Review
COTS	Commercial Off The Shelf
CRC	Combat Readiness Center
DA	Department of the Army
DAL	Development/Design Assurance Level
DCMA	Defense Contract Management Agency
ESOH	Environmental Safety and Occupational Health
EXSUM	Executive Summary
FHA	Functional Hazards Analysis
FMEA	Failure Modes and Effects Analysis
FoS	Family of Systems
FRACAS	Failure Reporting, Analysis and Corrective Action System
FTA	Fault Tree Analysis
GCS	Ground Control Station
GFE	Government Furnished Equipment
GOTS	Government Off The Shelf
HazTrak	Hazard Tracking System
HHA	Health Hazard Assessment
HSI	Human Systems Integration
HRED	Human Research and Engineering Directorate
IMA	Independent Medical Assessor(s)
IPT	Integrated Product Team
IV&V	Independent Verification/Validation
JSSEH	Joint Software Systems Safety Engineering Handbook
JS-SSA	Joint Services – Software Safety Authorities
JWSR	Joint Services Weapons Safety Review
LOR	Level of Rigor
MDA	Milestone Decision Authority
MBD	Model Based Development
MDR	Milestone Decision Review
MIL-STD	Military Standard
MUM-T	Manned-Unmanned Teaming
OO	Object Oriented
PAM	Pamphlet
PdM	Product Manager
PDR	Preliminary Design Review
PEO	Program Executive Office(r)
PHC	Public Health Command
PM	Project Manager
PMHASA	PM Handbook for Aviation Software Airworthiness
PMO	Project/Program Management Office
PO	Project Office

POR	Program of Record
PRAM	Preliminary Report of Aviation Mishap
RAC	Risk Assessment Code
RDM	Risk Decision Memorandum
RFP	Request for Proposal
RM	Risk Management
SCC	Software Control Categories
SDP	Software Development Plan
SED	Software Engineering Directorate
SHA	System Hazards Analysis
SIL	Software Integration Laboratory
SM	Safety Manager
SMO	Server Management Objects
SOP	Statement of Procedures
SOF	Safety of Flight
SOW	Statement of Work
SRR	System Requirements Review
SSHS	Subsystem Hazard Analysis
SSMP	System Safety Management Plan
SSP	System Safety Program
SSPP	System Safety Program Plan
SSRA	System Safety Risk Assessment
SSSTRP	Software System Safety Technical Review Panel
SSSPP	Software System Safety Program Plan
SSWG	System Safety Working Group
SwCI	Software Criticality Index
SwSS	Software System Safety
SwSSWG	Software System Safety Working Group
TALS	Tactical Automated Landing System
TCM	TRADOC Capabilities Manager
T&E	Test and Evaluation
TFA	Test Flight Authorization
TFN	Tactical Field Notices
TM	Technical Manual
TMD	Technical Management Division
TRADOC	Training and Doctrine Command
TRR	Test Readiness Review
UAS	Unmanned Aircraft System
UGCS	Universal Ground Control Station
USAACE	U.S. Army Aviation Center of Excellence
USAARL	U.S. Army Aeromedical Research Laboratory
V&V	Verification/Validation

APPENDIX A - Product Manager System Safety Working Group (SSWG) Charter

1.0 PURPOSE

Establish a technically qualified advisory group for the PM on System Safety management as a means to enhance the safe design, sustainment and operation of the system and its mission and kits and enable the integration of Universal products and other integrated systems.

2.0 MISSION

The mission of the SSWG is to function as an element of project management and actively identify and assess hazards, monitor System Safety task accomplishment, identify system requirements, organize and coordinate interfacing functions, and provide timely and effective recommendations through the PdM to the PM.

3.0 AUTHORIZATION

Product Manager Charter, UAS, U.S. Department of the Army (DA).

4.0 REFERENCES

- a. AR 385-10, The Army Safety Program, 24 Feb 17.
- b. DA PAM 385-16, System Safety Management Guide, 13 Aug 13.
- c. MIL-STD-882E, System Safety Program Requirements, 11 May 12.
- d. PEO AVN Policy Memorandum Number 13-08, System Safety Risk Management Process 27 September 2013

5.0 TASKS

- a. Oversee the log of System Safety hazards, provide appropriate risk assessments, and track resolution actions. Recommendations to close hazards will be made through the PdM to the PM. Hazard closure shall be in accordance with the current risk management procedures defined in the UAS PM System Safety Management Plan.
- b. Respond to requests by the PdM for recommendations on matters impacting System Safety.
- c. Coordinate with appropriate activities to identify and evaluate those areas in which System Safety implications exist.
- d. Provide recommendations for establishing or revising System Safety requirements.
- e. Identify and tailor the DA documentation applicable to an effective SSP. Tasks are:
 - 1) Ensure integration of tailored System Safety requirements into UAS concerned contracts.
 - 2) Ensure coordination of health concerns with the Army Materiel Command Office of the Surgeon.

- 3) Maintain the SSMP and the SSWG Charter.
- 4) Ensure integration and involvement from associated systems such as Universal products in applicable System Safety activities.
- 5) Ensure that safety issues for test and evaluation are identified and integrated into the appropriate test strategy and plans.
- 6) Coordinate System Safety documentation required for materiel acquisition milestone decisions.
- 7) Ensure corrective and/or acceptance action is taken on all hazards.
- 8) Analyze mishap/incident data for indications of new hazards and for the degree of success with previous assessments and resolution actions.
- 9) Review the status of open hazard corrective actions, including accident findings and SSWG Action Items.
- 10) Coordinate safety deficiencies with the Human Systems Integration Team.

6.0 OPERATION

6.1 Membership

- a. The SSWG will be jointly Co-chaired by the PM, or his designee, and the AMCOM Safety Office Representative.
- b. Primary (regular) members are required to attend each meeting to successfully fulfill the purpose of the group. Primary members are the representatives of the following organizations:
 - 1) Project Office
 - 2) AMCOM Safety Office
 - 3) TCM
 - 4) PEO AVN (SFAE-AV-ET)
 - 5) AED

NOTE: U.S. Army Combat Readiness/Safety Center (CRC) is a designated DA observer (in accordance with AR 385-16).

- c. Associate Members will receive meeting notification and minutes for all meetings. The following Associate Members will only be requested to attend for specific actions in their System Safety area:
 - 1) AMRDEC Human Engineering Division, RAM Engineering and System Assessment Division

- 2) AMRDEC SED
 - 3) AMCOM Environmental Office
 - 4) AMCOM Logistics Center (ALC), UAS Fleet Management Division
 - 5) U.S. Army PHC HHA Program
 - 6) U.S. Army Communications-Electronics Command (CECOM), Intelligence Materiel Management Center
 - 7) U.S. Army Test and Evaluation Command (ATEC)
 - 8) U.S. Army Aeromedical Research Laboratory (USAARL)
 - 9) U.S. Army Aviation Center of Excellence (USAACE) Directorates
 - 10) HSI Representative
- d. Advisory Members are representatives of other organizations, agencies, contractors, suppliers, etc., who will be invited to participate as-required.
 - e. Changes to the SSWG member organizations (primary members) require PM approval. Changes of advisory and associate member organizations will be made as required and approved by the Co-chairmen.

NOTE: Contractor members will be excluded from participation upon request of the Chairman when the potential for conflict of interest exists, proprietary information is discussed, or for other reasons when the propriety of their presence is questioned. The meeting announcement will, when possible, reflect any restrictions.

6.2 Meetings

- a. System Safety Working Group meetings will be held to work on individual issues and will usually include in-depth informational discussions of relevant System Safety issues and advancements. Tasking will be recorded and managed by the PdM to completion.
- b. Primary SSWG member meetings shall also be held at the call of the Safety Manager to assist in identification, definition, assessment, and resolution of immediate System Safety issues. These meetings will normally be held telephonically and are not required to be concurrent conversations. These meetings will be an adjunct to the PdM management team and, with the exception of new hazard list or tracking system input, will be reported under their procedures.

7.0 ADMINISTRATION

- a. Agenda items may be proposed by any organization but will be approved by the PdM Safety Manager. For regularly scheduled SSWG meetings, the agenda and any proposed hazards to be adjudicated will be distributed to the primary members not later than the Friday prior to the meeting.
- b. Minutes will be prepared by the PdM Safety Manager for formal SSWG meetings. Primary SSWG members, and the cognizant Product Manager will review the draft SSWG minutes before they are signed by the PM. A summary of key issues, action items and action agencies will be briefed prior to SSWG meeting termination to assure complete understanding and accuracy.
- c. SSWG recommendations will include minority opinions as applicable.

APPENDIX B - PM UAS Software Safety Minimum Level of Rigor (LOR) Table

Legend:

PR: Prerequisite Requirement-Required Regardless of LOR or required in order to assess and determine LOR
R: Required for Assigned LOR AD: As directed by Customer/Contract
IV&V: Independent Verification and Validation N/A: Not Applicable for this program or LOR

PM-UAS LOR Table								
Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of- Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
SSE-1: Document the Developer plans and processes to meet the requirements of the System Safety and Software System Safety programs. Section 3.0 Process and Process Tasks for Software System Safety MIL-STD-882E, Task 102 AMCOM Reg 385-17 Sections 3.b(1), 3.b(2), Table 1, 4.a(1), 4.a(3), 4.a(10), Table 2	Developer System Safety Manager Developer Software Safety	Developer Program Manager Developer Hardware and Software Design Engineering Developer Software Design Architect Developer Configuration Management	PR					System Safety Program Plan (SSPP) and Software System Safety Program Plan (SwSSPP). SOW, CDRL Acquirer Approved SSPP/SwSSPP
SSE-1.1: Define the safety-related terms (and the definitions) to be used on the program Section 3.1, Prepare the SSPP; Subsections 3.1.1 - 3.1.2 AMCOM Reg 385-17 Sections 3.b(2), 4.a(1), Table 2 [Best Practice]	Acquirer System Safety Manager Developer System Safety Manager Developer Software Design Architect	Developer System Safety Acquirer SSWG Review and Approval	PR					Documented Program-Specific Terms and Definitions. MIL-STD-882E definitions and terms are required unless approved by appropriate authorities Acquirer Approved SSPP
SSE-1.2: Detail within the SSPP/ SwSSPP, how the SwSS tasks will be accomplished within the specific software development life-cycle for the project. Section 3.1.3 Prepare the SSPP MIL-STD-882E, Task 102 AMCOM Reg 385-17 Sections 3.b(2), 3.b(3), Table 1, 4.a(1), 4.a(3), 4.a(5), 4.a(8), 4.a(10), Table 2	Developer Software Safety Developer Software Development	Acquirer SSWG Review and Approval	PR					SOW, CDRL. SSPP/SwSSPP Acquirer Approved SSPP/SwSSPP
SSE-1.3: Develop safety entry/exit criteria for each program phase of the software development life cycle to include concept refinement, requirements, preliminary and detailed design, coding, Test V&V, software release and support). AMCOM Reg 385-17 Sections 3.b(1), 3.b(2), Table 1, 4.a(1), 4.a(6), 4.a(7), 4.a(10), Table 2 [Best Practice]	Developer Software Safety Developer Software Development and Test Configuration Mgmt	Acquirer SSWG Review and Approval	PR					Input to SwSSPP Input to SDP Input to STP Input to CMP Input to SwQAP SSWG Minutes

Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of- Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
SSE-1.4: Develop (or update) the Software Control Category (SCC) Definitions to be used on the program Section 3.1 Prepare the SSPP MIL-STD-882E AMCOM Reg 385-17 Sections 3.b(2), 4.a(1), 4.a(6)	Developer Software Safety Developer Software Development and Test Developer Software Design Architect	Acquirer SSWG Review and Approval	PR					Defined Software Control Category Definitions SwSSPP SSWG Minutes
SSE-1.5: Develop (or update) the Software Criticality Matrix (SCM) for the program Section 3.1 Prepare the SSPP [MIL-STD-882E, Table V] AMCOM Reg 385-17 Sections 3.b(2), Table 1, 4.a(1), 4.a(6), Table 3	Acquirer System Safety Manager Developer Software Safety Developer Software Development and Test Developer Software Design Architect	Acquirer SSWG Review and Approval	PR					SSMP Program Software Criticality Matrix SwSSPP SSWG Minutes
SSE-1.6: Develop (or update) Level of Rigor (LOR) task table for the program to include tasks and work products for each LOR software development phase Section 3.2.2 Prepare Level-of-Rigor Table [MIL-STD-882E, Table V] AMCOM Reg 385-17 Sections 3.b(2), 4.a(1), 4.a(6), Table 3	Developer Software Safety Developer Software Development and Test Developer Software Design Architect	Acquirer SSWG Review and Approval	PR					LOR Table SwSSPP SSWG Minutes
SSE-2: Establish a chartered System Safety Working Group (SSWG) Section 3.1.1 Obtain Inputs from the SSMP [MIL-STD-882E, Task 105] AMCOM Reg 385-17 Sections 3.b(2), Table 1, 4.a(1), 4.a(5), 4.a(6)	Acquirer System Safety Manager Developer System Safety, Software Design Architect, Software Safety, Software Development & Test	Acquirer SSWG	PR					SSMP, SSPP, SSWG Charter and Proceedings
SSE-3: Set-up a Hazard Tracking System (HTS) for the program Section 3.1.1 Obtain Inputs from the SSMP Also, Statement of Work tasks [MIL-STD-882E, Paragraph 4.3.2] AMCOM Reg 385-17 Sections 4.a(6), 4.a(10), Table 2	Developer System Safety	Acquirer SSWG Review and Approval	PR, AD					Hazard Tracking Database SSWG Minutes

Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of- Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
SSE-3.1: Enter each hazard identified into the HTS Section 3.3.1 Identify Hazards Pertaining to the Baseline System to Include the Preliminary System/Software Architecture [MIL-STD-882E, Paragraph 4.3.2] AMCOM Reg 385-17 Sections 4.a(6), 4.a(10), Table 2	Developer System Safety	Acquirer SSWG Review and Approval	PR					Individual Hazard Records of the HTS SSWG Minutes
SSE-3.2: Assign the severity and probability of occurrence to each hazard identified and calculate the initial Mishap Index (MRI) based on the best available data documented, including provisions, alternatives, and mitigation measures to eliminate hazards or reduce associated risk Section 3.3.2 Categorize Hazards with Preliminary Hazard Risk Index [MIL-STD-882E, Para 4.3.3] AMCOM Reg 385-17 Sections 4.a(6), 4.a(8), 4.a(10)	Developer System Safety	Acquirer SSWG Review and Approval	PR					MRI/HRI Assignment for each Hazard Record SSWG Minutes
SSE-4: Perform a Preliminary Hazard Analysis (PHA) to identify the top level safety mishaps and hazards and top-level safety mitigation requirements Section 3.3 Preliminary Hazard Analysis (PHA) [MIL-STD-882E, Task 202] AMCOM Reg 385-17 Sections 4.a(6), 4.a(8), 4.a(10), Table 2	Developer System Safety	Acquirer SSWG Review and Approval	PR					List of Top-Level Mishaps List of Hazards and Hazard Failure Modes Preliminary Hazard Analysis (PHA) SSWG Minutes
SSE-5: Perform a Functional Hazard Analysis (FHA) to identify the safety-significant functions and provide inputs or updates to the PHA Section 3.4 Functional Hazard Analysis (FHA) [MIL-STD-882E, Task 208] AMCOM Reg 385-17 Sections 4.a(6), 4.a(10), Table 2	Developer System Safety	Acquirer SSWG Review and Approval	PR					Functional Hazard Analysis (FHA) List of Safety-Significant Functions LOR Assignment to Safety-Significant Functions SSWG Minutes

Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of- Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
SSE-7: Perform a System Hazard Analysis (SHA) and accomplish an in-depth causal, interface, and failure mode analysis of the identified hazards to identify specific hardware, software, and humanrelated causes and the safety mitigating requirements to eliminate or control them. Section 3.7 Perform In Depth Hazard Analysis [MIL-STD-882E, Task 205] AMCOM Reg 385-17 Sections 4.a(8), 4.a(10), Table 3	Developer System Safety	Developer Software Safety	PR					System Hazard Analysis
SSE-8: Perform a Sub-System Hazard Analysis and accomplish an in-depth causal, interface, and failure mode analysis of the identified hazards to identify specific hardware, software, and humanrelated causes and the safety mitigating requirements to eliminate or control them. Section 3.7 Perform In Depth Hazard Analysis [MIL-STD-882E, Task 204] AMCOM Reg 385-17 Sections 4.a(8), 4.a(10)	Developer System Safety	Developer Software Safety	PR AD					Subsystem Hazard Analysis for individual subsystems
SSE-9: Perform initial FTA/Event Tree/Logic Diagram on prioritized hazards Section 3.7 Perform In Depth Hazard Analysis AMCOM Reg 385-17 Sections 4.a(6), 4.a(10), Table 3 [Best Practice]	Developer System Safety	Developer Software Safety	PR, AD					Fault Tree Analysis on prioritized (by SSWG) mishaps or hazards
SSE-10: Perform a System-of-System Hazard Analysis (SoS) to identify unique SoS hazards Section 3.7 Perform In Depth Hazard Analysis [MIL-STD-882E, Task 209] AMCOM Reg 385-17 Sections 4.a(6), 4.a(10), Table 2, Table 3	Developer System Safety	Developer Software Safety	PR, AD					SoS Hazard Analysis

Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of- Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
SSE-12: Review of all Software Trouble Reports for safety applicability to safety-significant functions and mishaps/hazards (STR) Section 3.12.3 Monitor Test Defects and Corrective Actions, 3.12.4 Review Final Software Test Results [MIL-STD-882E, Task A87304] AMCOM Reg 385-17 Sections 4.a(8), 4.a(10)	Developer System Safety	Developer Software Development and Test Developer Software Design Architect	PR					STR Review Results NOTE: Refer to subsequent Life-Cycle (LC) Support Tasks required to support sustainment after design is put under Configuration Control
SSE-13: Produce Safety Case or Safety Assessment Report as directed by the customer (SAR). Ensure the SAR captures all of the relevant SSS elements applicable to the system assessed Section 3.0 Process and Process Tasks for Software System Safety [MIL-STD-882E, Task 301] AMCOM Reg 385-17 Sections 4.a(6), 4.a(10)	Developer System Safety	Developer Software Safety	PR, AD					Safety Case Safety Assessment Report SSWG Minutes
SSE-14: Maintain records of compliance with the tailored program safety requirements. [MIL-STD-882E, Tasks 102, and 104] AMCOM Reg 385-17 Sections Table 1, 4.a(6), 4.a(9), 4.a(9)(b), 4.a(10), Table 2	Developer Software Safety Software Quality Assurance Developer Software Development & Test	Acquirer SSWG Review and Approval	PR, AD					All System Safety and Software Safety Engineering Artifacts SSWG Minutes SQA Audits and Results
REQUIREMENTS PHASE (RP) TASKS								
RP-1: Review generic software safety requirements from other standards, including coding standards or industry best practice and identify the software safety requirements that are deemed appropriate for the system/software. Tag and track these Software Safety Requirements in the Requirements Traceability Management (RTM) tool Section 3.6.3 Identify and Tag Generic Safety Significant Requirements [MIL-STD-882E, Task 203] AMCOM Reg 385-17 Sections 4.a(6), 4.a(8), Table 2, Appendix D	Developer System Safety Developer Software Safety	Acquirer Review and Approval		R	R	R	R	List of Generic Safety-significant Requirements documented in RTM tool SSWG Minutes

Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of- Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
RP-2: Review System Requirements Specification (SRS), and identify the functional requirements that contribute to the hazards. Tag and track these safety-significant Requirements in the Requirements Traceability Management (RTM) tool Section 3.6.1 Review System and Functional Specifications Section 3.6.2 Identify and Tag Contributing Safety Significant Requirements (CSSR) [MIL-STD-882E, Task 203] AMCOM Reg 385-17 Sections 4.a(8), Table 2, Appendix D	Developer System Safety Developer Software Safety			R	R	R	R	List of Contributing Safety-significant Requirements documented in the RTM Tool
RP-3: From the FHA and the PHA Analyses, derive high-level safety requirements to mitigate identified hazards and failure modes. Tag and track these mitigating safety-significant Requirements in the Requirements Traceability Management (RTM) tool. Section 3.6.4 Identify and Tag Mitigating Safety Significant Requirements (MSSR) [MIL-STD-882E, Task 202, 203, and 208] AMCOM Reg 385-17 Sections 4.a(8), Table 2, Appendix D	Developer System Safety Developer Software Safety			R	R	R	R	List of Derived Safety-significant (high-level) Requirements
RP-4: Determine Software Criticality and assign an LOR to each Safety-significant Requirement based on the software control category and the highest severity of the associated hazard (functional contribution) Section 3.5 LOR Allocations to Safety Significant Functions [MIL-STD-882E, Task 203] AMCOM Reg 385-17 Sections Table 1, 4.a(8), 4.a(9)(d), Table 3, 5.c(1), 5.c(5), Appendix D	Developer Software Safety	Developer Software Requirements		R	R	R	R	LOR Assignments for Each Safety-Significant Requirement

Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of- Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
RP-5: Create traceability matrix from safety significant requirements (generic, contributing or mitigating requirements) to identified hazards Section 3.6 Preliminary Safety Requirements Analysis (SRA) Section 3.9 Perform Safety Requirements Traceability [MIL-STD-882E, Task 203] AMCOM Reg 385-17 Sections 4.a(4), 4.a(6), 4.a(8), Table 3, Appendix D	Developer System Safety Developer Software Safety	Acquirer Review and Approval		R	R	R	R	Requirements-to-Hazards Traceability Artifact SSWG Minutes
RP-6: Ensure that SwSS requirements (generic, contributing, or mitigating) are flowed down and traceable to the lower level software requirements specifications (SRS) safety requirements, as they are developed. Section 3.6 Preliminary Safety Requirements Analysis (SRA) [Summary Task for RP-1 to RP-3] AMCOM Reg 385-17 Sections 3.b(3), 4.a(4), 4.a(8), Appendix D	Developer System Safety	Developer Software Safety		R	R	R	R	Requirements-to-Specifications Traceability Artifacts
RP-7: Derive requirements to insure that safety significant interfaces are validated and controlled at all times AMCOM Reg 385-17 Section 4.a(4) [Best Practice]	Developer Software Requirements	Developer Software Safety Developer Software Design Architect				R	R	Functional and Physical Design Interface Analysis
RP-8: Coordinated Safety-significant Requirements Review for correctness and completeness AMCOM Reg 385-17 Sections 3.b(1) Figure 1, 4.a(8), 4.a(9)(a), 4.a(9)(b), 4.b(3) [Best Practice]	Developer Software Requirements	Developer Software Safety Developer Software Design Architect				R	R	Safety Requirements Review
RP-9: Derive high-level requirements for a fault tolerant design and tag as Derived Safety significant Requirements AMCOM Reg 385-17 Section 4.a(4) [Best Practice]	Developer Software Requirements	Developer Software Safety Developer Software Design Architect					R	Derived Fault Tolerant Requirements

Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of- Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
RP-10: Independent review of all Contributing, Generic, and Mitigating Software Safety Requirements MIL-STD-882E Tasks 101.2.5, 102.2.8.c, Appendix B B.2.2.5.b AMCOM Reg 385-17 Sections 4.a(9)(b), 4.b(3), 4.b(4) [Best Practice]	Someone Other Than the Developer	Independent Software Safety	IV&V, AD					Independent Safety Requirements Review
RP-11: Define the verification method (inspection, demonstration, analysis, or test) for each Safety-Significant Requirement AMCOM Reg 385-17 Sections Figure 3, Table 3, 4.c(5), Appendix D [Best Practice]	Developer Software Requirements	Developer Software Safety Developer Software Design Architect		R	R	R	R	Requirements Traceability Matrix (includes verification method) SW Development and Test Artifacts
DESIGN PHASE (DP) TASKS								
DP-1: Update all analyses (PHA, FHA, SRA, SSRA, SHA, and FTA) for depth and fidelity based on the maturing design concepts in the design phase of the program Section 3.3 – 3.8 [MIL-STD-882E, Tasks 202, 203, 204, 205, 208] AMCOM Reg 385-17 Sections 4.a(8), 4.a(10), Table 2	Developer System Safety	Developer Software Safety Acquirer Review and Approval	RP, AD					Updated safety engineering analysis artifacts Acquirer Approval
DP-2: From DP-1, identify and add to the SRS generic safety and coding standard requirements for fault detection, isolation, annunciation, and tolerance, error logging, and safe state transitions, and tag these as Mitigating Safety-significant Requirements Section 3.6.3 AMCOM Reg 385-17 Section Table 3 [Best Practice]	Contactor System Safety	Developer Software Safety Developer Hardware and Software Design Engineering Developer Software Development and Test Developer Software Design Architect			R	R	R	List of Safety-Specific Requirements Considered to be Safety Best Practice

Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of- Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
DP-3: From DP-1 and DP-2, identify and add to the SRS mitigating software requirements for hazards causal factors, and tag these as Mitigating Software Safety Requirements or defects against existing high-level Safety significant Requirements. Section 3.6.4 AMCOM Reg 385-17 Section 4.a(8) [Best Practice]	Contactor System Safety	Developer Software Safety Developer Software Design Architect		R	R	R	R	Derived Safety Requirements OR Defects against existing Safety Requirements
DP-4: From DP-2 and DP-3, document the newly derived safety-significant requirements in the RTM tool, and track, and trace these requirements to design implementation. Section 3.6.2-3.6.4 AMCOM Reg 385-17 Section 4.a(8) [Best Practice]	Contactor System Safety	Developer Software Safety Developer Software Design Architect		R	R	R	R	RTM Tool Update Software Design Artifacts
DP-5: Review the design for compliance with the corporate safety design standards and guidelines, and Acquirer directed best practices (i.e., STANAG 4404, Appendix E of the JSSSEH, etc) AMCOM Reg 385-17 Sections 3.b(3), Appendix A, Appendix E 1.1.5 [Directed Best Practice]	Acquirer System and Software Safety Developer System and Software Safety	Developer Software Design Architect Acquirer SSWG Review and Approval			R	R	R	As directed Assessment of Compliance Artifact
DP-6: Review of the user interface design for safety-significant issues AMCOM Reg 385-17 Sections 4.a(4), 6.b.B Code interface analysis [Best Practice]	Developer System Safety Developer Software Safety	Developer Hardware and Software Design Engineering Developer Human Factors				R	R	Assessment of User Interfaces with Software Functionality
DP-7: Create traceability from all safety significant requirements to the system and software architecture Section 3.6 Section 3.9 AMCOM Reg 385-17 Section 4.a(8), Table 3 [Best Practice]	Developer Software Design Architect	Developer Software Safety		R	R	R	R	Safety Requirements-to-design Traceability

Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of- Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
DP-8: Functionally partition all implementations of high LOR requirements from lower LOR requirements in the design AMCOM Reg 385-17 Sections 3.b(2), 4.a(1), 4.a(6), Table 3 [Best Practice]	Developer Software Design Architect	Developer Software Safety				R	R	Functionally Partitioned Design in Design Documentation Artifacts
DP-9: Assess design's stress tolerant (i.e., memory, processing through-put, timing, etc). Make appropriate recommendations to update requirements for stress tolerant design. AMCOM Reg 385-17 Sections 6.b.H, 6.b.A-F [Best Practice]	Developer Software Design Architect	Developer Software Safety Developer Software Requirements and Design				R	R	Stress Tolerant Design
DP-10: Perform Design Interface Analysis to evaluate internal and external interfaces of safety-critical units to ensure functional and physical compatibility across the interface. AMCOM Reg 385-17 Sections 4.a(4), 6.b.B Code interface analysis, 6.b.H, 6.b.B Code interface analysis [Best Practice]	Developer Software Design Architect	Developer Software Safety					R	Verification that the design controls the functional and physical interfaces with safety significant functionality
DP-11: Analyze all safety functional threads to ensure that all paths lead to their desired outcomes and that there is no dead/unused code, unused/undesired entry/exit points into/out of the software thread AMCOM Reg 385-17 Sections 4.a(8), 6.b.A, Appendix D [Best Practice]	Developer Software Design Architect	Developer Software Safety					R	Safety (functional) Thread Analysis
DP-12: Verify that every variable and functional statement in safety-critical modules of code have a predefined behavior that fulfill the criteria of the functional objective AMCOM Reg 385-17 Section Table 3, Appendix D [Best Practice]	Developer Software Design Architect	Developer Software Safety					R	Safety-specific Behavioral Review Results for Safety-Critical Modules of Code
DP-13: Independent Safety Review of Requirements-to-Design for Safety Coverage AMCOM Reg 385-17 Section Table 3 [Best Practice]	Someone Other Than System Safety Team	Independent Software Safety Independent Software Design	IV&V, AD					Independent Safety Review of Requirements-to-Design Coverage Artifact
IMPLEMENTATION (CODING) PHASE (IP) TASK								

Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of- Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
IP-1: Update existing FTA/Event Tree/Logic Diagram on prioritized hazards [MIL-STD-882E] AMCOM Reg 385-17 Sections 4.a(8), Table 3	Developer System Safety	Developer Software Safety	R, AD					Updated FTA/Event Tree/Logic Diagram on Prioritized Hazards
IP-2: Update all Hazard Analyses to include the in-depth causal analysis that reflects the mature(ing) design Section 3.3 – 3.8 [MIL-STD-882E, Tasks 204, 205] AMCOM Reg 385-17 Section Table 3	Developer System Safety	Developer Software Safety	RP, AD					Updated Hazard Analysis
IP-3: Update Safety Case or Safety Assessment Report (SAR) as required by Customer [MIL-STD-882E, Task 301] AMCOM Reg 385-17 Sections 4.a(10), Table 3	Developer System Safety	Developer Software Safety	RP, AD					Updated Safety Case or Safety Assessment Report
IP-4: Participate in Test Readiness Reviews AMCOM Reg 385-17 Sections 3.b(1), 4.a(10) [Best Practice]	Developer System Safety	Developer Software Safety			R	R	R	Test Readiness Review Artifacts
IP-5: Mark safety-significant code header with the appropriate safety-criticality or LOR assignment AMCOM Reg 385-17 Sections 3.b(2), 4.a(1), 4.a(6), Table 3 [Best Practice]	Developer Software Developer	Developer Software Safety		R	R	R	R	Code Headers Reflect Correct Safety Significance
IP-6: Perform high-level reviews of code for compliance with safety-significant coding standards and guidelines (e.g. MISRA) AMCOM Reg 385-17 Section 4.a(10) [Best Practice]	Developer Software Developer	Developer Software Safety Developer Software QA	RP					Artifacts Demonstrating Compliance with Best Practices for Safety-Critical Code Development
IP-7: Perform detailed code walkthroughs and analysis of safety-critical code Section 3.10 Perform Code Level Safety Analysis AMCOM Reg 385-17 Section 4.a(8) [Best Practice]	Developer Software Design Architect Developer Software Developer	Developer Software Safety					R	Code Level Review Results

Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of- Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
IP-8: Create traceability from code to safety significant design requirements Section 3.9 AMCOM Reg 385-17 Section 4.a(8), Appendix D [Best Practice]	Developer Software Design Architect Developer Software Developer	Developer Software Safety		R	R	R	R	Requirements-to-Code Traceability
IP-9: Participate in acceptance review of safety significant code AMCOM Reg 385-17 Section 4.a(8) [Best Practice]	Developer Software Safety	Developer Software Developer and Software Test			R	R	R	Acceptance Review of Safety significant Software
IP-10: Independent Safety Review of Safety-Significant Code Section 3.10 Perform Code Level Safety Analysis [MIL-STD-882E] AMCOM Reg 385-17 Section 4.a(8)	Independent Design	Independent Software Safety	IV&V, AD					Safety Code-Level Review
IP-11: Perform detailed code inspections for fault contributions of Safety-Significant Code Section 3.10.4 Analyze the Safety-critical code AMCOM Reg 385-17 Section 4.a(8) [Best Practice]	Software Development Team	Software Test Software Safety					R	Safety Code-Level Analysis for Fault Management
IP-12: Review unit test plan to ensure that it defines the requirements for testing units of safety-significant code Section 3.11.2 Ensure Safety Functionality is Tested AMCOM Reg 385-17 Sections 6.b.H, 6.b.A-F [not unit test specific] [Best Practice]	Developer Software Safety			R	R	R	R	Assessment of Unit Test Plan for Requirements Definition
IP-13: Execute unit tests AMCOM Reg 385-17 Sections 6.b.H, 6.b.A-F [not unit test specific] [Best Practice]	Developer Software Developer			R	R	R	R	Documented results of Unit Test Execution
IP-14: Unit test results review AMCOM Reg 385-17 Sections 6.b.H, 6.b.A-F [not unit test specific] [Best Practice]	Developer Software Developer	Developer Software Safety		R	R	R	R	Assessment of Unit Test Results

Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of- Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
IP-15: Review unit test results and verify that the unit tests provide the required unit test coverage and were executed in compliance with the unit test plan AMCOM Reg 385-17 Sections 6.b.H, 6.b.A-F [not unit test specific] [Best Practice]	Developer Software Test	Developer Software Safety		R	R	R	R	Documented results of Unit Test Review
TEST PHASE (TP) TASKS								
TP-2: Mark safety-significant test cases with the appropriate LOR AMCOM Reg 385-17 Sections Table 3, Table 4 [Best Practice]	Developer System Safety	Developer Software Test			R	R	R	Evidence within the Safety-Specific Software Test Cases
TP-3: Perform a safety review of each test case 3.11 Perform Software Test Planning AMCOM Reg 385-17 Sections 4.a(5), Table 3 [Best Practice]	Developer System Safety				R	R	R	Safety Review Results
TP-4: Review all requirements traceability matrices for coverage and completeness AMCOM Reg 385-17 Sections 4.a(8), Table 3, Table 4 [Best Practice]	Developer System Safety	Developer Software Safety			R	R	R	Requirements Traceability Review Results
TP-5: Develop software test case procedures to demonstrate software structure (statement coverage) is achieved AMCOM Reg 385-17 Sections Table 3, Table 4, 6.b.A-F [Best Practice]	Developer Software Test	Developer Software Design Architect Developer Software Safety			R	R	R	Evidence within the Software Test Plan Documented Code Structural Coverage evidence
TP-6: Develop software test case procedures to demonstrate software structure (condition/decision coverage(C/DC)) is achieved. AMCOM Reg 385-17 Section Table 3 [Best Practice]	Software Test Software Design	Software Safety				R	R	Safety-Specific Software Test Cases Documented Code Structural Coverage evidence
TP-7: Develop software test case procedures to demonstrate software structure (modified condition/decision coverage (MC/DC)) is achieved. AMCOM Reg 385-17 Section Table 3 [Best Practice]	Developer Software Test	Developer Software Design Architect Developer Software Safety					R	Safety-Specific Software Test Cases Documented Code Structural Coverage evidence

Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of- Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
TP-8: Perform a software structural coverage analysis to demonstrate that the appropriate level of software structural coverage, including data coupling and control coupling, has been achieved. AMCOM Reg 385-17 Section Table 3 [Best Practice]	Developer Software Test	Developer Software Design Architect Developer Software Safety				R	R	Safety-Specific Software Test Cases Documented Code Structural Coverage evidence
TP-9: Develop software test cases to demonstrate that the software satisfies its requirements and those anomalous conditions or software errors cannot lead to a hazardous condition as identified by the Hazard Analyses from the System Safety process. AMCOM Reg 385-17 Section Table 3, Table 4, Appendix D [Best Practice]	Developer Software Test	Developer Software Design Architect Developer Software Safety				R	R	Safety-Specific Software Test Cases
TP-10: Each software requirement identified as safety significant in the System Safety Hazard Analysis process shall be traced to a test case and each test case shall trace back to a software requirement. AMCOM Reg 385-17 Sections 4.a(8), 4.a(10), Table 4 [Best Practice]	Developer Software Test	Developer Software Design Architect Developer Software Safety				R	R	Safety-Specific Software Test Cases

Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of- Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
TP-11: Develop software test cases to demonstrate the ability of the software to correctly respond to off-nominal, robustness, and failure mode conditions as identified by the system Safety Hazard Analysis process. Off Nominal and robustness conditions that must be considered are: abnormal, out-of-bounds, and invalid variable input values including zero, zero crossing and approaching zero from either direction or similar values of trig functions; proper state transitions and possible disallowed state or mode transitions; system initialization under abnormal and failure conditions; errors in input values or counters associated with time or rate functions and algorithms; failure modes of input data strings and messages; out of range loop counters and other loop failure conditions; exception handling correctness; fault and error handling correctness AMCOM Reg 385-17 Sections 4.a(10), Table 3, Table 4, 6.b.A-H, Appendix D [Best Practice]	Developer Software Test	Developer Software Safety				R	R	Safety-Specific Software Test Cases
TP-12: Perform a software test coverage analysis to demonstrate that test case procedures meet the requirements based test coverage criteria: a test case exist for each software requirement; test cases satisfy the criteria for normal; robustness, and failure mode testing; all test procedures used to satisfy structural coverage are traced to requirements; and that requirements or structural coverage deficiencies are resolved by identification or new requirements or new test cases. AMCOM Reg 385-17 Sections 4.a(8), Table 3, Table 4, Appendix D [Best Practice]	Developer Software Test	Developer Software Safety				R	R	Safety Requirements-to-Test Cases Trace

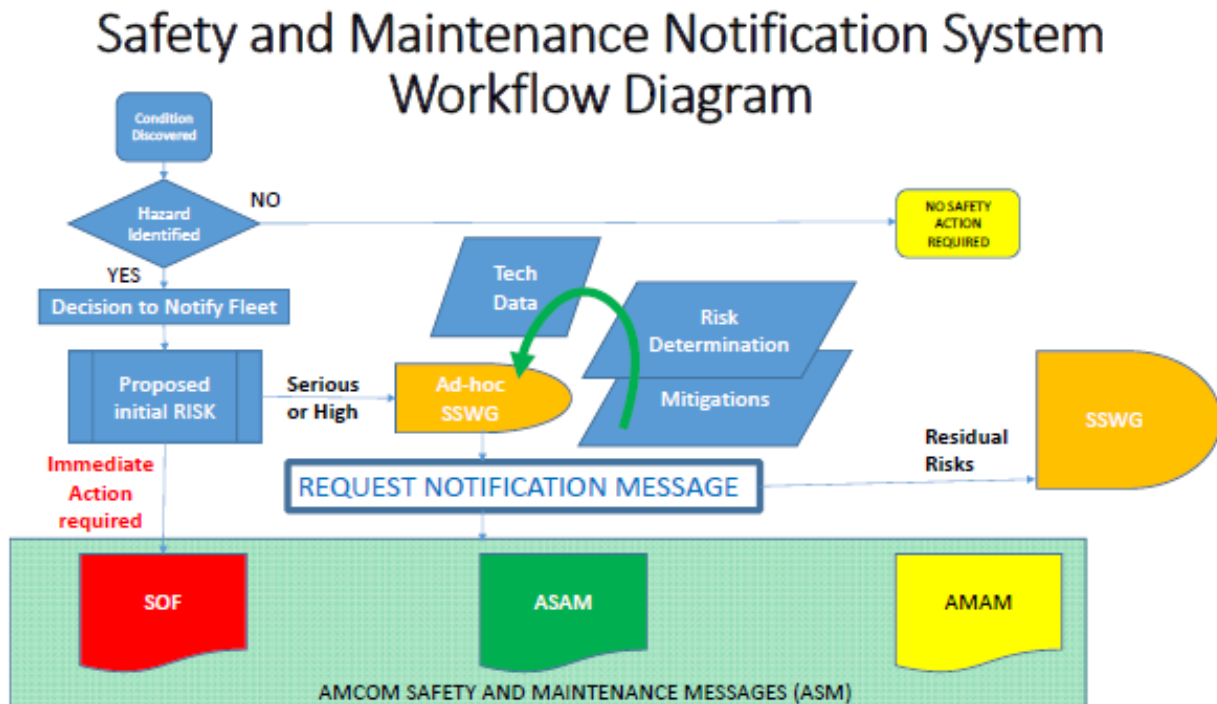
Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of- Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
TP-13: Create a safety-significant test report documenting the safety-significant formal testing compliance and execution results AMCOM Reg 385-17 Sections Table 3, Table 4, Appendix D [Best Practice]	Developer Software Test	Developer Software Safety		R	R	R	R	Safety-Critical Test Report
TP-14: Review safety-significant test results and verify that the safety-significant test cases provide the required test coverage and were executed in compliance with the formal test plans. AMCOM Reg 385-17 Sections Table 3, Table 4 [Best Practice]	Developer Software Test	Developer Software Safety Developer Software Quality			R	R	R	Verification of Test Case Implementation
TP-15: Track safety verification failures and participate in test anomaly resolution Section 3.12.3 Process Subtask 12.3: Monitor Test Defects and Corrective Actions AMCOM Reg 385-17 Sections 4.a(10), Table 3, Table 4 [Best Practice]	Developer Software Design Developer Software Test	Developer Software Safety			R	R	R	Attendance Log
TP-16: Plan, perform, and review functional and Failure Modes and Effects Test (FMET) regression test plans and procedures. Section 3.12.4 Review Final Software Test Results AMCOM Reg 385-17 Sections 4.a(8) [Best Practice]	Developer Software Design Developer Software Test	Developer Software Safety			R	R	R	Regression Test Plans and Procedures
TP-17: Add test cases to the Regression Test Plan to support 100% regression testing AMCOM Reg 385-17 Section 6.b.F Complete regression testing [doesn't specify 100%] [Best Practice]	Developer Software Test	Developer Software Design Developer Software Safety			R	R	R	Regression Test Plans and Procedures
TP-18: Perform 100% regression testing Regression testing must include testing of nonpartitioned non-safety-significant software at the same LOR as the safety-significant software. AMCOM Reg 385-17 Sections 6.b.F Complete regression testing [doesn't specify 100%], Appendix D [Best Practice]	Developer Software Test	Developer Software Safety			R	R	R	Regression Test Results or Report

Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of- Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
TP-19: Calculate and document the residual safety risk (after mitigation) Section 3.13 Perform Residual Safety Risk Assessment [MIL-STD-882E, Task 301] AMCOM Reg 385-17 Sections 4.a(10), Table 3	Developer System Safety	Developer Software Safety		R	R	R	R	Residual Safety Risk Assessment
TP-20: Gain accreditation and validation of models and simulations that are used to support software system safety verification in accordance with DoDI 5000.61, DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A). AMCOM Reg 385-17 Section 4 [Best Practice]	Developer Software Engineering					R	R	
TP-21: Validate models and simulations against actual hardware and data. AMCOM Reg 385-17 Section 4 [Best Practice]	Developer Software Engineering					R	R	
LIFE CYCLE (LC) SUPPORT PHASE TASKS								
LC-1: Review of all Engineering Change Proposals for safety applicability to safety-significant functions and mishaps/hazards (ECP) Section 3.14 Participate in Life-cycle Management and Support [MIL-STD-882E, Task 304] AMCOM Reg 385-17 Sections 4.a(5), 4.a(8), 4.a(10)	Developer System Safety Team	Developer Software Safety	RP					ECP Review Results with System Safety assessment indicated
LC-2: Identify and track safety-significant requirements to mitigate the safety risk potential of the Software Trouble Reports (STRs) or Engineering Change Proposals (ECPs) being processed. Section 3.13.3 Assess Partial Mitigation or Failure to Mitigate, Section 3.14 [MIL-STD-882E, Task 304] AMCOM Reg 385-17 Sections 4.a(5), 4.a(10)	Developer System Safety Team	Developer Software Safety	RP					

Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of- Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
LC-3: Update SSHA, SHA, and FHA (as required) Section 3.14.6 Update all Safety Related Artifacts [MIL-STD-882E, Task 204, 205, 208] AMCOM Reg 385-17 Sections 4.a(8), 4.a(10), Table 5	Developer System Safety Team	Developer Software Safety	R, AD					Updated FHA Updated SSHA and SHA NOTE: If the safety analysis has NOT been accomplished on the system (e.g., legacy system), then it must be accomplished now)
LC-4: Update the FTA (as required) Section 3.14.6 [MIL-STD-882E] AMCOM Reg 385-17 Sections 4.a(8), Table 4, Table 5, Appendix D	Developer System Safety Team	Developer Software Safety	R, AD					Updated FTA
LC-5: Update the HTS (as required) Section 3.14.6 [MIL-STD-882E] AMCOM Reg 385-17 Sections 4.a(10), Table 2, Table 4, Table 5, Appendix D	Developer System Safety Team	Developer Software Safety	R, AD					Updated HTS
LC-6: Participate in Configuration Management process and Configuration Control Board (CCB) AMCOM Reg 385-17 Sections 4.a(10), Table 2, Table 4, Appendix D [Best Practice]	Developer System Safety Team	Developer Software Safety	RP					Safety Review and Approval of ECPs and STRs
LC-7: Mark safety-significant software ECPs and items in CM with the appropriate LOR as determined by the criticality AMCOM Reg 385-17 Sections 4.a(5), 4.a(10), Table 2, Table 5 [Best Practice]	Developer Software Safety	Developer Configuration Management Developer Software Design Architect	RP					ECP Review Results
LC-8: Review problem reporting/defect tracking, change control, and change review activities for safety impact and compliance AMCOM Reg 385-17 Sections 4.a(5), Table 3, 4.c(3), Table 5 [Best Practice]	Developer Software Safety	Developer Configuration Management Developer Software Design Architect	RP					Software Trouble Report and Defect Tracking Results
LC-9: Document the results of any Safety Reviews AMCOM Reg 385-17 Sections 3.b(1), 4.a(10), Table 5 [Best Practice]	Developer Software Safety	Developer Software Safety	RP					Safety Review Results

Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of- Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
Note: Regression testing must be performed on all changed or modified software in system sustainment. See TP-18 and TP-19 AMCOM Reg 385-17 Section 6.b.F					R	R	R	Regression Test Plans Regression Test Results
LC-10: Review Test Reports [Safety, Test] AMCOM Reg 385-17 Section 4.a(10), Table 3 [Best Practice]	Developer System Safety Team	Developer Software Safety	RP					Test Report Review
LC-11: Review and give signature approval on safety-significant CRs AMCOM Reg 385-17 Section 3.b(1), 4.a(10) [Best Practice]	Developer System Safety Team	Developer Software Safety	RP					Safety-significant CR Signature from Software Safety
LC-12: Independently review safety-significant code changes implemented by ECPs within the CM process AMCOM Reg 385-17 Section 3.b(1), 4.a(5), 4.a(10), Table 2 [Best Practice]	Someone Other Than Designer/Developer		IV&V, AD					Independent Safety Review Results

APPENDIX C - Safety and Maintenance Notification System (UAS Workflow Diagram)



APPENDIX D – System Safety Risk Assessment (Example Format)

(For Acceptance of Serious and High Risk)

PART I

1. Item/System Description

2. Hazard

For each residual hazard, provide the following:

- a. Hazard Identification.
- b. Hazard Description (including source, mechanism and outcome).
- c. Hazard Classification (Severity and Frequency according to PEO AVN 13-08).
- d. Source Documentation or Reference.
- e. Alternatives. Actions that could reduce hazard level.

3. PM recommendations/signature.

PART II

AMCOM Safety recommendations/signature.

PART III

Airworthiness Authority, (AMCOM Commander) recommendations/signature.

PART IV

Combat Developer, (Aviation Center) recommendations/signature.

PART V

(Serious Risk) Decision of Materiel Developer, PEO AVN; or
(High Risk) Materiel Developer, PEO AVN recommendations/signature.

PART VI

(High Risk) Decision of Army Acquisition Executive.

APPENDIX E - SSSTRP Finding/Assessment Response (Template)

1. Description of the deficiency:
2. Material Hazard identified: (indicate one) NONE/HAZTRACK#_____
3. Efforts planned to address/resolve the deficiency
4. Detailed overview of the required resources to include cost and schedule
5. Interim mitigations
6. SED FLARE tool
 - a. Probabilistic assessment results:
 - b. Current level of confidence:
7. Date Reviewed by the SSWG
8. Risk acceptance documents completed:
 - a.
 - b.
 - c.
9. Planned end state and completion date.