

Department of the Army
Pamphlet 385-16

Safety

System Safety Management Guide

Headquarters
Department of the Army
Washington, DC
13 November 2008

UNCLASSIFIED

SUMMARY of CHANGE

DA PAM 385-16
System Safety Management Guide

This major revision dated 13 November 2008--

- o Updates guidance on the revised Army system safety and engineering and management policy (para 1-1).
- o Reflects realignment of key Army staff system safety responsibilities, and reorganization of the research, development, and acquisition process (para 1-4).
- o Provides guidance on the 5 step composite risk management processes (para 2-1 and fig 2-1).
- o Provides guidance on communication of risk between mishap risk management and composite risk management (paras 2-2 and 2-3).
- o Update terminology in the system safety program (paras 2-12 through 2-17).
- o Updates Human Factors Engineering portion as a domain in Manpower and Personnel Integration (para 3-6).
- o Defines Manpower and Personnel Integration and its key objectives in the System Safety Interface (para 3-8).
- o Provides a Independent Safety Assessment Program and the effectiveness of the system safety program evaluation tool (app I).


Safety

System Safety Management Guide

By Order of the Secretary of the Army:

GEORGE W. CASEY, JR.
General, United States Army
Chief of Staff

Official:


JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army

History. This publication is a major revision.

Summary. This pamphlet implements Army guidance and procedures for conducting system safety programs in accordance with Army Regulation 385–10.

Applicability. This pamphlet applies to the Active Army, the Army National Guard/Army National Guard of the United

States, the U.S. Army Reserve, and Department of Army civilian employees, unless otherwise stated. It also applies to all Department of Defense personnel and foreign military personnel working with and under Army operational control. It applies to all Army materiel systems and facilities during all phases of the life cycle. The concepts also applies to smaller procurement and acquisition programs such as those done at installation level. Medical-related materiel may require more intensive management, including coordination with other government agencies.

Proponent and exception authority.

The proponent for this pamphlet is the Chief of Staff, Army. The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this pamphlet by providing justification that includes a full analysis of the expected benefits and must include formal

review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Director, Army Safety (DACS–SF), 200 Army Pentagon, Washington, DC 20310–0200.

Distribution. This pamphlet is available in electronic media only and is intended for command levels C, D, and E for the Active Army, Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Part One

System Safety Management, page 1

Chapter 1

System Safety Management, page 1

Purpose • 1–1, page 1

References • 1–2, page 1

Explanation of abbreviations and terms • 1–3, page 1

Participants/key players • 1–4, page 1

Army Safety Action Team • 1–5, page 3

Chapter 2

Risk and Hazard Management, page 4

* This pamphlet supersedes DA Pamphlet 385–16, 4 September 1987.

Contents—Continued

Section I

Risk Management, page 4

Composite risk management • 2-1, page 4

Mishap risk management • 2-2, page 5

Identify hazard • 2-3, page 5

Assess hazard • 2-4, page 7

Develop controls and make risk decisions • 2-5, page 8

Implement controls • 2-6, page 12

Supervise and evaluate • 2-7, page 13

Hazard tracking • 2-8, page 13

Hazard closeout • 2-9, page 14

Objectives for the program executive officer/program manager/materiel developer/Life Cycle Management Command/ combat developer during system safety mishap risk management • 2-10, page 14

Section II

System Safety Program Management Activities within the Life Cycle, page 15

Program elements • 2-11, page 15

Adapting the system safety program • 2-12, page 19

Concept refinement phase • 2-13, page 20

Technology development phase • 2-14, page 21

System development and demonstration phase • 2-15, page 24

Production and deployment phase • 2-16, page 25

Operations and support phase • 2-17, page 26

Chapter 3

Integration of System Safety Associated Disciplines, page 26

General • 3-1, page 26

Reliability, availability, and maintainability • 3-2, page 26

Quality engineering • 3-3, page 27

Integrated logistic support • 3-4, page 27

Combat survivability • 3-5, page 27

Human factors engineering • 3-6, page 28

Health hazards • 3-7, page 28

System safety in the MANPRINT process • 3-8, page 29

Environment • 3-9, page 30

Chapter 4

System Safety for Testers and Evaluators, page 30

Section I

Introduction, page 30

General • 4-1, page 30

Definition • 4-2, page 30

Section II

Test Planning, page 31

Adaptation • 4-3, page 31

Checklists • 4-4, page 31

Test integration • 4-5, page 31

Section III

Conduct of Test, page 31

General • 4-6, page 31

Developmental tests • 4-7, page 31

User tests • 4-8, page 32

Contents—Continued

Non-developmental item tests • 4–9, *page 32*

Section IV

Evaluations, page 32

Independent evaluators • 4–10, *page 32*

U.S. Army Combat Readiness Center independent safety assessment • 4–11, *page 32*

Part Two

Facility System Safety, page 33

Chapter 5

Facility System Safety Management, page 33

Objectives • 5–1, *page 33*

Participants • 5–2, *page 33*

Chapter 6

Facility System Safety Program Management, page 34

General • 6–1, *page 34*

Background • 6–2, *page 34*

Using or activity installation responsibilities • 6–3, *page 34*

Engineering organization responsibilities • 6–4, *page 35*

Design agent functions • 6–5, *page 36*

Standard designs • 6–6, *page 37*

Self-help projects • 6–7, *page 37*

Construction facility system safety • 6–8, *page 37*

Facility/project operation and maintenance • 6–9, *page 37*

Chapter 7

Facility System Safety Program Contracting, page 38

General • 7–1, *page 38*

Contractor selection • 7–2, *page 38*

Task selection • 7–3, *page 38*

System Safety Program Plan • 7–4, *page 38*

Appendixes

A. References, *page 40*

B. Preparation Guidance for a System Safety Working Group Charter, *page 43*

C. System Safety Management Plan, *page 45*

D. Preliminary Hazard List/Analysis, *page 48*

E. System Safety Risk Assessment Preparation Guidance, *page 50*

F. Safety Release Preparation Guidance, *page 50*

G. MANPRINT Joint Work Group System Safety Checklist, *page 51*

H. Non-developmental Item System Safety Market Investigation/Survey Questions, *page 51*

I. Independent Safety Assessment, *page 52*

Table List

Table 2–1: Hazard probability definitions, *page 7*

Table 2–2: Hazard severity definitions, *page 7*

Table 2–3: Hazard Tracking System – sample format for a hazard tracking record, *page 13*

Table D–1: Format of preliminary hazard analysis (typical), *page 49*

Contents—Continued

Figure List

Figure 2-1: The CRM Process, *page 5*

Figure 2-2: Hazard Identification Process, *page 6*

Figure 2-3: Process for developing alternatives, *page 10*

Figure 2-4: System safety risk decision authority matrix, *page 12*

Figure 2-5: Fielded systems/concept refinement phase of system safety activities during life cycle of a program, *page 16*

Figure 2-6: Technology development phase/system development demonstration phase of system safety activities during the life cycle of a program, *page 17*

Figure 2-7: Production deployment phase of system safety activities during the life cycle of a program, *page 18*

Figure 2-8: Operation support phase of system safety activities during the life cycle of a program, *page 19*

Figure C-1: Milestones, *page 47*

Glossary

Part One

System Safety Management

Chapter 1

System Safety Management

1-1. Purpose

This pamphlet identifies the procedures in accordance with Army Regulation (AR) 385-10 for program executive officers (PEO), program/project/product managers (PM), combat developers (CBTDEV), materiel developers (MATDEV), testers, independent evaluators, and system safety engineers to—

- a. Conduct system safety programs to minimize risks throughout the system life cycle.
- b. Conduct hazard identification, system safety composite risk management (CRM), and hazard closeout procedures during system development.
- c. Identify and manage significant hazards discovered during operation and use of fielded systems.

1-2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1-3. Explanation of abbreviations and terms

Abbreviations and special terms used in this pamphlet are explained in the glossary.

1-4. Participants/key players

The effectiveness of the system safety program can be directly related to the aggressive and cooperative spirit of the participants. No program can be effective without aggressive pursuit of safety as a program goal, nor can it be effective without the active support and cooperation of the following players:

a. *Combat developer.* The CBTDEV has a vital role in the success of any system safety effort in all stages of a System's life cycle. During concept development/refinement, the CBTDEV should ensure that system safety is considered an integral component. They will seek system safety expertise, as soon as it is determined a new system is the appropriate solution to correct deficiencies identified during the mission area analysis (MAA). If a modification (MOD) or a doctrine change is the solution for a fielded system, then the CBTDEV should also seek system safety expertise to determine the potential safety impact of the selected solution. Some CBTDEVs have system safety expertise within their organizations; however, for those who do not, the principal sources of help are at the installation/proponent safety office and the CBTDEV's Army Command (ACOM) safety office. The CBTDEV is the integrator of system safety until a PM is chartered, usually after Milestone B. The principal systems safety responsibility of the CBTDEV is to articulate the user's system safety requirements throughout the system life cycle. Users forced to make do with inadequate or poorly designed equipment have an increased safety risk and a higher potential for loss of combat resources. The CBTDEV must incorporate system safety performance objectives into the concept formulation package. Accident potential should be considered in concept studies and tradeoff analyses (TOAs). The CBTDEV—

- (1) Develops user safety test issues and criteria.
- (2) Monitors the development program to ensure that the system's operational capabilities match its mission requirements.

(3) Represents the user in recommending system safety CRM decisions throughout the life cycle.

b. *Research and Development Organization.* For a system in the technology base, the Research and Development (RD) Organization must charter and maintain a Technology Safety Working Group (TSWG). The TSWG is responsible for reviewing emerging technologies and assessing and recommending steps to be taken in developing a safety technology.

c. *Program executive officers/program managers/materiel development/Life Cycle Management Command or direct reporting program manager.*

(1) The PEO/PM/MATDEV/Life Cycle Management Command (LCMC) ensures that hazards associated with the design, operation, maintenance, servicing, support, and disposal of the system are identified and resolved early in the life cycle through the application of system safety management and engineering. To accomplish this objective, the PEO/PM/MATDEV sets goals and establishes mechanisms to attain these goals. A PEO can best fulfill system safety officer responsibilities by requiring—

- (a) Program managers to be personally involved in their system safety programs.
- (b) Program managers to fully integrate their system safety program into their development programs. To accomplish this, the PM must charter and fund a System Safety Working Group (SSWG) (see app B) to provide the technical expertise needed to manage the system safety effort. The PEO/PM/MATDEV ensures that a System Safety Management Plan (SSMP) (see app C) is prepared, to outline the system safety activities throughout the system life cycle.
- (c) Program managers to establish and maintain a Hazard Tracking System (HTS) throughout the systems life cycle.

(d) Program managers may obtain systems safety engineering management support through their MATDEV and CBTDEV.

(2) The PEO can monitor the safety programs by—

(a) Including high and serious safety hazards in program status reviews. This demonstrates the PEO's personal interest in safety and assures the PEO is kept current on all hazards he may be requested to accept for the Army or may have to elevate to the Army Acquisition Executive (AAE) for a decision. Depending on program thresholds, the U.S. Army Combat Readiness Center (CRC) or U.S. Army Materiel Command (AMC) program evaluation reports identify strengths and weaknesses within the various PMs' programs and provide valuable information for use by the PEO.

(b) Requesting the CRC to conduct Independent Safety Assessments (ISA) for Acquisition Category (ACAT) I and ACAT II and selected high visibility programs in support of milestone decision reviews or AMC conduct periodic technical reviews of the safety programs for ACAT III and below.

(c) Coordinating with the appropriate U.S. Army Training and Doctrine Command (TRADOC) or U.S. Army Medical Command (USAMEDCOM) school commandant/proponent for annual reviews of the accidents associated with their fielded systems.

(d) Reviewing the status of safety related MODs periodically.

(e) Conducting periodic equipment improvement reports (EIR), quality deficiency reports (QDR), and accident reviews get the PMs personally involved. This demonstrates a shared concern with the user for the safe performance of the system, provides a forum for discussing the appropriateness of material and procedural fixes, and provides an excellent opportunity to solicit support for safety related MODs. Periodic review of safety related MODs for fielded systems are an indicator of the success of the original safety program conducted during development. Large numbers of such changes may indicate a weak program or poor management participation and safety emphasis. Regardless, if safety problems are allowed to be created and remain undetected until late in development, the fixes can wreak havoc with budgets and schedules.

(f) Notifying AAE and Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA(ALT)) on acceptance of the risk associated with any hazard under their purview.

(3) Ultimately, a PEO's or PM's success must be measured in terms of the performance of the system. Safety is one key aspect of its performance. Unsafe systems never perform to their full potential because the confidence of the user is reduced, resulting in poor system employment/utilization and mission accomplishment. The LCMC will assist in the logistics support of assigned materiel, and the development, acquisition, and support of non-system and system training aids, devices, simulators, and simulations (TADSS). It will manage the assigned technology base and provides matrix safety support to the PEOs and PMs for all acquisition and fielded systems to include input for any system safety risk assessment (SSRA).

d. Integrator. Chapter 3 discusses the integration of other disciplines. These include the seven domains of Manpower and Personnel Integration (MANPRINT) and other disciplines such as the Integrated Logistic Support (ILS), reliability, availability, and maintainability (RAM), system engineering, and research, development, and engineering (RDE) components, (for example, propulsion, warheads, software, and so forth).

e. Tester. The tester supports the hazard identification and tracking process by structuring tests based upon the Test and Evaluation Master Plan (TEMP), System Evaluation Plan, and test design plan. Testing will provide data to assess the effectiveness of the "fixes" made to previously identified hazards and it may identify new hazards. Hazards identified by the tester will be provided to the PEO/PM/MATDEV for incorporation into the HTS. A Safety Confirmation is developed by Developmental Test Command (DTC) and provided to the PM and to the independent evaluator, the latter copy to be used to support development of the independent evaluation. The sources of data can be contractor testing, technical testing, or user testing. The safety confirmation is a standalone document required at each MS review and may identify unresolved hazards and risks.

f. Independent evaluator. The independent evaluator consolidates test data from all available sources to address the technical and user test issues and requirements developed for a system; from this process comes the safety confirmation, the technical/operational independent evaluator's final evaluation/assessment of the overall safety of the system at the end of a phase of development. This confirmation can be a letter to the MATDEV or part of the independent evaluation/assessment. The sources of data can be contractor testing, technical testing, or user testing. As a part of continuous evaluation, the evaluator should assess and report the cumulative impact of unresolved hazards on the system's effectiveness. In the design of the TEMP, emphasis should be placed on both evaluation of the "fixes" made to previously identified hazards and identification of new hazards.

g. User.

(1) Initial activity occurs during early concept exploration/development/refinement and user testing during System Development and Demonstration and Production and Deployment (includes low-rate initial production (LRIP)) phases and after the system is fielded (Operations and Support Phase). Two major roles are—

(a) Identification of hazards in order to improve the safety of existing systems (for example, by submitting an EIR, QDR, SF 368 (Product Quality Deficiency Report) and by participation in the conduct of Post-Fielding Training Effectiveness Analysis (PFTEA).

(b) Development of historical data that can be used by the CBTDEV and PEO/PM/MATDEV to produce safer systems through hazard identification in the future.

(2) Primary activity should be tactical employment feedback to the CBTDEV and MATDEV during deployment and after fielding. The user should also communicate to the CBTDEV and MATDEV the following:

(a) Changes to mission requirements, operating spectrum, and tactical and doctrinal revisions.

(b) Early identification of new mission requirements.

(3) Development activity, sometimes with the cooperation through AMC FAST (Field Assistance in Science and Technology) Program, identifies new operational requirements. AMC FAST or REF (Rapid Equipping Force) community is responsible for reviewing and identifying safe systems, to identify any residual risks to users, and obtaining risk acceptance in accordance with this pamphlet. If the program does not go into a full developmental project, the user must perform the role of the CBTDEV, MATDEV, and tester/independent evaluator. The user will use this pamphlet for identifying operational and material risks involved with the equipments configuration and operation. Consideration must be given that equipment often classified as "prototype" may be used for many years.

(4) The user is represented by the TRADOC System Manager (TSM) and will coordinate with the end users especially the first unit equipped.

1-5. Army Safety Action Team

a. Objectives. The objectives of Army Safety Action Team (ASAT) are the following:

(1) Provide the Office of the Chief of Staff, Army (OCSA) with recommendations and information involving air and ground equipment safety issues.

(2) Coordinate, expedite, advise, and provide recommended direction to ensure safety correction measures maximize Army readiness, safety, and training.

b. Participants. Meetings of principal members and advisory members, as needed, will receive hazard executive summaries (EXSUMs) upon notification of a meeting without delay. Principle and advisory members include the following:

(1) Principal members are as follows:

(a) Office of the Assistant Secretary of Army for Acquisition, Logistics and Technology (OASA(ALT)).

(b) Office of the Deputy Chief of Staff, G-3/5/7 (DCS, G-3/5/7).

(c) Office of the Deputy Chief of Staff, G-4 (DCS, G-4) (Chairman).

(d) Office of the Deputy Chief of Staff, G-8 (DCS, G-8).

(e) Director of Army Safety (DASAF).

(f) Army Materiel Command.

(g) Appropriate PEO.

(h) Applicable proponent branch chief.

(i) Applicable MATDEV.

(2) Advisory members are as follows:

(a) Office of the Deputy of Chief of Staff, G-1 (ODCS, G-1).

(b) Office of the Chief Public Affairs (OCPA).

(c) Office of the Chief, Legislative Liaison (OCLL).

(d) Office of the Chief, Army National Guard (ARNG).

(e) Office of the Chief, Army Reserve (OCAR).

(f) Office of the Assistant Secretary of the Army (Installations and Environment) (OASA (I&E)/Environment, Safety and Occupational Health (ESOH).

(3) Other agencies and subject matter experts, for example, FORSCOM, USASOC, may be included as directed by the Director of Army Staff or the chairperson.

c. Army Safety Action Team reporting requirements. The chairperson will maintain and distribute a list, by name, of principal ASAT members and action officers, for use in coordination of safety-of-flight (SOF)/Army Equipment Safety and Maintenance Notification System (AESMNS).

d. Reporting functions. The PM will provide hazard alert information to the MATDEV and CBTDEV commands and the appropriate staffs within HQDA, to provide for the timely management of the associated risks. Information updates will be provided in accordance with the overall procedures outlined below, as supplemented by the materiel development command to address commodity-specific requirements. (Ammunition and explosives malfunctions covered by established surveillance procedures are covered by AR 75-1 and are excluded from these procedures and the AESMNS process outlined in AR 750-6. Medical supplies, equipment, drugs, and biological concerns are covered by AR 40-61 and are also excluded from the AESMNS process.)

(1) When a hazard is identified that has a potentially significant impact upon Army training or operations, the PM, in conjunction with the cognizant MATDEV agency, will immediately alert the ASAT Chairman. This notification will be in the form of a Hazard EXSUM. This Hazard EXSUM will normally include a description of the problem, a preliminary determination of risk, the potential operational impact, the current logistical status and the get-well concept.

However it should not be delayed if this data is not yet available. It is understood that the accuracy and completeness of this initial assessment will be dependent upon the technical and operational data available at that point; the intent is to provide an early hazard alert to provide the basis for a timely and collective assessment of the risks and potential controls as more information is gained on the nature and extent of the problem. The Hazard EXSUM will be updated as additional technical and operational knowledge become available.

(2) Significant hazards will normally be eliminated or minimized by immediate materiel modifications or changes to operational or maintenance procedures. If it is not feasible to eliminate the hazard, the PM will initiate a SSRA to coordinate the decision on the controls to be implemented and the acceptance of any residual risk. The PM will recommend options that mitigate the hazard and/or recommend acceptance of the residual risk. The SSRA will evolve from the Hazard EXSUM above. SSRAs on fielded systems will be processed as follows:

(a) *High level risks.* If a hazard has been validated (that is, the analysis for Part I of the SSRA has been completed by the program office or equivalent managing activity) and there are no resources available to reduce the risk to a lower level, the high risk SSRA will be brought before the ASAT for coordination. The ASAT will meet without delay. Telephonic or electronic notification of a proposal to accept a high level risk should precede written notification of the ASAT members.

(b) *Serious level risks.* If a hazard has been validated as a Serious-level risk and available controls cannot reduce the risk to a lower level, an SSRA will be staffed within 21 calendar days from initiation (Part I) to completion (Part V). Concurrent processing by multiple agencies is encouraged when one organizations evaluation is not dependent on someone's input.

(c) *Medium level and low level risks.* Medium and low level risk hazards are managed by the responsible PM or other managing activity (MA) and will be documented and tracked. Implementation of controls and decisions to accept residual risk will be made as quickly as possible, consistent with accurate assessment of the hazard and potential options.

e. *Fielded System/Materiel Army Safety Action Team.* For fielded systems or materiel, establish procedures for alerting the ASAT Chairman of impending safety issues with significant risk or that have the potential for significant impact upon operations and training. If such changes require transmission of safety information to the field, the MATDEV agency will develop and coordinate a SOF/Aviation Safety Action Message (ASAM), or a AESMNS. Specific procedures for developing and coordinating these messages are contained in AR 750-6 for aviation and ground systems. The MATDEV command will publish a supplement to this regulation to tailor those requirements and establish criteria as follows:

- (1) The specific levels of risk requiring a Hazard EXSUM.
- (2) Procedures for validation of the level of risk associated with the hazard.
- (3) Specific procedures, formats, and timelines for distribution of the Hazard EXSUM.
- (4) The content and organization of technical supporting information to be provided during coordination external to the PM organization.

Chapter 2 Risk and Hazard Management

Section I Risk Management

Composite risk management, along with its component Mishap risk management, joins to minimize Army safety system hazards.

2-1. Composite risk management

The CRM is the umbrella five (5) step process that the Army uses to minimize system hazards while managing affordability and system effectiveness. The CRM process is shown in figure 2-1.

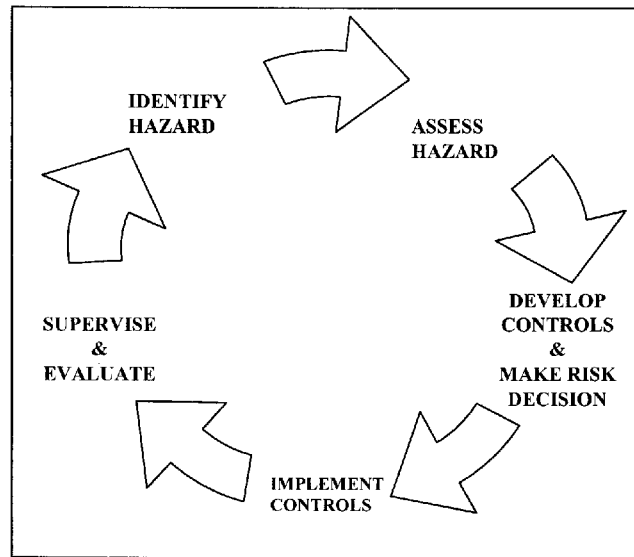


Figure 2-1. The CRM Process

2-2. Mishap risk management

Mishap risk management provides an environment in which CRM can be effectively performed. It supports CRM by capturing hazards and providing a communication forum, the HTS. Additionally, it provides hazard close-out methods and criteria within the functional steps of the CRM process by which hazards can be officially closed. Development of the mechanics and criteria to capitalize on this concept for the overall benefit to the Army is a dynamic process and requires “real time” communication among all concerned to ensure its application.

2-3. Identify hazard

a. The standard for hazard identification is a concise statement containing a source, mechanism, and outcome capturing relevant man, machine, and environment conditions that can lead to a mishap. By definition, a hazard is an actual or potential condition that can cause injury, illness, or death of personnel, damage to the environment, damage to or loss of equipment, property or mission degradation. In order to effectively describe a hazard, the hazard statement must consist of three basic components:

- (1) Source (an activity, condition, or environment where harm can occur).
- (2) Mechanism (means by which a trigger or initiator event can cause the source to bring about harm).
- (3) Outcome (the harm itself that might be suffered expressed as a severity).

b. The hazard will be expressed at the system level. It begins with the gathering of information and produces viable hazards for which follow-on actions may influence the design, modification, or use of the system.

c. Information collection is inclusive of all sources and not limited to the receipt of accident reports. The effort should extend outside the Army to include other services, federal agencies, and private industry. Aggressive information collection looks for sources of potential hazardous conditions. Figure 2-2 shows the hazard identification process.

d. The sources of these potential or real hazards might be lessons learned hazards analyses, accident experience, technology base development data, operational experience, testing, government studies, or information from non-military usage of similar technology. These hazards include any issues which have the potential to result in materiel losses or injury (accidental and/or health related) to any personnel. Potential causes of losses must be translated (if possible) into a potential system hazard. For example, a “human error” cause of an accident may have been induced by a system design hazard. All potential system hazards are then added to the hazard tracking list (HTL). Once a real or potential hazard is identified, it is handled and treated as a real hazard. It will be formally considered, tracked in the HTL, and reviewed. Several types of analyses usually performed by the contractor can contribute to the HTL. Other related disciplines, such as those listed in chapter 3, will identify hazards or other information that must be evaluated to identify hazards.

e. Once a PM receives notification of a potential safety issue, the PM will validate the issue to identify the hazard.

When conditions are identified that have potentially significant impact on Army training or operations, the conditions must be documented and translated into a hazard. This requires a narrative description of the human, machine, and environmental conditions leading to a mishap. These conditions are parlayed into three elements to express the hazard (source, mechanism and outcome). The outcome is the potential consequence of the hazard (such as damage to equipment, injury, death). Outcomes will be considered at the system level. Hazard statements containing multiple sources, mechanisms, or outcomes represent a family containing multiple hazards. Each hazard within the family will have its own hazard statement containing a single source, mechanism, and outcome. Once a real or potential hazard is identified, it is handled and treated as a real hazard. It will be formally considered, tracked in the HTL, and reviewed. The PM will ensure that the hazard is completely identified.

HAZARD IDENTIFICATION PROCESS

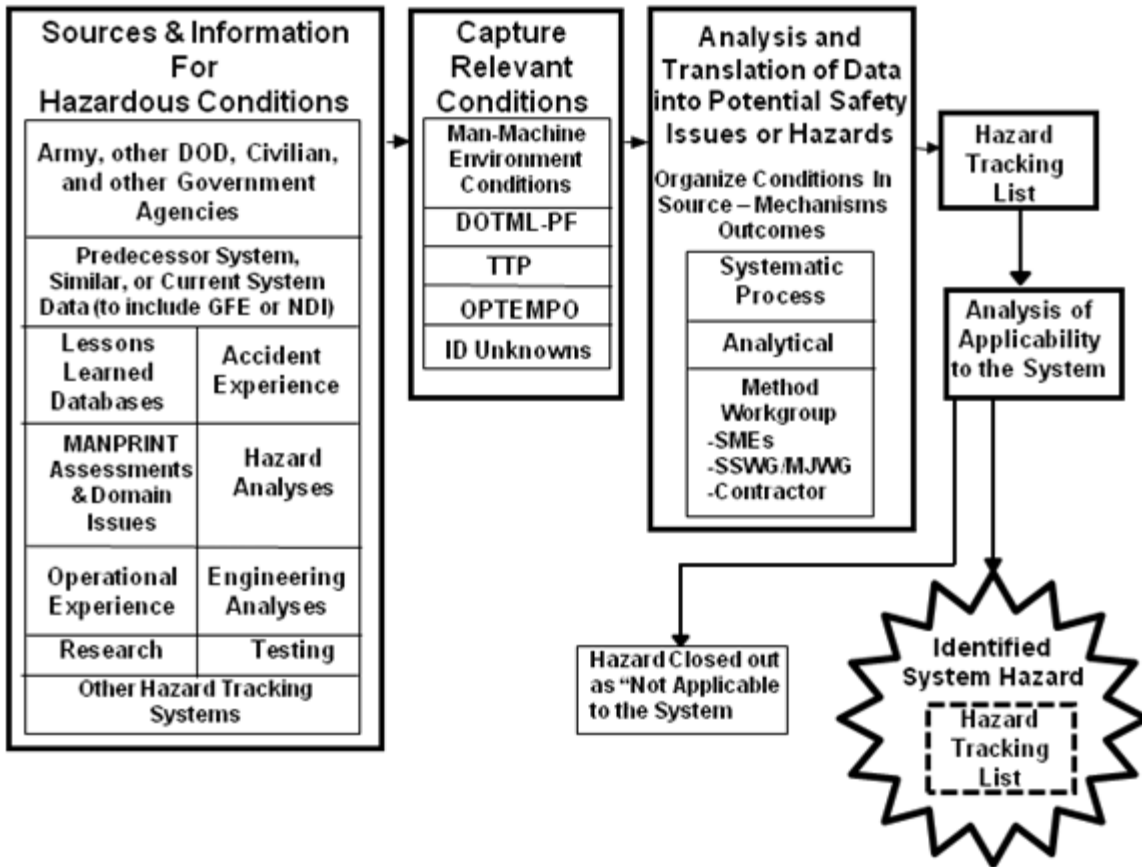


Figure 2-2. Hazard Identification Process

f. Although hazard identification goes on continuously throughout the life cycle of a system, it is of paramount importance when considering an acquisition strategy. The presence of system hazards should be one of the determining factors when considering accelerated acquisition, Non-developmental item (NDI), or use of government furnished equipment (GFE) subsystems.

(1) Early hazard identification can influence MA decisions on source selection for NDI or types of GFE to utilize. Also, this hazard identification can drive effective TOAs as well as identify other required testing to assure materiel in these types of acquisitions deliver the maximum operational effectiveness to the Army.

(2) Certain accelerated acquisition programs may not allow a period to discover hazards in time to initiate an alternate acquisition program. This reinforces the importance of identifying hazards early on.

(3) Materiel developers may choose or be required to use GFE hazard considerations in the development of their systems. Regardless, proponent MATDEVs are required to consider hazards associated with GFE to include the interfaces of the GFE with other components. All identified hazards associated with the GFE will be documented in some form, such as permanently retained hazard analyses or entry into a permanent HTL.

g. Close out criteria during hazard identification.

(1) During this step of CRM, a hazard can only be closed out as being “Not Applicable to the System.” This approach identifies those potential hazards which are not applicable to the system in the acquisition process. Closeout by this method requires a thorough evaluation of the hazard relative to the system design and the planned or potential usage in the operation, training, maintenance, storage, and transportation to disposal environment.

(2) However, if the exact system configuration and operational factors are not sufficiently known to identify the hazard’s applicability to the system, the hazard remains open to continue in the CRM process.

(3) The inherent safety characteristics of major pieces of GFE selections will be considered early in the design process during TOAs to ensure the safest possible GFE is selected, consistent with mission accomplishment. This is the proactive method whose ends would apply the “not applicable to the system” approach to hazard closeout.

2-4. Assess hazard

This step of the CRM process begins with a viable system hazard and assesses the risk of the hazard. The output of the hazard assessment step is a risk assessment of the viable system hazard. The following guidance for hazard assessment is provided:

a. *Hazard assessment.* In establishing priorities for correcting a system’s hazards, hazards must be evaluated to determine their probability levels and severity categories. Hazard probability can be categorized as shown in table 2-1 (taken from military standard (MIL-STD)-882). To aid in classification, these probability definitions can be supplemented in terms of exposure (that is, passenger miles or number of flight hours) at the discretion of the SSWG. Hazard severity can also be categorized quantitatively. The severity categories defined in MIL-STD-882 are shown in table 2-2.

**Table 2-1
Hazard probability definitions**

Description	Level	Individual item	Fleet or inventory
Frequent	A	Likely to occur frequently	Continuously experienced
Probable	B	Will occur several times in life of item	Will occur frequently
Occasional	C	Likely to occur sometime in life of item	Will occur several times
Remote	D	Unlikely, but possible to occur in life of item	Unlikely but possible reasonably be expected to occur
Improbable	E	So unlikely it can be assumed occurrence may not be experienced	Unlikely to occur but possible

**Table 2-2
Hazard severity definitions**

Description	Category	Accident definition
Catastrophic	I	Death, system loss, or severe environmental damage
Critical	II	Severe injury, severe occupational illness, major system damage, or environmental damage
Marginal	III	Minor injury, minor occupational illness, minor system damage, or environmental damage
Negligible	IV	Less than minor injury, occupational illness, system damage, or environmental damage

(1) Care should be taken to ensure the system is adequately defined. For example, if a tank engine is defined as the system, a hazard that causes it to stop could be catastrophic since there was a total system loss. Now if the system were the tank and the engine stopped, then the hazard may not be catastrophic. Care also must be taken to look at associated hazards. For example, if the tank engine also powered the brakes, then the hazard of an engine stoppage might be higher.

(2) The risk associated with a hazard is a function of its probability and severity. Tables 2-1 and 2-2 combined provide a matrix for assigning a code to the risk associated with a hazard. These codes are known as risk assessment codes (RACs). Single-digit RACs could be created by using numerical rather than alphabetical rankings of probability, then multiplying probability by severity. This method should be avoided because the use of single-digit codes presumes that the lower the product, the higher the risk associated with the hazard. This presumption is not always true, and common products (such as 1x4 and 2x2) mask prioritization.

b. Government furnished equipment risk assessment. Previously identified and documented hazards associated with previously fielded GFE will normally continue to be considered acceptable provided no unique hazard is created because of the interfaces with the new system. A hazard caused by GFE is considered unique to the new system interface if—

(1) Verification indicates the environment of the proposed GFE use exceeds the environment for which the GFE is designed.

(2) The severity of a potential accident that could result from the identified GFE hazard when used with the new system is materially greater than when used as originally designed.

(3) The probability of a potential accident that could result from the identified GFE hazard when used with the new system is materially greater than when used as originally designed.

c. Close out criteria during risk assessment. During this step of the CRM process, the only way a hazard can be closed out is by “meeting or exceeding acceptable standards.” Unfortunately, this method requires careful consideration by system safety practitioners and program managers as abuses of the process may occur. Use of this method should not be the first line of defense, but the last. MAs are encouraged to consider all hazard fixes that derive a level of safety that is in concert with program cost and schedule as well as maximize warfighting capability. System safety programs that consider all programmatic assets can provide the leading edge for quality.

(1) *Design meets or exceeds applicable standards.* The goal of this approach is to ensure that personnel and systems are not exposed to hazards in excess of equipment designed to specifically applied standards. For example, any pressure vessel presents a hazard; however, if it has been designed to meet or exceed American Society of Mechanical Engineers (ASME), American National Standards Institute (ANSI), and MIL-STD-1522, and it is used in an environment appropriate to these standards, then it will not be considered a residual hazard.

(a) Identification/definition of the root cause of the hazard.

(b) Determine/review the standard for applicability and sufficiency for the equipment design.

1. Is the standard applicable and sufficient as applied to the system design?

2. Is the standard current and state of the art?

(c) Analyze the operational environment of the system to ensure that the standard is applicable to the envisioned environment.

(2) *Government furnished equipment hazard closeout.* The assessment of GFE hazards as outlined above, mirrors the “design meets or exceeds applicable standards” approach. To closeout GFE hazards, previous type classification of GFE will be considered to have constituted acceptance by the Army of risks inherent in the GFE in its previous application. For applicable hazards, the hazards analysis or HTL needs to annotate “type classification” as the rationale for closing the hazard.

2-5. Develop controls and make risk decisions

During the first two steps in the Mishap Risk Management Process of CRM process, the MA could agree the design meets or exceeds all applicable consensus and/or military design standards (or is verified through testing, where standards do not exist) and that the environment in which it will operate is consistent with that envisioned by the design. Hazards which cannot be eliminated by design during hazard identification or the hazard assessment processes will be considered residual hazards. The goal of this step is to develop risk reduction alternatives and obtain a decision by the appropriate decision authority.

a. With the risk of the hazard assessed, the next task is to develop alternatives. Here alternatives should be generated using the system safety design order of precedence, determining which alternative or method will be applied given the program’s resource constraints. Therefore, cost and other programmatic impacts must be identified with each alternative. While effectiveness of specific countermeasures may vary, the system safety order of precedence for mitigating identified hazards generally is—

(1) *Eliminate hazards or reduce hazard risk through design selection.* If unable to eliminate an identified hazard, reduce the associated mishap risk to an acceptable level through design selection or alteration.

(2) *Incorporate engineered safety features.* If unable to eliminate the hazard through a design change, reduce the risk through engineered safety features that actively interrupt the mishap sequence (examples: emergency core cooling

system of a nuclear reactor and loss-of-tension braking for elevators full-time, on-line redundant path(s); interlocks; ground-fault circuit interrupters, uninterruptible power supplies).

(3) *Incorporate safety devices.* If unable to eliminate the hazard through design or engineered safety features, reduce the mishap risk to an acceptable level using protective safety features or devices. These protective safety features or devices could be implemented using hardware, software, or a combination of both.

(4) *Provide warning devices.* If safety devices do not adequately lower the mishap risk of the hazard, include a detection and warning system to alert personnel to the particular hazard.

(5) *Develop procedures and training.* Where it is impractical to eliminate hazards through design selection or to reduce the associated risk to an acceptable level with safety and warning devices, incorporate special procedures and training. Procedures may include the use of personal protective equipment. For hazards assigned Catastrophic or Critical mishap severity categories, avoid using warning, caution, or other written advisory as the only risk reduction method.

b. The decisionmaking task involves selecting the alternatives identified in the develop controls portion of this step, as shown in figure 2–3. Formal acceptance of any residual hazard, which exists from the alternatives selected, must be documented in SSRA.

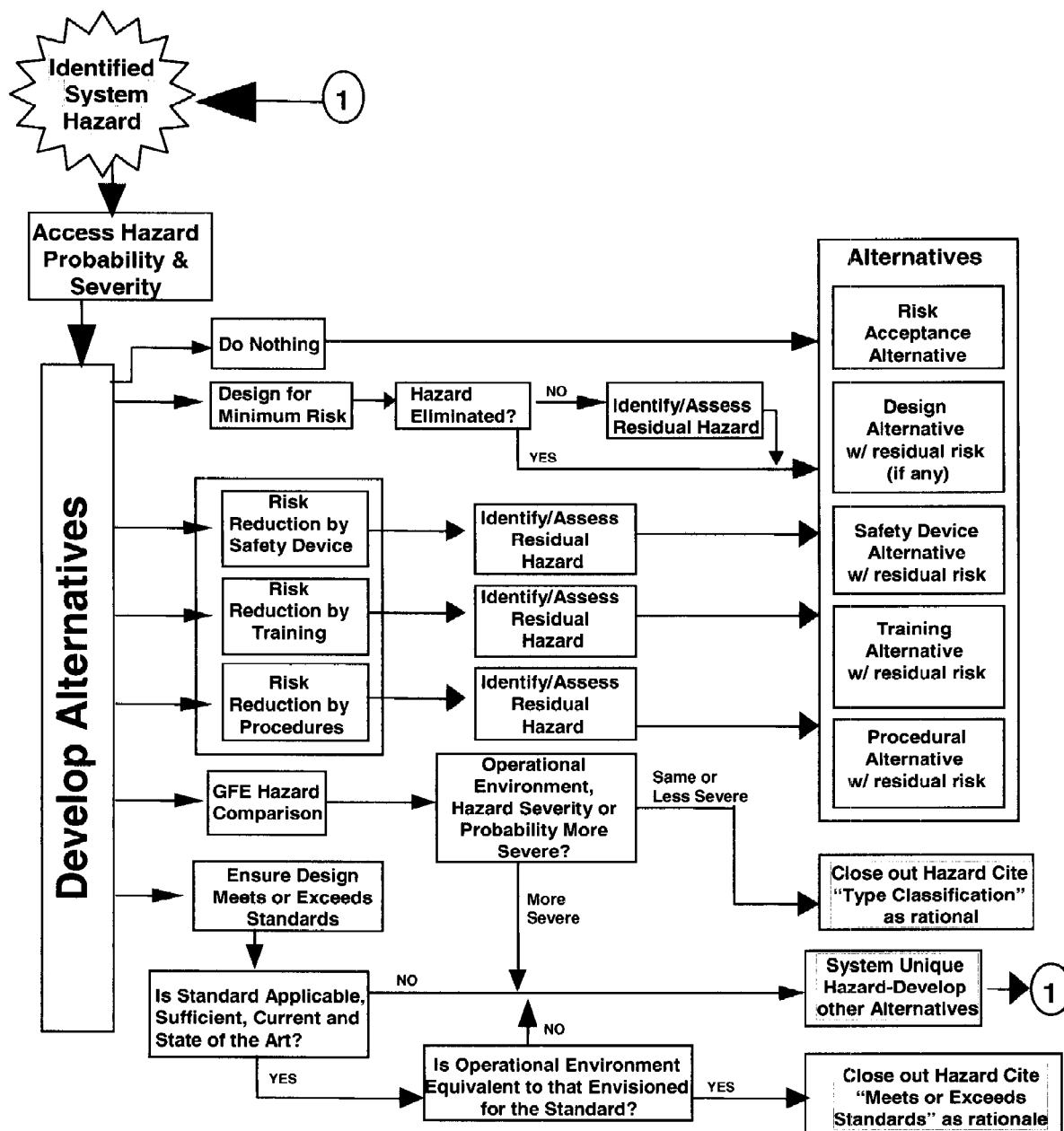


Figure 2-3. Process for developing alternatives

c. The residual hazard RACs in figure 2-3 refer to the risk remaining after corrective action(s) have been applied. For example, a hazard is identified and assigned a RAC of IA. The PM allocates additional funds for the contractor to apply an engineering "fix" to the system, which would reduce the RAC to 2D. The cost to further reduce the risk is prohibitive in the judgment of the PM; however, given the matrix in figure 2-4, the PM must decide whether or not to accept the risk for this residual hazard. If the decision authority decides that the risk is acceptable, then the engineering "fix" should be applied and tested. In another example, a IIA hazard is identified, but the PM's recommended engineering "fix" will only reduce the RAC to IIIA. The PM cannot accept that level of risk; therefore, the PEO must decide on risk acceptability. If the decision authority decides that IIIA is an unacceptable level, then the PM will have to take necessary action(s) to reduce the risk.

d. Determining which alternative or method to be applied is important. The decision to accept the risk of a residual hazard must be at a level appropriate to the priority of the residual hazard. From a safety standpoint, the goal should be

to achieve the lowest level of risk in concert with mission effectiveness. The residual hazard control alternatives in paragraph 2–5a, above, are listed in their order of effectiveness to reduce risk. Designing for minimum risk, incorporating safety devices, and providing warning devices usually require engineering design changes. Because such changes become increasingly more expensive later in the life cycle, early hazard identification is essential. Caution should be taken when relying on procedures or training as corrective measures.

e. The residual hazard close-out procedures during the “develop controls and make risk decision” step of the CRM process are:

(1) *Design approach.* The goal of this approach is to implement design changes that would result in the elimination of the hazard or minimization and control of any residual hazards.

(a) Identify/define the source, mechanism and outcome of the hazard.

(b) Develop a design eliminating or controlling that root cause.

(c) Complete an adequate test program to verify fix (with favorable results).

(2) *Devices/training/procedures approach.* The goal of this approach is the identification and implementation of procedures that reduce the probability of the hazard and subsequent acceptance of any residual risk.

(a) Identify/define the source, mechanism and outcome of the hazard.

(b) Develop devices, training, or procedures that reduce the probability of the hazard.

(c) Complete an adequate test program to verify the procedures.

(d) Identify the residual risk associated with the device, training, or procedural fix. (These fixes generally reduce the probability but do not eliminate the hazard entirely and do not affect the hazard severity.)

(e) Develop and coordinate a SSRA for the residual risk.

(3) *Risk acceptance.* The final step is the risk acceptance approach and the goal of this approach is associated with a residual hazard that has not been controlled by one of the preceding alternatives. During this step, residual hazards are closed out by—

(a) Identify/define the source, mechanism and outcome of the hazard.

(b) Conduct studies to identify potential design options, if available, to eliminate the hazard and the associated program cost.

(c) Anticipate rationale for not eliminating the hazard.

(d) Identify the residual risk associated with the hazard.

(e) Develop and coordinate an SSRA for the hazard. (See app E.)

(f) Obtain a decision by the appropriate decision authority to accept the residual risk associated with the hazard.

f. Program requirements—

(1) The PEOs will develop a risk-acceptance matrix in accordance with MIL–STD–882. When necessity requires an alternate risk matrix due to the type of the materiel acquisition, the PEO will submit risk-acceptance matrix to the AAE for approval. The PM will include the matrix in the SSMP. (See app C.)

(2) Residual risk will be accepted in accordance with the SSMP or in absence of a SSMP, MIL–STD–882. Each potential corrective measure should be identified, and the risk, if it is applied, should be projected. The consequences of risk acceptance and of each alternative corrective measure should be expressed using projected costs in terms of deaths, injuries, system damage, and program delay.

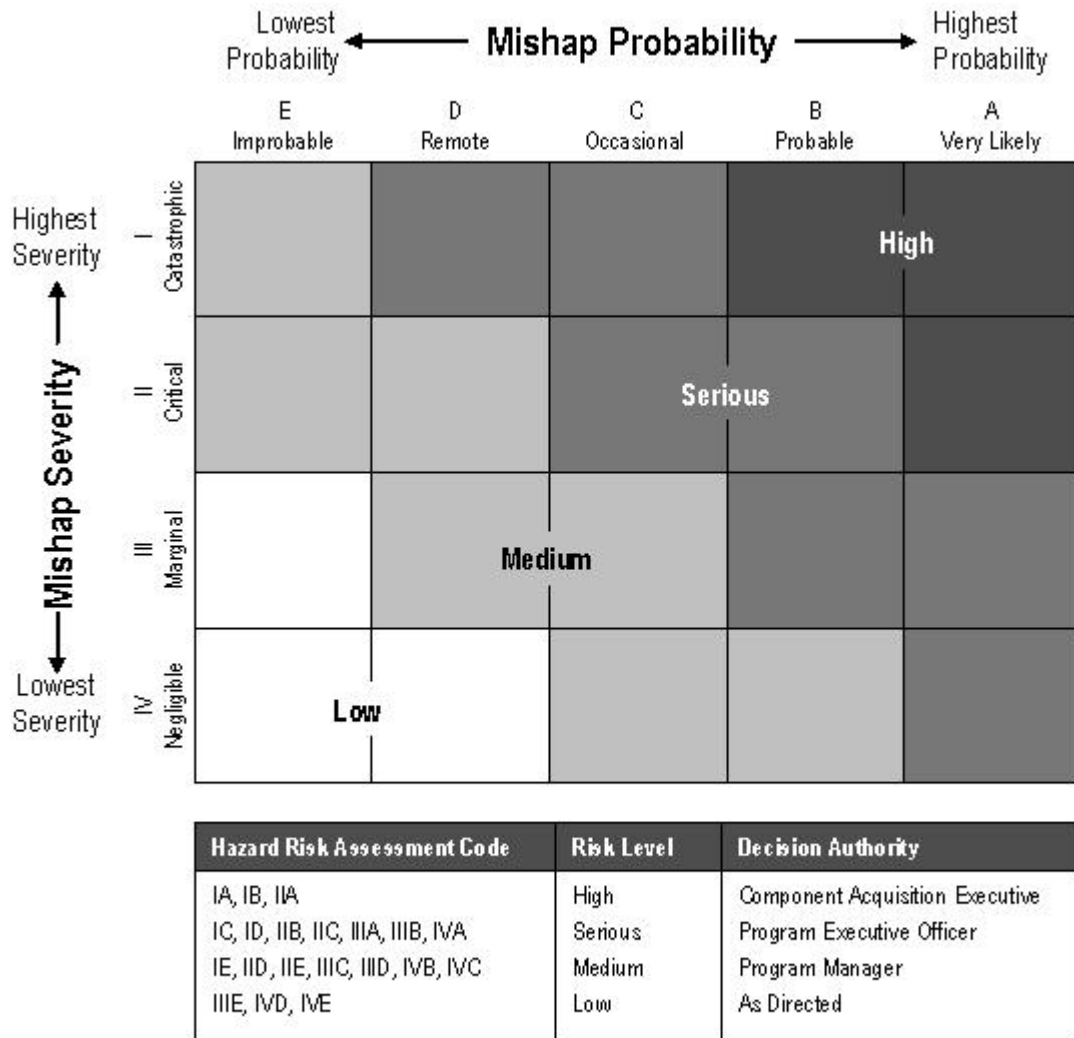


Figure 2-4. System safety risk decision authority matrix

2-6. Implement controls

Step four of the MISHAP RISK MANAGEMENT process is actual implementation of the risk decision made on the residual hazards in step three, “develop controls and make risk decision.” During this step, the following actions are accomplished:

- a. Designate or obtain funding for the fix.
- b. Develop and implement an action plan for implementation of the risk decision.
 - (1) Production and retrofit.
 - (2) Follow-up plan for monitoring corrective action and implementation status.
 - (3) Implement devices, training, or procedures.
 - (4) Publish the procedures in the appropriate manuals.
- c. Develop and execute a follow-up plan to verify anticipated/assigned hazard severity/probability and adequacy of the fix in the operational environment.

d. Testing is the primary method of verifying the effectiveness of the hazard controls implemented as described in chapters 2 and 4.

2-7. Supervise and evaluate

a. Step five of the mishap risk management process is supervising and evaluating the implementation of the risk decision made on the residual hazards in step three, “develop controls and make risk decisions.” It is during this process that the effectiveness of the risk decision is ensured and that standards are being maintained at the highest level possible. Also during this step, the evaluation of the system safety program efforts are reviewed and the mishap risk management process reentered at the step that is required to maintain the high safety standard of the system.

b. Only when the above criteria have been met, including the addressing of the residual risk and the effectiveness of the system safety effort has been determined or evaluated during this step, can a hazard be officially closed out on the HTL. The closure of a hazard does not eliminate the requirement to retain the hazard in the HTL. The hazard and its disposition should always be retained to provide future program visibility and as an audit trail of the actions. Also, the closed out actions, including implementation status and accident data, are necessary to determine if further action is required.

2-8. Hazard tracking

a. The HTS tracks the status of all identified hazards throughout the life cycle of the system. A preliminary hazard list (PHL) and Analysis (PHA) (see app D) should be performed on each technology or conceptual system and then used as the basis for establishing the HTS if the technology matures into a concept. The data elements for an automated hazard tracking record format are shown in table 2-3. The status will reflect approval by the appropriate decision authority and whether the corrective measure has been applied. Once identified, the hazard should never be removed from the HTS during the life cycle of the hardware and successor systems.

b. The PM will prepare SSRAs (see app E), coordinate with the CBTDEV, and keep on file. Since thousands of hazards may be identified over the life of a major system, automation of the HTS is essential.

Table 2-3
Hazard Tracking System – sample format for a hazard tracking record

Item description	Definitions
HTS log number	An alphanumeric code identifying hazards.
Type, model, series	The model type and series of the equipment for which the hazard is affecting.
Subsystem	The subsystem name.
System description	The narrative for describing the system in which the hazard is located.
Date hazard identified	The date the hazard was identified.
Hazard tracking item revised date	The date which additional information has been added to the information on the hazard.
Status	The status of the hazard and its processing stage. The stages of the status could be proposed, open, monitor, recommended closed, mitigated (designed out or managed).
Hazard classification RAC	The (RAC) for the hazard during the life cycle. Maybe initial, current, or final.
Hazard classification RAC source	A single code describing the source of determination of the RAC, based upon the equipment damage, system damage, or personal injury.
Hazard classification severity	Projected/expected "worst creditable severity" information.
Hazard classification probability	The projected or expected probability of occurrence for the RAC.
Life cycle cost	The projected cost of the initial hazard if not corrected.
Life cycle deaths	The expected or projected deaths if the hazard is not corrected.
Hazard type	Field for organizing the hazards into groups.
Hazard description	The hazard described in full detail.
Life cycle occurrence	The expected mission, time or period where the hazard would exist.
Failure mode	How the hazard would manifest itself during the life cycle.
Engineering mitigation alternatives (EMA)	The various Engineering and design changes which if applied would reduce or eliminate the hazard. The solutions should be numbered and contain the resulting residual RAC. Cost of the engineering solutions should be projected.

**Table 2-3
Hazard Tracking System – sample format for a hazard tracking record—Continued**

Item description	Definitions
Procedural mitigation alternatives (PMA)	The procedural changes which if applied may reduce the probability of the occurrence. The solutions should be numbered and the solution would contain the resulting residual RAC. Cost of application should be projected.
Warnings, cautions, and notes mitigation alternatives (WCNMA)	The warnings, cautions, and notes in the technical manuals which could reduce the probability of occurrence. The solutions should be numbered and contain the resulting residual RAC. Cost of application should be projected.
Status of EMA	The status of all the engineering solutions.
Status of PMA	The status of all the Procedural changes.
Status of WCNMA	The status of all the warnings, cautions, and notes mitigation alternatives.
SSRA required (Y/N)	Indicates the need for an SSRA.
SSRA completed (Y/N)	Indicates whether or not the SSRA is complete.
SSRA signature date	Date the SSRA was finalized.
Signature fields	The necessary signature fields for the SSRA.

2-9. Hazard closeout

a. The SSWG plays a key role in making recommendations to the PM on specific hazard/risk issues and initiating the coordinating process for mishap risk management decisions. The SSWG also determines when it is appropriate to initiate a hazard closure recommendation and officially close a hazard on the HTL. Five methods or approaches exist for recommending hazard closeout—

- (1) Not applicable to the system.
- (2) Eliminated by design modification.
- (3) Design meets or exceeds applicable Federal, Department of Defense (DOD) or DA standards, regulations or guidance or by a recognized national authority on the subject for the operating environment.
- (4) Reviewed and certified by the appropriate authority, for example, AFSRB, IM Board, Ignition Safety Board, or DOD Explosives Safety Board (DDESB).
- (5) Risk acceptance.

b. The criteria for determining the appropriateness and timeliness for submitting a hazard closure recommendation, and subsequent closeout on the HTL, are highlighted in the description of each step of the mishap risk management process.

2-10. Objectives for the program executive officer/program manager/materiel developer/Life Cycle Management Command/combat developer during system safety mishap risk management

a. The PEO/PM/MATDEV/LCMC will—

(1) Establish procedures to ensure that hazards will be identified, tracked, eliminated, and managed as the risk associated with the hazard is accepted by the appropriate decision authority throughout the life cycle of the system to include Systems of Systems, NDI, and integration of GFE.

(2) Identify potential corrective actions for each hazard and project the total life cycle accident costs for each potential corrective measure.

(3) Document final resolution for each identified hazard. For each high and serious residual risk identified throughout the system's life cycle, the PM will ensure the preparation and staffing of a SSRA. The PM has the option to prepare a SSRA for medium and low risk hazards.

(4) Establish criteria to select the appropriate decision authority for each hazard as described in paragraph 2-5. From the HTS, the SSWG will provide the PM a list of hazards that meet the above criteria. The PM then selects a recommended corrective action(s) on the SSRA. Each SSRA must be coordinated with the Matrix Support Command and the CBTDEV, who represents the user. The appropriate decision authority will be presented with a completed SSRA for each hazard requiring a decision.

(5) Be responsible for a system safety presentation to the Army Systems Acquisition Review Council (ASARC). This presentation includes a brief description of each high and serious risk residual risk and a recommended corrective action based on the SSRA. Agendas for the ASARC are established by an ad hoc working group per AR 15-14. Additional safety issues deserving ASARC attention will be presented to this group with adequate agenda time.

(6) Provide matrix safety support to the PEOs and PMs for all acquisition and fielded systems to include input for any SSRAs.

b. The CBTDEV will—

- (1) *Measures.* Make recommendations as to the operational suitability of each corrective measure.
- (2) *Developmental systems.* As the user's representative, make a recommendation on acceptability of residual risk associated with proposed corrective alternatives to control a hazard. (See para 2–5.) This recommendation is part of the SSRA (see app E) for each hazard. It should be forwarded to the appropriate decision authority as defined by the SSMP decision authority matrix. If engineering change proposals (ECP) are submitted, the CBTDEV must assess their impact and develop the user position regarding acceptability.
- (3) *Fielded systems.* The CBTDEV's recommendation on the acceptability of residual risk will be incorporated into any MOD. The CBTDEV's recommendation must be provided to the materiel proponent, the CRC, and DCS, G–3/5/7.
 - c. *Integrator.* Chapter 3 discusses the integration of other disciplines. These include the seven domains of MANPRINT and other disciplines such as ILS and RAM.
 - d. *Testers.* Testers should validate the effectiveness of the correction imposed. The user collects accident and failure data to be used by the user's ACOM/Army Service Component Command (ASCCs)/Direct Reporting Units (DRUs) to verify the estimated severity and probability of occurrence and/or the merit of the hazard control or "acceptance" decision.
 - e. *Independent evaluators.* The independent evaluators will prepare reports for Materiel Acquisition Decision Process (MADP) reviews. The SSWG will verify that the independent evaluators have copies of the appropriate documents for evaluation prior to the MADP review date.

Section II

System Safety Program Management Activities within the Life Cycle

2–11. Program elements

a. Army leader involvement, creation of a SSMP, and the acquisition of dedicated system safety expertise are the key ingredients of a successful program. The major effort should be directed toward identifying, tracking, assessing, and resolving hazards. An effective system safety program established early in the system's life cycle will result in the identification and resolution of most hazards before the system's maturity makes production design or material changes extremely costly.

b. Figure 2–5 through 2–8 contain a list of activities that occur in a system safety program.

Note. All elements are not required for every program. Each system safety program should be tailored to fit the needs of the particular acquisition strategy (AS).

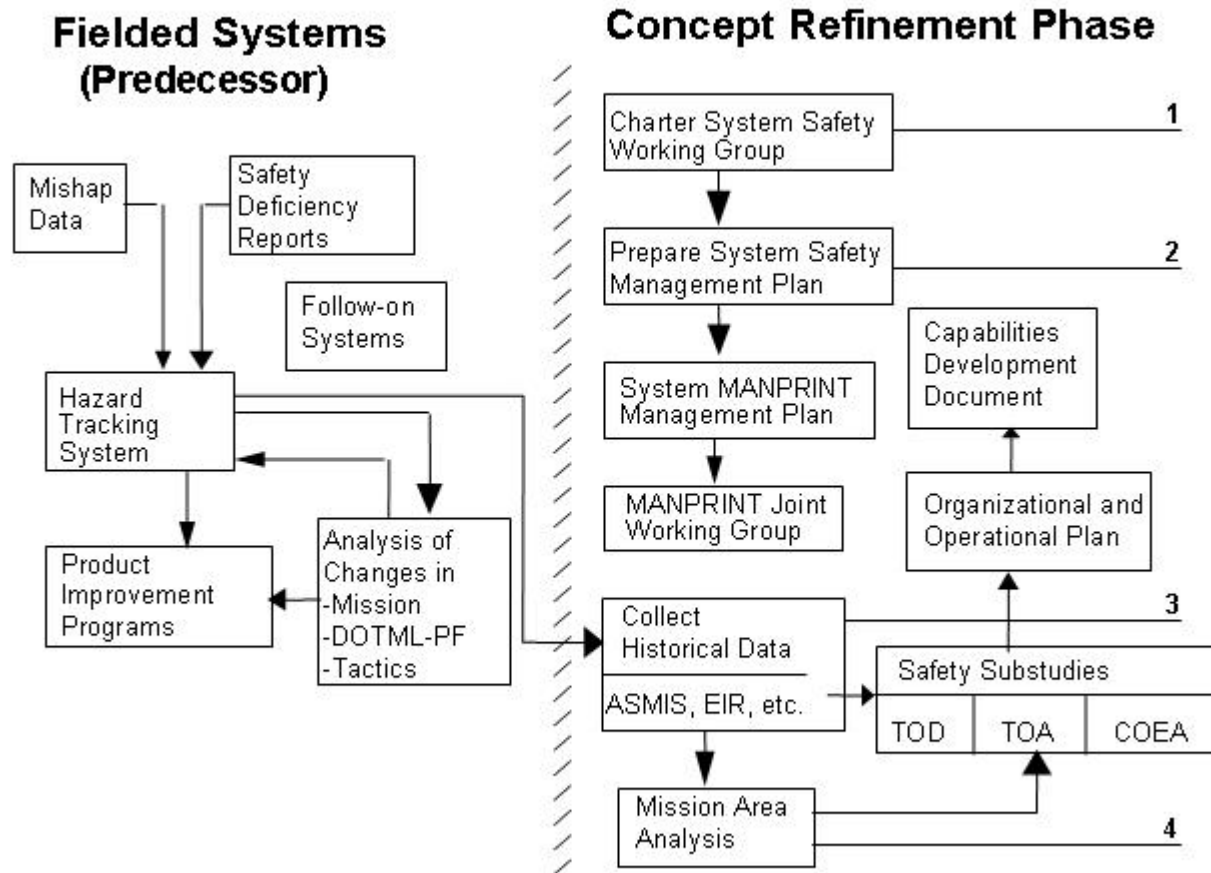


Figure 2-5. Fielded systems/concept refinement phase of system safety activities during life cycle of a program

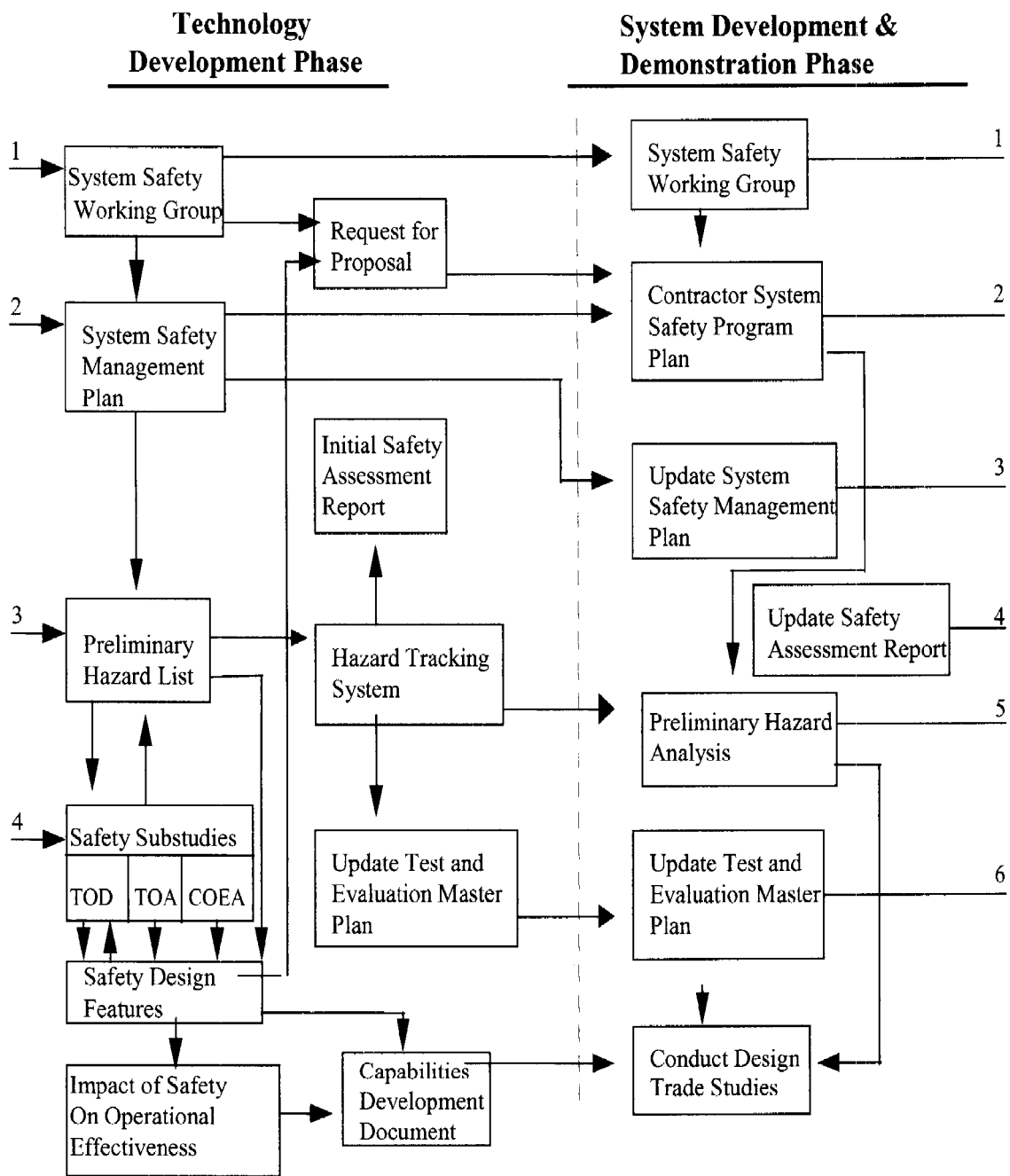


Figure 2-6. Technology development phase/system development demonstration phase of system safety activities during the life cycle of a program

Production & Deployment Phase

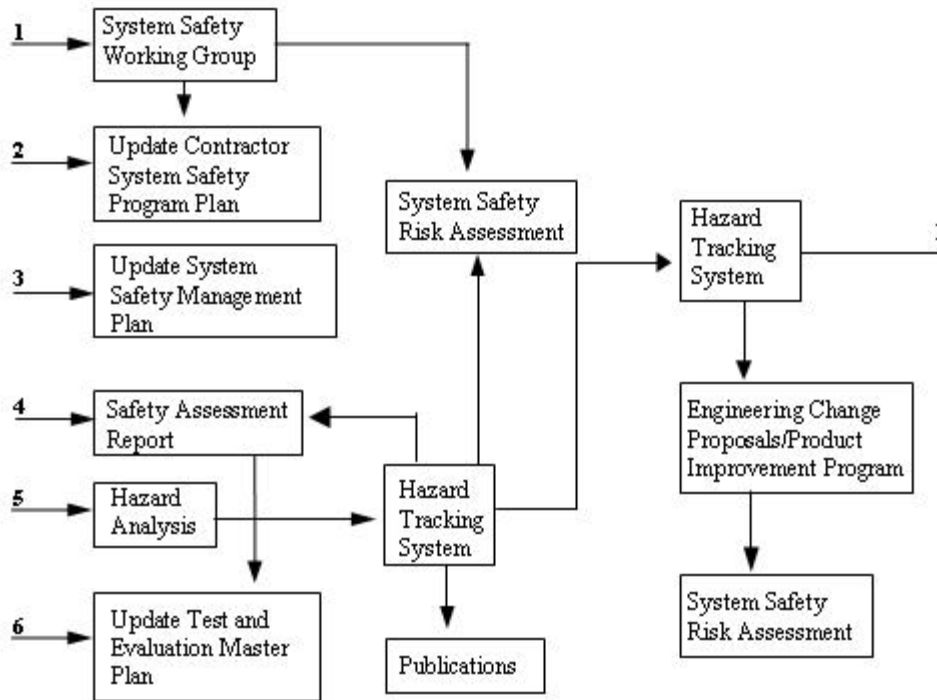


Figure 2-7. Production deployment phase of system safety activities during the life cycle of a program

Operation & Support Phase

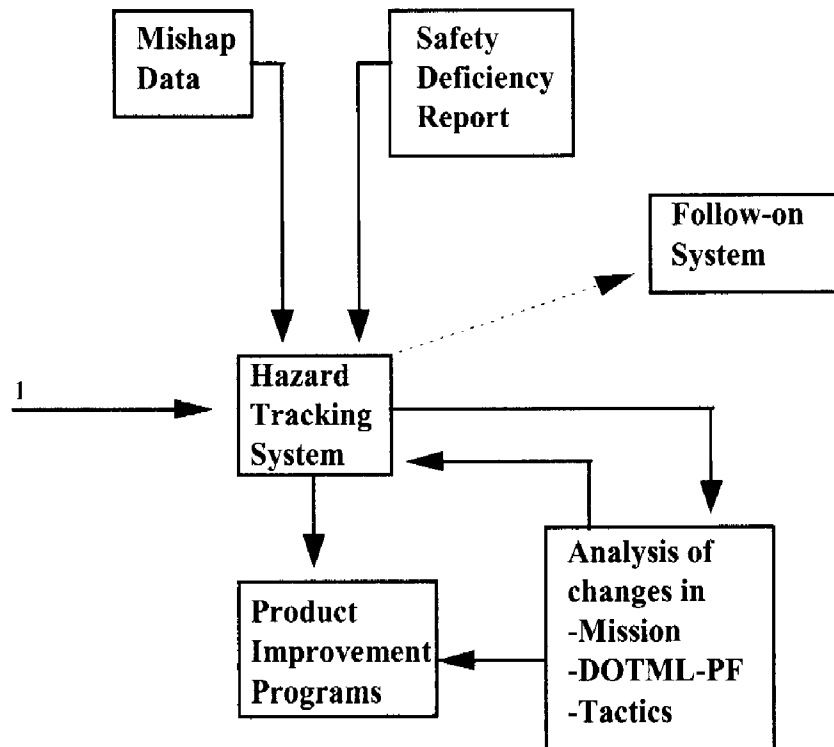


Figure 2–8. Operation support phase of system safety activities during the life cycle of a program

2–12. Adapting the system safety program

a. A major step in establishing an effective system safety program is to get the PEO/PM involved early in the system's life cycle. Early recognition of hazard identification is achieved by front-end loaded system safety efforts and documentation. The positive implications of this approach are numerous—

- (1) It requires an "early on" system safety program, which equates to a more effective program.
- (2) It eliminates redundancy in system safety documentation.
- (3) It provides a tailoring technique for the system safety documentation.
- (4) It provides for management input and review of system safety documentation and decision milestone reviews.

b. Evolutionary acquisition is DODs preferred strategy for rapid acquisition of mature technology for the user. An evolutionary approach delivers capability in increments, recognizing, up front, the need for future capability improvements. The success of the strategy depends on the consistent and continuous definition of requirements and the maturation of technologies that lead to disciplined development and production of systems that provide increasing capability towards a materiel concept.

c. The approaches to achieve evolutionary acquisition require collaboration between the user, tester, and developer. They include the following:

(1) *Spiral development.* In this process, a desired capability is identified, but the end-state requirements are not known at program initiation. Those requirements are refined through demonstration and mishap risk management; there is continuous user feedback; and each increment provides the user the best possible capability. The requirements for future increments depend on feedback from users and technology maturation.

(2) *Incremental development.* In this process, a desired capability is identified, an end-state requirement is known,

and that requirement is met over time by development of several increments, each dependent on available mature technology.

d. Representatives from the user, tester, and developer communities will assist in the formulation of broad, time-phased, operational goals, and describe requisite capabilities in the capabilities development document (CDD). They will examine multiple concepts and materiel approaches to optimize the way these capabilities are provided. The examination will include robust analyses that consider affordability, technology maturity, and responsiveness.

e. A successful system safety effort requires adaptation in order to fit the particular materiel acquisition program. This is particularly true for NDIs and other programs with accelerated acquisition cycles. This is also true when a “materiel system” interfaces with a “facility.” Special care must be taken so the life cycles of the two are connected. The best document for this is the Support Facilities Annex (SFA) of the Logistic Support Agreement (LSA). A summary of actions typically performed by the PM during a system’s life cycle are covered in figure 2–5 through figure 2–8 which may be used as a checklist, but each activity need not be performed for every system. The PM’s system safety advisor will recommend activities that are necessary for his system. The selected activities are then included in the SSMP.

Note. The HTL will be maintained and updated during all phases of the life cycle, as will the mishap risk management requirements.

2–13. Concept refinement phase

The purpose of this phase is to refine the initial concept and develop a Technology Development Strategy (TDS). Entrance into this phase depends upon a validated CDD resulting from the analysis of potential concepts and documented Initial Capabilities Document (ICD) to insure accomplishment of the Army’s mission as documented in the approved CDD. The TDS will document the rationale for adopting either an evolutionary strategy or a single-step-to-full-capability strategy. For an evolutionary acquisition, either spiral or incremental, the TDS will include a preliminary description of how the program will be divided into technology spirals and development increments, an appropriate limitation on the number of prototype units that may be produced and deployed during technology development, how these units will be supported, and specific performance goals and exit criteria that must be met before exceeding the number of prototypes that may be produced under the RD program.

a. The PEOs/PMs/MATDEVs/LCMC if appointed during this phase of the acquisition cycle will—

(1) Charter and manage a SSWG and develop the SSMP and TEMP to ensure they are current with the programs system safety goals.

(2) Conduct/develop a PHA/PHL to include a study of similar systems based on the historical safety data collected above. This will be completed to identify any desirable safety design features and is best accomplished as part of the Trade-off Determination (TOD). Any desirable safety design features identified during the TOD will be incorporated into the best technical approach (BTA) and the Request for Proposal (RFP).

(a) *Preliminary hazard list.* The PHL provides to the MA a list of hazards that may require special safety design emphasis or hazardous areas where in-depth analyses need to be done. The PHL may be required as part of the bidder’s response to an RFP. The MA may use the results of the PHL to determine hazards associated with the proposed concept, system safety capability of the contractor, or the scope of follow-on hazard analyses (PHA, sub-system hazard analysis (SSHA) and so forth). The PHL may be obtained using DI-SAFT-80101A.

(b) *Preliminary hazard analysis.* The PHA effort should be commenced during the initial phases of system concept, or in the case of a fully operational system, at the initiation of a safety evaluation. This will help in the use of PHA results in tradeoff studies that are important in the early phases of system development or, in the case of an operational system, aid in an early determination of the state of safety. The output of the PHA may be used in developing system safety requirements and in preparing performance and design specifications. In addition, the PHA is the basic hazard analysis which establishes the framework for other hazard analyses which may be performed. See appendix D for more details on PHL/PHA.

(3) Prepare and maintain the TEMP with the assistance of the Test and Evaluation Working Integration Process Team (TEWIPT). The PM must ensure adequate safety representation in the TEWIPT and all safety performance issues will be included. Ideally, these representatives also serve on the SSWG. The TEMP provides the basis for all testing and evaluation during the system’s life cycle. It integrates the activities of the test and evaluation community with the PEO/PM/MATDEV. The tests will be planned to prove systems operate as advertised or required and eliminate the deficiency noted in the MAA. The CBTDEV will provide safety issues and criteria for both technical and user testing. The safety representatives in the Test Integration Working Group (TIWG) must ensure that safety design features are adequately tested during development and user testing. (see paras 4–6, 4–7, and 4–8) The SSWG and HTS using information from the PHA/PHL must be fully functional by this time.

(4) The PM will ensure that selected members of the SSWG aid in preparation of the RFP. Key inputs include the statement of work (SOW), safety design, and evaluation criteria. The PM must get advice from the SSWG on which proposals are acceptable from a design safety standpoint. When applicable, the SSWG can recommend design concept changes that are necessary to make the proposal acceptable.

b. The CBTDEV/user representative will—

(1) Conduct system safety substudies to define the maximum allowable accident rate consistent with system

availability soon after completion of the MAA. That accident rates may be significantly higher in combat must be considered. Care must be taken in specifying accident rates, since testing is impractical. An early accident rate projection can serve the CBTDEV/user representative as a basis of comparison for accident rates projected for specific candidates. Also, an early accident rate projection is useful in defining safety requirements (for example, crashworthiness levels, roll over dynamics, or other appropriate safety requirements). The accident rate is directly related to the number of systems bought (“buy quantity”) to fulfill the need identified during the MAA. In projecting the “buy quantity,” the DCS, G-3/5/7 must allow for attrition due to accidents. The DCS, G-4 assists in determining the attrition rate. The CBTDEV/user representative must coordinate with the DCS, G-3/5/7 and the DCS, G-4 to ensure consistency between the attrition rate and the maximum allowable accident rate.

(2) Review the PEO/PM/MATDEV’s TOD safety substudy (if conducted) to ensure user safety issues are addressed. The purpose of the TOD safety substudy is to identify desirable safety design features. Safety design features fall into the following two categories:

(a) Design features that prevent accidents. These features can be determined from historical safety information. For example, if vehicle rollovers have been a problem for a past system, then features that make the new system more stable should be incorporated.

(b) Design features that contribute to the system’s ability to prevent or reduce injury once an accident occurs (for example, roll bars, and so forth).

(3) Conduct a safety substudy as a part of TOA. Any historical safety information not examined during the TOD must be studied. The safety design features identified during the TOD should be reexamined and trade-offs made within the context of overall system effectiveness. The purpose of this substudy is to identify mission-oriented safety requirements that will be incorporated into any requirements documents. Requirements documents should not specify a particular design, but must provide the designer with statements that define system performance/mission requirements. Given the system whose predecessor was prone to rollover, a statement regarding the desired stability of the new system is an example of a mission-oriented safety requirement.

(4) Determine the effectiveness of the safety design features and life-cycle accident costs will be estimated for each candidate during a safety substudy conducted as part of the Cost and Operational Effectiveness Analysis (COEA). The life cycle accident costs will be incorporated into the overall COEA. Estimates of life cycle accident costs are made based on the accident history of predecessor systems. The CRC can assist in the development of an appropriate methodology for a particular system.

(5) Prepare input to the human factors engineering analysis (HFEA). He must identify through analysis any safety issues within the MANPRINT area that may affect the system’s overall performance. Input to the HFEA will be provided to the Army Research Laboratory-Human Research and Engineering Directorate (ARLHRED). (See AR 602-1.)

(6) Participate in the TEWIPT if organized at this phase of the acquisition cycle. The following safety test issues and criteria will be developed and incorporated into the TEMP:

(a) The quality of the user test in the area of safety depends on the development of safety issues. During the substudies described above, the CBTDEV must be alert for potential safety test issues.

(b) User test criteria are expressions of the operational level of performance required of a military system operated by typical Soldiers. Criteria will be developed for each safety issue and, whenever possible, stated in quantitative terms.

c. The tester, if required during this phase of the acquisition cycle, will monitor the HTS/HTL and if appropriate initiate the test and evaluation plans and any safety releases that may be required.

d. The CBTDEV provides safety requirements for inclusion in operational requirements documents.

e. The user will request ACOM and installation safety offices to—

(1) Provide user safety requirements for inclusion in system specification requirements documents. These requirements will include all projected locations and operational specific requirements of all users.

(2) Evaluate the updated SSMP and System MANPRINT Management Plan (SMMP) and assess risk on operational effectiveness.

(3) Assist CBTDEVs as they conduct studies to point out critical safety-related operational requirements.

2-14. Technology development phase

a. The purpose of this phase is to reduce technology risk and to determine the appropriate set of technologies to be integrated into a full system. Technology Development is a continuous technology discovery and development process reflecting close collaboration between the science and technology community, the user, and the system developer. It is an iterative process designed to assess the viability of technologies while simultaneously refining user requirements. The CDD and the TDS will guide this effort. Multiple technology development demonstrations may be necessary before the user and developer agree that a proposed technology solution is affordable, militarily useful, and based on mature technology. The TDS will be reviewed and updated upon completion of each technology spiral and development increment. Updates will be approved to support follow-on increments.

b. If an evolutionary strategy is used, the initial capability represents only partial fulfillment of the overall capability

described in the CDD, and successive technology development efforts will continue until all capabilities have been satisfied. In an evolutionary acquisition, the identification and development of the technologies necessary for follow-on increments continues in parallel with the acquisition of preceding increments, allowing the mature technologies to more rapidly proceed into System Development and Demonstration (SDD). Each increment of an evolutionary acquisition program will have an associated milestone decision authority (MDA)-approved TDS.

c. The MATDEV/LCMC's Army (Basic and Applied Research) and Technology Base Laboratories will develop or update a PHL for each technology indicating all potential hazards. A system safety professional will perform appropriate hazard analyses prior to the project being presented to the TSWG for final review. After the TSWG has approved a technology from a safety standpoint, the technology will continue into the developmental phase. Once a PM has been assigned, the traditional system safety program will begin which will contain those items/events discussed in paragraph 2-13a. If the technology continues into the development phase without a designated PM, the safety office providing matrix support in coordination with the TRADOC Branch Safety Office will, at a minimum, develop a SSMP to guide the system safety program through development. For small items, it may be useful to develop a SSMP for a family of items (that is, fuses, batteries, and so forth).

d. Upon appointment, the PM should immediately evaluate the system safety program. A SSWG is required for major and designated acquisition programs. The purpose of the SSWG is to provide program management with system safety expertise and to ensure communication among all participants. Its authority is defined by the PM through the SSWG charter. A sample SSWG charter is at appendix B. The SSWG will accomplish the following:

(1) Prepare/update the SSMP. The SSMP formally organizes the safety program for the entire life cycle of the item being developed. It is prepared by the SSWG (for programs with a chartered SSWG) or the supporting safety office as soon as the source of system safety expertise has been identified. The SSMP is the instrument used to—

- (a) Apply system safety requirements to a particular program.
- (b) Designate the Government program system safety manager.
- (c) Set forth a plan of action for the SSWG.
- (d) Establish ground rules for Government and contractor interaction.
- (e) Assign tasks, financial requirements, training requirements, schedules, data, and personnel.
- (f) Designate which safety analyses and trade studies are required and when they should be performed.
- (g) Identify decision authority for specific levels of risk.

(2) The SSMP will be written to ensure system safety task outputs contribute to timely program decisions and objectives. Evaluation of system safety program progress will be in accordance with the SSMP and the system safety program milestones established therein. A sample SSMP with preparation guidance is provided at appendix C. The SSMP then becomes a part of the PM's overall acquisition strategy.

(3) The SSWG members, as listed in the charter, recommend actions to the PM to ensure that all system safety program requirements are met in a timely manner. To provide adequate system safety emphasis through personal leadership/involvement, the PM or their deputy will chair the SSWG. If they are not available, the PM will appoint an individual within their office to serve as chairman. This individual will also serve as a single point of contact for the system safety program. Based on the system safety qualifications of the individual from the PM's office, it may be desirable to appoint a system safety professional from an appropriate local safety office as co-chairman. The CBTDEV will be represented by a system safety professional or representative at the SSWG. A CRC representative will attend SSWG meetings for major systems as a DA Observer.

(4) The frequency of SSWG meetings will be set forth in the SSWG charter based on program milestones or on an as-needed basis as determined by the PM. A sample SSWG meeting agenda is as follows:

- (a) Review of safety plan milestones.
- (b) Description of new systems or changes to systems.
- (c) Status report of current safety efforts.
- (d) Review of accidents and failures; RAM data; human factors; and test and evaluation reports.
- (e) Review of individual system safety hazards (old and new) and system safety reports.
- (f) Review of documents supporting safety, such as test plans, budgets, contracts, and System Safety Program Plans (SSPP).

- (g) Assignment of actions and reports resulting from requests for action.
- (h) Preparation and approval of draft SSWG minutes.

(5) Other programs that do not follow the standard system life cycle phases, the responsible activity must carefully integrate the requirements of system safety into the acquisition process being used. The PM should formally request the support of a dedicated system safety professional from an appropriate safety office. The PM will then ensure that communication takes place between the Program Management's Office (PMO), the system safety professional, the user, and representatives of the various related disciplines. The PM should task the system safety professional with the development of an SSMP, which serves two purposes:

- (a) It provides a blueprint for the system safety program.

(b) It serves as a tasking agreement between the PMO and the safety office as to the level of effort required in terms of man-hours.

(c) Coordinate with the CBTDEV for collection of historical safety data on predecessor systems and the application of lessons learned which are critical to the development of a safe system.

e. The CBTDEV will—

(1) Participate in the TSWG and/or SSWG during all phases of the life cycle as a voting member.

(2) Assemble historical system safety information on similar predecessor systems. The CBTDEV must begin to collect this information soon after approval of the ICD or the CDD. Historical safety information is available from the following sources:

(a) CRC maintains a computerized data base containing accident information. Safety lessons learned are also available at <https://crc.army.mil>.

(b) The ARLHRED develops lessons learned in the area of human factors. These are available at <http://www.arl-army.mil>.

(c) The Air Force maintains a lessons learned data base. All lessons learned (including safety) are consolidated at the U.S. Air Force Aeronautical Systems Center (ASC) by the Directorate of Lessons Learned. These are available at <http://www.military-aerospace-technology.com>.

(d) The Navy maintains computerized safety lessons learned and accident data. These are available at <http://www.safetycenter.navy.mil>.

(e) The U.S. Army Materiel Systems Analysis Activity (AMSAA) prepares liaison activity reports that compile safety-related and other data regarding user perceptions on the effectiveness of fielded systems. These are available <http://www.amsaa.army.mil>.

(f) The materiel proponent maintains SOF and Ground Safety Notification System messages, EIRs, and QDRs. (AR 95-1, AR 750-6, DA Pam 750-8, and DA Pam 738-751.)

(g) The Defense Technical Information Center (DTIC) can provide information on research being planned, research currently being performed, and results of completed research. Information is available <http://www.dtic.mil>.

(h) Users of predecessor systems maintain historical safety information. User ACOMs/ASCCs/DRUs safety offices can provide system safety input/data.

(i) The Army Environmental Center (AEC) and U.S. Army Center for Health Promotion and Preventive Medicine (USACHPPM) maintain a repository of Health Hazard Assessment Reports. These are available at <http://aec.army.mil/usaec> and <http://chppm-www.apgea.army.mil>. AR 40-10 (Health Hazard Assessment Program in Support of the Army Materiel Acquisition Decision Process) provides guidance on integration of health issues into all phases of the acquisition process.

(3) Coordinate its SMMP with the SSWG to assure compatibility with the SSMP. (For more information on the MANPRINT Joint Working Group (MJWG), refer to AR 602-2.)

(4) The U.S. Army Materiel Command has a Web site titled the Army Logistics Electronic Product Support Network. The Web site is <https://aeps.ria.army.mil/aepspublic.cfm>. By entering into the Restricted Access area a CBTDEV can access the Safety Messages which includes GPMs, SOUMs, Safety Advisory/Alert Messages, ASAMs, SOFs, Air Crew Integrated System Messages that can assist the developer in historical problems.

(5) Determine the maximum allowable accident rate and coordinate with the user to identify user safety requirements for specific user locations, consistent with system availability. The tone for future system safety activity will be set by incorporating system safety objectives into all documents prepared by the CBTDEV such as the ICD.

f. During pretest planning, the PM will provide a copy of the hazard tracking list and a copy of the safety assessment report (SAR) to the tester. Test directives and test design plans for all tests will ensure that adequate data for an independent assessment of hazards is provided. If the PM has not established a HTS, the tester will ensure his test plans and test reports are complete enough to serve as a basis for starting a HTS. The tester will ensure that the results of these safety tests are accurately analyzed and covered in test reports and provided to the evaluator. Emphasis will be placed on checking hazards that have fixes applied and identifying those residual/uncorrected hazards about which the tester must be aware. In addition, this information will serve to support the development of a Safety Release by DTC prior to the conduct of testing involving Soldiers. DTC will develop a Safety Confirmation to support the System Evaluation Report and the Milestone B Acquisition Strategy Review. The user will request ACOMs/ASCCs/DRUs and installation safety offices to

(1) Assist CBTDEVs collecting historical safety information.

(2) Evaluate the SSMP and SMMP and assess risk on operational effectiveness.

g. The evaluator will evaluate the safety hazards or issues stated in the System Evaluation Plan (SEP) and the overall safety of the system at the end of the Milestone A phase and before entering the Milestone B phase of development. As part of continuous evaluation, the evaluator should assess and report the impact of unresolved hazards on the system effectiveness. In the design of the TEMP and the SEP, emphasis should be placed on both evaluation of the fixes made to previously identified hazards and identification of new hazards.

2-15. System development and demonstration phase

a. The purpose of the SDD phase is to develop a system; reduce integration and manufacturing risk (technology risk reduction occurs during Technology Development); ensure operational supportability with particular attention to reducing the logistics footprint; implement human systems integration (HSI); design for productability; ensure affordability and the protection of critical program information (CPI); and demonstrate system integration, interoperability, safety, and utility. Development and demonstration are aided by the use of simulation-based acquisition and test and evaluation integrated into an efficient continuum and guided by a system acquisition strategy and TEMP. The independent planning of dedicated Initial Operational Test and Evaluation (IOT), as required by law, and Follow-on Operational Test and Evaluation (FOT), if required, will be the responsibility of the Army Test and Evaluation Command (ATEC). A Director, Operational Test and Evaluation (DOT)-approved live-fire test and evaluation (LFT&E) strategy will guide LFT&E activity.

b. The critical design review during SDD provides an opportunity for mid-phase assessment of design maturity as evidenced by such measures as, for example, the number of completed subsystem and system design reviews successfully completed; the percentage of drawings completed; planned corrective actions to hardware/software deficiencies; adequate development testing; an assessment of environmental, safety and health risks; a completed failure modes and effects analysis; the identification of key system characteristics and critical manufacturing processes; and the availability of reliability targets and a growth plan; etc. Successful completion of the Critical Design Review ends System Integration and continues the SDD phase into the System Demonstration effort.

c. The broad system safety objective during this phase is to establish a satisfactory level of safety in design and performance specifications. The system safety characteristics are validated and refined through extensive analysis and testing. Trade studies will be conducted and risks identified. The contractor's SSPP is then put into effect. The SSWG Charter, SSMP, TEMP, PHA, and SAR will be reviewed and updated.

d. The PEOs/PMs/MATDEVs/LCMC should require delivery of the SSPP as part of the contractor proposal. This plan should be required of each integrating and prime contractor. The SSPP defines in detail those contracted elements required to conduct a comprehensive system safety program with emphasis on the required contractual performance. Preparation of an SSPP is included in the SOW within the RFP. After negotiations, the plan must be made part of the contractual agreement. The contractor SSPP will contain a brief description of the system, including such items as ground support equipment and test and handling gear. Due to the practical limitations of cost, schedule, and performance, not all of the identified hazards can be controlled by design. The SSPP will include the method selected by the contractor to establish relative priorities and acceptable risk. Government awareness and approval of this method is essential.

Note. The Government is considered the integrating contractor when one is not named and for in-house development projects, and as such will prepare the SSMP which incorporated the principle requirements of the SSPP.

e. Safety issues should be thoroughly evaluated and brought to the attention of the PM. Identification of safety failures in Engineering and Manufacturing Development (EMD) models is preferred to those in production models. Early identification of safety failures allows timely and more cost effective corrective action(s). The PM should ensure maintenance and operational hazard analysis results are reflected in maintenance and operator technical publications.

f. The CBTDEV will—

(1) Evaluate the impact of increased risk on operational effectiveness as tradeoffs are made for cost, weight, or schedule purposes. Mission-oriented safety requirements must be incorporated into requirements documents such as the CDD.

(2) Include safety in all training procedures and techniques for new systems. Particularly important is ensuring that equipment limitations are incorporated into the training and technical publications. Safety notes, cautions, and warnings are critical. Equally important is information regarding the actual operational constraints of the system. This information should be written to guide the operator in those situations not clearly defined in prior training. This information will be essential to the CBTDEV as new tactics and methods of employment are developed. Assuring that the operator is properly trained is a vital element of the total system safety effort. Training and technical manuals (TMs) must be reviewed to ensure inclusion of safety. Manuals must be very specific about what an item of equipment can and cannot do.

(3) Ensure the list of hazards controlled by training or procedure modifications are current and also maintained by the training developer. Training or procedure modifications are a last-resort control measure used when funding is critical. Unfortunately, neither training nor procedure modifications can completely eliminate a hazard. The effectiveness of training as a hazard control measure is frequently overestimated. It is essential for the training developer and CBTDEV to be realistic regarding the capability of the operator to overcome system inadequacies. The CBTDEV's recommendation should be made on the SSRA.

(4) Ensure that the safety of training equipment and devices will not be taken for granted. Many current acquisition strategies call for simultaneous development of such equipment. In addition to concern over the safe use of training devices, the CBTDEV and training developer must examine the degree to which the devices emulate the actual system. As more reliance is placed on training with devices rather than with actual equipment, the "realism" of the devices becomes a safety issue.

(5) The CBTDEV will attend design and program reviews to provide immediate user recommendations for risk-management decisions.

g. The tester will—

(1) Ensure precautions are taken to protect personnel and equipment during tests. SARs (DI-SAFT-80102A) and safety releases are used to integrate safety into test planning and procedures and for shipping and handling of the system.

(2) Prior to development and operational testing—

(a) Ensure a SAR is received from the contractor, reviewed, and accepted by the PEO/PM/MATDEV. The SAR is a formal, comprehensive safety report that summarizes the safety data that has been collected and evaluated during the life cycle. It expresses the judgment of the contractor regarding the hazard potential of the item and any actions or precautions that are recommended to minimize these hazards and to reduce the exposure of personnel and equipment to them.

(b) The PEO/PM/MATDEV sends the SAR and any additional comments to the test agency or command certifying that the system is safe to test. Technical testing cannot begin until the SAR has been received, reviewed, and accepted by the technical test agency or command. If no contractor is involved, the PEO/PM/MATDEV will prepare the SAR.

(3) Ensure that all safety releases are provided to the ACOMs/ASCCs/DRUs commander of the organization supplying the test Soldiers, thereby informing them of the risk. No test involving troops will begin until a safety release has been issued to the test organization (such as TRADOC boards and government laboratories) and the commander of the test Soldier has acknowledged the safety hazards and limitations for both Operational Testing and Evaluation (OT) and Developmental Testing and Evaluation (DTE). (AR 73-1) Safety releases are provided to user test organizations by ATEC.

(4) Monitor the HTS/HTL and update/revise the test and evaluation plans and so the safety releases describe the specific hazards of the item or system and will include technical and operational limitations and precautions. The format for a safety release is provided at appendix F. The test agency or ACOMs/ASCCs/DRUs command will ensure that test objectives can be met within the limits stated in the release.

h. The user will—

(1) Provide CBTDEVs recommendations for mishap risk management decisions.

(2) Ensure the ACOMs/ASCCs/DRUs safety offices evaluate the updated SSMP and SMMP and assess impact of increased risk on operational effectiveness of trade-offs.

2-16. Production and deployment phase

The purpose of the Production and Deployment phase is to achieve an operational capability that satisfies mission needs. Operational test and evaluation will determine the effectiveness and suitability of the system. The MDA will make the decision to commit the Department to production at Milestone C. Milestone C authorizes entry into LRIP (for major defense acquisition programs (MDAPs) and major systems), into production or procurement (for non-major systems that do not require LRIP) or into limited deployment in support of operational testing for MAIS programs or software-intensive systems with no production components.

a. The PEOs/PMs/MATDEVs/LCMC will—

(1) Evaluate and document the safety impact of each MOD and ECP submitted during this phase. The PM will ensure that all safety-coded MODs and ECPs contain a risk assessment. The purpose of the risk assessment is to provide the decision authority sufficient information to properly understand the amount of risk involved relative to what it will cost in schedule and dollars to reduce that risk to an acceptable level.

(2) Address the adverse safety trends identified by accident and safety deficiency reporting during the deployment phase. Invariably, unanticipated hazards are discovered during this phase. Maintenance of the HTS is essential. Previously identified hazards will have to be tracked to ensure the criteria associated with the accepted risk have not changed. If the accident probability or severity is worse than anticipated, the CBTDEV must be notified so that a MOD can be initiated. In addition, the using ACOMs/ASCCs/DRUs must be advised and supplied with any information/documentation on these hazards.

b. The CBTDEV will—

(1) Provide performance objectives to the user to provide available criteria by which to evaluate the system.

(2) Initiate MODs if accident severity or probability exceeds accepted residual risk associated with a specific residual hazard.

(3) Review MOD risk assessments and incorporate the user's recommendation on acceptability of residual risk into the MOD package. The MOD process is described in AR 70-1.

(4) Formally coordinate mission changes with the PEO/PM/MATDEV and the user to ensure that system capabilities are not exceeded. Mission changes include modification of tactics or doctrine as well as changes to mission profiles. Such mission changes may create hazards. When mission changes are being developed, the CBTDEV will coordinate with the PEO/PM/MATDEV and the user to determine the safety impact of that mission change. The PEO/PM/MATDEV will determine if there are adverse impacts (such as, performance limitations or MANPRINT factors) on the system. In addition, the CBTDEV, in coordination with the user, will review modifications of doctrine, tactics,

techniques, and procedures (to include those developed in the Battle Lab) for safety impact. If hazards are identified during these reviews, the mishap risk management process described in section I of this chapter will be used to resolve them.

c. The tester will—

- (1) Ensure all activities in paragraph 2–15c have been completed and updated/revised, as appropriate.
- (2) Assist in testing ECPs or MODs, as required.

d. All user safety offices will—

- (1) Monitor field failures and accidents to identify hazards.
- (2) Assist in identifying system failures that exceed accepted residual risk specifications.
- (3) Issue a safety confirmation to support development of the SER and the Milestone decision, as required by the DTC.
- (4) Provide input to CBTDEVs of residual risks on MODs.
- (5) Review system safety assessment to identify potential problems.
- (6) Monitor new or modifications to existing facilities in order to identify hazards.

2–17. Operations and support phase

a. The objective of this phase is the execution of a support program that meets operational support performance requirements and sustains the system in the most cost-effective manner over its total life cycle. When the system has reached the end of its useful life, it must be disposed of in an appropriate manner. Effective sustainment of weapon systems begins with the design and development of reliable and maintainable systems through the continuous application of a robust systems engineering methodology. As a part of this process, the PM will employ human factors engineering (HFE) to design systems that require minimal manpower; provide effective training; utilize representative personnel; and are suitable (habitable and safe with minimal environmental and health hazards) and survivable (for both the crew and equipment).

b. At the end of its useful life, a system must be demilitarized and disposed in accordance with all legal and regulatory requirements and policy relating to safety (including explosives safety), security, and the environment. During the design process, PMs will document hazardous materials contained in the system, and will estimate and plan for demilitarization and safe disposal.

c. The PEOs/PMs/MATDEVs/CBTDEVs/users/LCMC will track system maturity and deficiencies as discussed in paragraph 2–16. Further, they will document all adverse safety trends identified by accident and safety deficiency reporting to insure a complete historical document for any follow-on system development activities. Documentation will include a complete and accurate HTL.

Chapter 3 Integration of System Safety Associated Disciplines

3–1. General

a. Associated disciplines are integrated into the system safety program by the PM through the SSWG. This integration is extremely beneficial to the safety effort since hazards are identified through the efforts of an associated discipline. In many cases the boundaries that distinguish between the disciplines are unclear. In fact, difficulties have arisen in previous acquisitions due to isolation of the various disciplines. For example, the assumption by one group that another group will identify a hazard leads to an unresolved hazard.

Note. Regardless of who identifies a hazard, it is the responsibility of the SSWG to track the hazard to/through resolution.

b. The areas discussed in this section are considered an associated discipline, and their representatives must be participants in the system safety program. The SSWG must consider their outputs and actions as the source for identification of hazards.

3–2. Reliability, availability, and maintainability

a. A RAM program is required for most systems per DODD 5000.1.

b. Reliability is the probability that an item will perform its intended function for the duration of a mission or a specific time interval. It is usually stated as a mean time (or distance, rounds, and so forth) between failures (MTBF). The requirement for a reliability program plan (DI–R–1730) is normally incorporated into the RFP. Provisions will be made for the SSWG to examine Reliability Test Reports (DI–TMSS–81586A) and Failed Item Analysis Reports (DI–R–7039). Environmental factors, failure rates, failure modes, MTBFs, and problems associated with major items of system equipment are usually contained in these reports.

c. Availability is the percentage of time an item is in a mission-committable status expressed as inherent, achieved, or operational availability. A failure modes, effects, and criticality analysis (FMECA) report (DI–QCIC–81722) will

normally be required as a part of the reliability program. The contractor's integration of the results of the FMECA into their system safety program will be established as criteria for the SSPP evaluation during source selection in those cases where the FMECA is required.

d. Maintainability is a measure of the ease with which an item is maintained and repaired. It is usually stated as a mean time to repair (MTTR). A maintainability program will normally be required per military handbook (MIL-HDBK)-470A). Interface must be established between the maintenance program and the system safety program to obtain maintenance-related information for the operating and support hazard analysis (O&SHA). This exchange of information should be reflected in the maintainability program plan (DI-MNTY-81600).

3-3. Quality engineering

As part of the quality program, the critical items safety program, produces data that affects the system safety effort.

a. The objective of the program is to establish policies and responsibilities for the identification and control of critical items throughout the life of the system. This objective is to be achieved through identification of critical items, development of life cycle control policies, and implementation. Accomplishment of the objective requires that critical items be identified and tracked from design through purchasing, manufacturing, transportation, and maintenance to the user.

b. One key tool in the overall critical items program is the service life surveillance program. Its objective is to assure that design requirements are valid and retained during storage and use. The primary function of the service life surveillance program is to—

- (1) Monitor existing product quality.
- (2) Detect any safety or other unsatisfactory conditions and trends.
- (3) Investigate failures.
- (4) Identify improvements.
- (5) Encourage disposition of unsatisfactory items.

c. The PM will ensure that the SSWG monitors the critical items and service life surveillance programs. Also, the PM must ensure contractor integration of those programs into the contractor's system safety program by requiring a quality program plan (DIR 1710) in the RFP and establish it as evaluation criteria for the SSPP and for the quality program plan during source selection.

3-4. Integrated logistic support

As one of its primary tools, ILS employs a management science application termed LSA.

a. A LSA is required for all acquisition programs by AR 700-127 and should be established per MIL-STD-13881. The Logistic Support Analysis Record (LSAR) (MIL-STD-13-882A) is a manual and/or automated database that is used to document, consolidate, and integrate the detailed engineering and logistics data generated by the LSA process.

(1) All operator and maintenance tasks are documented on LSAR Data Records C and D (also known as "input data sheets").

(2) Operator and maintenance TMs are prepared using LSAR Data Records C and D and related LSAR output report summaries (for example, maintenance allocation charts, repair parts, and special tools lists).

(3) The PM must ensure that current facility-related safety and health information is identified and documented in the SFA of the ILS plans.

b. Government LSA Review Team representatives in the research and development effort will meet on a regular, contractually established schedule to review the status and content of the LSA/LSAR with the contractor. Maintenance tasks will have to be identified before conducting a good maintenance hazard evaluation. Consequently, final safety assessments should not be required before completion and Government acceptance of the LSAR Data Records C and D and final drafts of operator and maintenance TMs.

c. The contractor's integration of the results of the LSA/LSAR program into the system safety program will be established as evaluation criteria for the SSPP during source selection.

3-5. Combat survivability

Normally, survivability is a general term used to describe a system's ability to avoid and/or withstand man-made damage-causing mechanisms. The "avoid" part of the definition is termed "susceptibility," and the "withstand" portion is termed "vulnerability." Areas of mutual interest between system safety and combat survivability are discussed below.

a. Within the area of vulnerability, the disciplines share a desire to eliminate single-point failures and incorporate crashworthiness or other specified safety features.

b. Survivability design features will affect both crashworthiness and emergency egress. However, the term survivability has recently been expanded to include both Soldier and equipment unless otherwise specified. Survivability features of a system and Soldier survivability must be designed to be maintainable throughout the system or facility's life cycle. Additionally, when the system is modified, the threat changes, or there is a change in the doctrine of system deployment, a survivability review by the CBTDEV and MATDEV will be required. The CBTDEV and MATDEV consider the threat from milestone 0 throughout the entire life cycle of each acquisition program.

c. Survivability analysis is a process that starts during phase 0 and continues throughout the life cycle of the system. Survivability analysis will be integrated over the full spectrum of battlefield threats to insure that synergistic threat effects are adequately addressed. Analyses of survivability against each threat, to include TOAs, will be done in the context of all threats and balanced across all survivability disciplines to maintain overall mission performance. The integrated survivability analysis will be maintained for use as a survivability audit trail of requirements, tradeoff decisions, and quantitative measures of effectiveness. Analysis will include consideration of training, doctrine, tactics, techniques, and procedures, and materiel capabilities. Training, doctrine, and materiel survivability objectives will be refined as the design progresses. The SSMP and SMMP will identify and track the resolution of safety and Soldier survivability concerns throughout the system's life cycle.

d. Shortfalls in the satisfaction of survivability requirements must be substantiated by the MATDEV, in coordination with the CBTDEV (see AR 70-1), and submitted to the MDA during the milestone review process. Rationale for failure to meet requirements, as well as risk analysis and risk mitigation approaches, will be included as part of the substantiation process. Shortfalls which introduce safety hazards must enter the system safety CRM process for resolution or acceptance.

e. Survivability must be considered at the force level as well as at the system level. Survivability of support items, including mission essential resupply and sustainment assets, must be balanced and integrated with the survivability goals of individual systems. Force protection, whereby individual systems provide mutual defense by sharing survivability assets will be considered.

f. Fratricide due to the collateral effects of friendly systems is to be considered a threat. Failure to control fratricide will be considered a safety hazard and will be managed in accordance with Army safety CRM requirements specified within this pamphlet.

3-6. Human factors engineering

a. The HFE Program is a domain of MANPRINT and a life cycle activity, responsible for properly integrating the human element into systems. The Deputy Chief of Staff, G-1 (DCS, G-1) exercises staff responsibility for the HFE Program and AMC has the system integration responsibility. AR 602-1 provides the policy and procedures guiding the program.

b. Making systems error-tolerant is one of the most critical tasks to be accomplished to enhance force protection and mission effectiveness. Lessons learned from wartime and peacetime operations indicate that accidents caused by inadequate HSI have been as effective as the enemy in killing Soldiers and destroying equipment. By effectively incorporating HFE lessons learned into our system design(s), they will be more error-tolerant.

c. Human factors hazard identification and management is an integral part of HFE. Life cycle tests, analyses, and other tasks must include efforts to ensure critical human performance problems (actual or potential) are being systematically identified and managed to reduce risk. Key sources of information include accident and incident data, system hazard analyses, and other information from predecessor and current systems. These analyses will help establish the probability and severity or safety related human performance problems for risk assessments, management, and tradeoffs. (See 2-14e for a listing of available data bases.)

d. Program interfaces must be established between HFE and system safety engineering (SSE) to assure a continuous dialogue exists throughout the system life cycle. Actions which will strengthen the interface between programs follow:

- (1) Joint participation in HFE and SSWG meetings.
- (2) Co-sharing of program analyses which identify safety related human performance problems, their relative probability, and severity, and mitigating actions.
- (3) Requiring HFE manager recommendations on all SSRAs relating to human performance; requiring SSE manager recommendations on all HFE assessments with safety implication.
- (4) Requiring HFE manager estimates of the effectiveness for all designs, training, procedures, warnings, and guards used to eliminate or mitigate hazards.
- (5) Ensuring program documents clearly delineate roles and responsibilities between HFE and SSE for identifying, managing, and communicating safety related human performance problems (predecessor or current system) throughout the life cycle.
- (6) The HFE participation in accident investigations and prevention programs.
- (7) SSE support to HFE with safety related information on user problems identified in accidents, incidents, tests, and other sources.

3-7. Health hazards

a. The USAMEDCOM is the proponent for the health hazard assessment/Systems Health Hazards Program through the AEC. AR 40-10 provides the policy and procedures for the conduct of the health hazard assessment (HHA). The health hazard program is an integrated effort throughout the materiel acquisition process which considers mission needs, concept analysis, research, development, testing, evaluation, production, procurement, training, use, storage, system maintenance, transportation, demilitarization, and disposal. The primary objective of the health hazard program is to identify and eliminate or control health hazards associated with the life cycle management of weapons, equipment,

clothing, training devices, materiel, and information systems. The HHA itself, identifies, evaluates, and provides recommendations to eliminate or control health related hazards. The Army designated manager for the HHA/Army Systems Hazards Program is the USACHPPM.

b. Typical categories of health hazards include the following examples:

- (1) Acoustic energy encompassing steady-state noise, impulse noise, and blast over pressure.
- (2) Biological substances, to include microorganisms, which cause disease, plus sanitation issues.
- (3) Chemical substances such as combustion products from weapons firing and engine exhaust, smokes and obscurant and other toxic materials.
- (4) Oxygen deficiency in crew or confined spaces or caused by operations in high altitude environments.
- (5) Radiation energy from ionizing, nonionizing, and radiant sources.
- (6) Shock due to rapid acceleration or deceleration.
- (7) Temperature extremes and humidity resulting in heat and/or cold injury.
- (8) Trauma resulting from blunt or sharp object impact or musculoskeletal injury.
- (9) Vibration affecting the entire body or specific parts causing physiological damage.

c. The HHA is an independent medical assessment that addresses materiel system hazards to prevent potential physiological damage to the operator, crew, or maintainer of the system under normal operating conditions. The HHA/Army systems HHA may change as the system develops. This requires the developers to request Army system HHAs early-on and whenever new data is obtained. These assessments provide complementary information for system safety functions such as hazard analysis, hazard tracking, and mishap risk management. Likewise, system safety hazard analyses can be a primary means of identifying potential health hazards. The SSWG must be prepared to support USAMEDCOM in the area of hazard identification and to develop a coordinated effort for resolution of identified hazards.

d. The PEO/PM/MATDEV will request an HHA and ensure the SSWG is placed on distribution for related HHAs. The PEO/PM/MATDEV will ensure the RFP requires contractor information to support the HHA based on the potential health hazard issues identified in the initial HHA or SMMP.

3–8. System safety in the MANPRINT process

Improving HSI to make systems more error-tolerant is one of the most critical tasks for enhancing force protection and mission effectiveness. The MANPRINT process provides the vehicle for system safety to influence the human-system integration aspects of materiel design, development, acquisition, and usage in accordance with AR 70–1.

a. MANPRINT is a comprehensive management and technical effort to ensure optimum human performance and reliability in the operation, maintenance, use of weapon, equipment, and information systems. Its objective is to influence Soldier-materiel system design for optimum total system performance by considering the seven MANPRINT domains of manpower (spaces), personnel (faces), training, human factors engineering, system safety, health hazards, and Soldier survivability before making a functional allocation of tasks between people, hardware, and software. MANPRINT integrates and represents seven previously listed domains at the decision reviews. United under the umbrella of MANPRINT, the domains as a group are expected to gain more influence on the decision making authority. System safety is not subordinate to MANPRINT. They co-exist and must be able to interface with each other.

b. One of MANPRINT's key objectives is to ensure stronger representation for each of the domains at the decision reviews. The fact that MANPRINT represents system safety at the reviews is a major change from the way safety has done business. The MJWG safety representative and reviewers of the SMMP must ensure certain system safety items are included in the document. (See app G.) The CRC will develop an independent safety assessment for ASARC-level MADPs and provide a copy to the PM, the Director for MANPRINT, DCS, G–1, and to the ASARC co-chairman through the ASARC data book.

c. The MANPRINT is tailored for all materiel acquisitions, ranging from major weapon systems, to less costly MOD, and NDI acquisitions (AR 602–2). The effort given to a system will depend on the type of system. If a system has little man-machine interface, such as an NDI acquisition of a computer printer, very little MANPRINT involvement will be needed. When considering a system such as a new helicopter system, a major MANPRINT effort will be needed to ensure all interface issues are considered.

d. The MANPRINT does not incorporate all areas that system safety defines. Certain tasks and processes required to implement system safety must be completed within the system safety function and independent of MANPRINT processes. These areas include, but are not limited to the following:

- (1) Budget requirements.
- (2) Facilities safety.
- (3) ECPs/MODs.
- (4) Post fielding safety tracking requirements.
- (5) Materiel only safety hazards.

e. System safety will continue with its responsibilities for these areas as defined prior to MANPRINT. MANPRINT has created additional integration responsibilities for system safety. MANPRINT requires two things of system safety:

- (1) Ensure that the human is included in safety analyses and tests.
- (2) Those system safety acquisition efforts are coordinated with each of the other domains.

3–9. Environment

a. Federal law, as implemented by 32 CFR 651, requires compliance with all Federal, state, and local environmental laws. Laws include those covering environmental compliance, restoration, pollution prevention, and conservation of natural and cultural resources. Environmental requirements cover prevention, remediation, and control of pollutants which may impact air, water, and natural and cultural resources. Pollutants include but are not limited to noise, radiation, and hazardous materials and wastes. Environmental documentation, which may include environmental impact statements, environmental assessments, and/or documentation of categorical exclusions, should be prepared and reviewed in accordance with 32 CFR 651.

b. Documentation in 32 CFR 651 tends to indicate those environmental concerns which already exist in the new system or facility design, test plans, or fielding events. Rather, an environmental hazard evaluation of the new system or facility design must be effectively integrated along with system safety and health hazard analysis to minimize the environmental impacts during the system or facility's life cycle.

c. The best approach is to "design for environment" by designing out the environmental hazards associated with a system or facility as is done for system hazards in the mishap risk management process. The environmental hazard identification and evaluation process is closely related to the system safety mishap risk management process identified in chapter 2.

(1) The environmental hazard analysis process requires a detailed review of existing system or facility design materials to ensure that they do not require the use of materials such as Ozone depleting substances (ODS Class I). If ODS Class I or other hazardous materials are identified, there are no substitutes, and they are required, these materials must be evaluated for their potential environmental impacts and the hazards identified, a RAC assigned, and any residual risk accepted by the appropriate decision authority. This includes reducing the use of hazardous materials in manufacturing processes and products rather than simply managing the hazardous waste created.

(2) Where the use of hazardous materials cannot be reasonable avoided, procedures for identifying, tracking, storing, handling, and disposing of such materials and equipment will be developed and implemented as outlined in DODD 4210.15 and DODI 6050.5. The AEC is available to assist as needed.

(3) Life cycle cost estimates must include the cost of acquiring, handling, using, and disposing of any hazardous or potentially hazardous materials during the system or facility's life cycle.

Chapter 4 System Safety for Testers and Evaluators

Section I Introduction

4–1. General

a. Army test and evaluation has the following three purposes:

- (1) To help the PEO/PM/MATDEV uncover system problems for correction.
- (2) To help the decision authorities determine whether development is progressing satisfactorily and whether the system is likely to meet operational needs.
- (3) To determine if hazard control measures are adequate.

b. This chapter provides the tester and evaluator the information they need to develop and conduct a system safety test or evaluation. The key to this effort is the formulation of a TEMP. The major effort of safety testing should be directed toward identifying, evaluating, and tracking hazards (see chap 2, sec I). Hazard resolution will be accomplished by the PEO/PM/MATDEV. System safety evaluations should focus on deficiencies in the system safety program as well as hazards.

c. Test and evaluations apply to both developmental and NDI acquisition strategies. Testers' system safety requirements by phase during the materiel acquisition life cycle are covered in chapter 2, section II.

4–2. Definition

a. Testing is the gathering and summarizing of empirical system data under controlled conditions. Technical testing of materiel systems is conducted by the PEO/PM/MATDEV in factory, laboratory, and proving ground situations to assist the engineering design and development process. This and other data are used by the technical evaluator to verify attainment of technical performance specifications and objectives.

b. User testing of materiel systems is conducted with representative operators, maintainers, crews, and units under realistic combat conditions. The evaluator uses these and other data to—

- (1) Estimate the operational effectiveness and suitability of the system.
- (2) Identify the need for modifications.
- (3) Examine the adequacy of concepts for doctrine, tactics, organization, and training.

c. In addition to test data, evaluations can be based on results of analytical or logical modeling such as computer simulations and war games. Information entered into the models may include combat data, experimental data, assumptions, and data generated by other models.

Section II

Test Planning

4-3. Adaptation

A successful system safety test and evaluation effort requires adaptation in order to fit the particular system test. Not every test event need be performed for every system. The test agency may consult the SSWG on which tests are necessary for a particular system. The selected tests or assessments are then included in the TEMP and the safety subsection of the test design plan or detailed test plan.

4-4. Checklists

Initial distribution is made by Headquarters, DTC, who is responsible for the initial placing of published documents into Versatile Information Systems Integrated On-line (VISION), an ATEC initiative to integrate data across test centers to provide a common web-based user interface is available at <https://vdlis.atc.army.mil>. Published documents are also distributed into the DTIC.

4-5. Test integration

System Safety tests for critical devices and components will be incorporated into tests required for other disciplines. This is accomplished through the TEWIPT. The PM will ensure adequate safety representation in this group.

Section III

Conduct of Test

4-6. General

a. There are some trade-offs between safe testing and safety tests. The tradeoffs are between the benefits to be gained from safety testing versus the risk and cost associated with a particular test. The safety release process should be used to resolve any conflicts in this area.

b. Safety testing can be used to—

- (1) Identify hazards, determine appropriate corrective actions, and establish corrective action priorities.
- (2) Determine and evaluate appropriate safety design and procedural requirements.
- (3) Determine and evaluate operational, test, and maintenance safety requirements.
- (4) Determine the degree of compliance with established qualitative objectives or quantitative requirements, such as technical specifications, operational requirements, and design objectives.

4-7. Developmental tests

a. Developmental tests (DT) are primarily concerned with determining whether the system or equipment has attained the technical performance specifications and objectives called for in the supplier's contract with the PEO/PM/MATDEV and to determine if the system is ready for user/operational testing.

b. It is imperative that the tester obtain the HTL before starting DT. The list is used along with the SAR to identify the remedies that have been applied to correct previously identified hazards. Safety tests within DT are then performed to verify the adequacy of the remedy.

c. During technical testing, specific safety and human health tests are also performed on critical devices or components to determine the nature and extent of materiel hazards. Requirements for such tests will be found in the TEMP and independent evaluation plans and are usually performed during DT when contractor testing and data are not sufficient to make a hazard assessment. Special attention is directed to—

- (1) Evaluating special safety and health hazards listed in paragraph 3-7.
- (2) Verifying the adequacy of safety and warning devices and other measures employed to control hazards.
- (3) Analyzing the adequacy of hazard warning labels on equipment and warnings, precautions, and control procedures in equipment publications.
- (4) Verifying the adequacy of safety/health guidance and controls in the SAR, TMs, and Initial Health Hazard Assessment Report (IHHAR).

(5) Considering hazard mitigating recommendations in reviewing and/or developing test center standing operating procedures (SOP).

(6) Including/coordinating any unique data requirements in the safety or human health test designs that are implied in test documentation (for example, SAR IHAR, and so forth).

(7) Identifying new hazards in reports and test incident reports when the risk assessment is inaccurate or requires revision.

4-8. User tests

a. The operational evaluator estimates total system performance of a materiel system when it is put to use, maintained, and supported by the Soldiers, crews, and units who will be expected to make the system work successfully in combat. The testing must occur in a realistic combat situation with as little interference with the conduct of the operation as feasible. Furthermore, a system must be certified to be safe for troop use under the conditions or limitations specified in the safety release before any user testing begins. Therefore, OT of safety issues is less systematic and less technical than that conducted during DT. It is common, however, for unanticipated hazards to occur when a system is placed in the hands of Soldiers and put in operation. Therefore, test planning must include disciplined observation and other data collection procedures to ensure that such hazards are identified and added to the HTL.

b. Hazards identified in previous DTs that have subsequently been corrected must be evaluated during the user test to see if the correction is adequate in an operational environment. A safety consideration unique to OT is whether any safety release restrictions imposed are so confining that the user's training needs cannot be met or that an adequate user test cannot be conducted.

4-9. Non-developmental item tests

a. Contrary to Government system development efforts, most NDI acquisition efforts effectively preclude the Army from obtaining detailed safety engineering evaluations or assessments from the prime contractor. Safety testing will be oriented to tests that are specifically required to fill gaps that have not been satisfied by contractor data. Specific test issues will be determined during the market survey and incorporated into the TEMP. (For more information on market surveys, see AR 70-1.

b. Non-developmental items tests frequently require as much testing as a pure development item because of utilization in an unplanned environment and assembly of parts in a new configuration. The SARs and safety releases are required for NDI testing.

Section IV Evaluations

4-10. Independent evaluators

a. The ATEC by means of the AEC conducts continuous evaluation (CE) on all assigned systems. Continuous evaluation is a process that provides a steady flow of evaluation information to the combat and materiel developers on a proposed acquisition, even as the acquisition evolves from a laboratory or experiment to an identified and recognized program or project. Continuous evaluation, conducted by ATEC, will be employed on all acquisition programs. Continuous evaluation is a strategy that ensures responsible, timely, and effective assessments of the status of a systems performance throughout its acquisition process. Continuous evaluation can begin as early as the battlefield functional mission area analysis and continue through system post-deployment activities. The continuous evaluation process includes system evaluation and system assessment. System evaluation focuses on issues of system technical and operational characteristics, performance, and safety as a part of system operational effectiveness, suitability, and survivability. The system evaluation report focuses on the capability of the system to accomplish its mission in its intended environment and is provided to the MDA.

b. In addition, other organizations assess the system's demonstrated logistics supportability, cost effectiveness, performance in a threat countermeasure environment, and ease of operation and maintenance by troops.

c. One element of analysis that is common to all independent evaluations is system safety. A system safety evaluation focuses on the existing status and impact of any hazards or program deficiencies in terms of the system's overall effectiveness.

d. System safety issues enter the CE process through continual dialogue among the PEO/PM/MATDEV, CBTDEV, technical and operational testers and evaluators, and other members of the acquisition team. Key activities for input of system safety issues to CE are the developed TEMP issues and criteria. Again, the forum for coordination of acquisition team activities is the TEWIPT. The SSWG ensures that the updated SSMP is used throughout the development process by the TEWIPT for updating the TEMP and by DTC for updating the System Evaluation Plan (SEP).

4-11. U.S. Army Combat Readiness Center independent safety assessment

An independent system safety assessment of each major system is prepared by CRC and provided to the ASA(ALT) at each milestone review. Prior to transmittal, these assessments are coordinated with the appropriate acquisition elements

and their supporting PEO/PM/MATDEV safety offices. A CRC evaluation provides an assessment of the system safety program and identifies the high risk residual hazards that require attention at the milestone reviews. In addition to the ASA(ALT), the independent safety assessment is provided to the DCS, G-1 (MANPRINT), the spokesman for safety at the reviews.

Part Two Facility System Safety

Chapter 5 Facility System Safety Management

5-1. Objectives

Construction, engineering, operations, research development and maintenance activities on Army property range from self-help projects performed by unit/organization personnel and housing residents to multi-million dollar U.S. Army Corps of Engineers (USACE) major construction projects performed by civilian contractors (including civil works projects). The objectives of the Facility System Safety (FASS) Management Program are—

- a. Conducting system safety programs to minimize risks throughout the facility system life cycle.
- b. Conducting hazard identification, FASS risk management, and hazard tracking procedures during facility development, construction, operation and disposal.
- c. Maximizing operational readiness and mission protection by ensuring that cost-effective hazard controls are efficiently designed and constructed.
- d. Ensuring that hazards inherent to the design, equipment, and intended use of the facility are eliminated or the resultant risks of the hazards are controlled to an acceptable degree.
- e. Reducing safety and occupational health retrofit and modification requirements after the design stage.

5-2. Participants

The effectiveness of the system safety program can be directly related to the aggressive and cooperative spirit of the participants. No program can be effective without aggressive pursuit of safety as a program goal, nor can it be effective without the active support and cooperation of the following participants:

a. *Using activity or installation.* The importance of active and meaningful participation by the user community cannot be overstated. As it is elsewhere in facility planning and design, appropriate input from the user during the initial planning stages is critical to the FASS Program. Without such input, the effectiveness of any system safety effort is seriously degraded while at the same time the cost of the effort becomes prohibitive. The using installation is responsible for identifying overall facility hazard level, including funding for the necessary facility system safety effort and initiating the FASS management program.

b. *Engineering organization.* The engineering organization (USACE or installation engineering organization) is responsible for the design and management of military construction and civil works projects. While USACE Districts serve as the engineering organization for the majority of military construction projects, these projects may also be designed and managed by the installation engineering activity. In either case, the engineering organization, with input from the using activity, establishes the scope of the FASS effort and incorporates any appropriate and necessary system safety tasks into the project design requirements. During construction, the engineering organization assures that design features for the control of hazards are properly installed in the project. The engineering organization will be the prime collaborator with the using activity for planning, executing, controlling and closing the design project.

c. *Design agent.* Design of a project is carried out by an A/E firm under contract or by the in-house USACE district or installation/activity personnel. In all cases, the designer is responsible for conducting and documenting any hazard analyses that are required during the design phase. The designer is responsible for completing any system safety tasks required by the FASS program and/or contract specifications, utilizing the output from hazard analysis as input to the design, and for developing, evaluating, and implementing appropriate hazard controls. During the design process, the design agent will review all proposed design changes for impact to FASS. The design agent will document residual hazards and initiate action to obtain risk acceptance decisions as required. The design agent should interface with the using activity and engineering organization to identify design impacts to/from the installation (for example, siting, utilities, hazardous materials, traffic patterns, adjacent facilities, and so forth).

d. *USACE Divisions and Direct Reporting Units.* The USACE Divisions and DRUs have responsibility for supervision and oversight of the system safety activities carried out by their subordinate organizations.

e. *Headquarters, U.S. Army Corps of Engineers.* Headquarters, USACE develops and maintains overall facility/project system safety policy and program guidance.

Chapter 6 Facility System Safety Program Management

6-1. General

The purpose of this chapter is to discuss the basic operating procedures used in the FASS effort. The following sets forth the actions required in the planning, design, and construction phases of Military Construction (MILCON) funded or civil works facilities. These actions will be performed by the responsible FASS participants identified in paragraph 5-2.

6-2. Background

The FASS process is structured to concentrate user and designer resources on the identification and control of hazards in the criteria development and design stages of projects. Further, the FASS process is structured to emphasize hazards that are not covered by codes and standards. The FASS process examines the specifics of the hazards involved, the level of risk and the appropriate control mechanisms. The FASS effort is intended to vary from project to project in scope and complexity. The FASS effort must be tailored to the project and the effort expended must be commensurate with the degree of risk involved. This is accomplished through a facility risk assessment process during the projects programming and planning stage.

6-3. Using or activity installation responsibilities

a. Appointment of a System Safety Project Team. The System Safety Project Team (SSPT) is the body that accomplishes those initial system safety tasks performed by the using installation or activity. Appointment of this team should be accomplished upon initiation of project planning. While membership and the level of participation may vary from organization-to-organization and from project-to-project, it is recommended that the initial SSPT be comprised of at least the following representatives:

- (1) Representatives from the appropriate MILCON stakeholders should be included in any MILCON SSPT—
 - (a) Member of the activity that will occupy the facility. This individual must have a detailed knowledge of the mission and function of the project and of specific hazards introduced by the work activities to take place within the structure and the impacts of the structure to/from adjacent activities.
 - (b) A representative from the Directorate of Public Works (DPW) or equivalent, or the appropriate USACE agency. This individual will provide the group with information regarding the project schedule, planning data, background information on the MILCON process. The Directorate of Engineering and Housing (DEH)/DPW representative will normally serve as the SSPT Chairperson in the initial SSPT.
 - (c) A representative from the installation safety office will provide background information and knowledge in the system safety process, address safety and occupational health standards applicable to the project design and construction, and will provide information related to accident and injury data regarding like or similar structures.
 - (d) A representative from the installation medical activity or clinic is generally an industrial hygienist or environmental health officer who has detailed knowledge of the health hazards associated with the installations mission and functions.
 - (e) A fire protection engineer or specialist brings detailed knowledge of fire hazards, fire prevention measures, and fire protection requirements.
 - (f) An environmental engineer or specialist brings knowledge of environmental requirements and hazards as related to facility/project design considerations.
 - (g) The FASS point of contact (POC) for the engineering activity is responsible for oversight and coordination of the SSPT activities.
- (2) Representatives from the appropriate civil works stakeholders should be included in the SSPT for civil works projects—
 - (a) Member of the activity that will occupy the project must have a detailed knowledge of the mission and function of the project and of specific hazards introduced by the work activities to take place within the structure and the impacts of the structure to/from adjacent activities.
 - (b) A representative from the requesting agency and the USACE for a civil funded facility/project.
 - (c) Applicable state, local and federal entities and/or other stakeholders.
 - (d) A fire protection engineer or specialist brings detailed knowledge of fire hazards, fire prevention measures, and fire protection requirements.
 - (e) An environmental engineer or specialist brings knowledge of environmental requirements and hazards as related to facility/project design considerations.
- (3) Appropriate stakeholders should make up the SSPT for other projects (for example, environmental, Superfund, Base Realignment and Closure (BRAC), Formerly Used Defense Sites (FUDS), and so forth).

b. Preparation of a preliminary hazard list. The SSPT will initially prepare or oversee the preparation of a preliminary hazard list. (PHL). The PHL a high level document upon which the system safety effort is based. As such, it must be completed in time to influence planning, design and funding documents. The PHL is used to initially

identify hazards to be controlled, uncertainties to be resolved, and other safety, health and fire protection concerns of the user that will require special attention in the design process. A well prepared and documented PHL helps to ensure design and construction of a facility acceptable to the user. The PHL is included as part of the DD Form 1391 (FY _____ Military Construction Project Data) funding documents. By requiring the PHL to accompany the funding documentation, funding for system safety tasks becomes an integral part of the budget process. If the scope of the system safety effort is to be extensive, funding for this effort will be obtained as part of the design/construction funds. The initial PHL will generate a list of safety-critical areas. Areas that need special safety emphasis (for example, hazard analysis) will be identified. Also, special requirements can be written into the detailed functional requirements to address these areas. This input may be in the form of specific design features that the facility must include or it may be requirements for hazard analyses to be performed as part of the design process. Once included in the design contract, safety is integrated into the design of a facility starting with concept design.

c. Facility risk categorization. After completion of an initial PHL, the SSPT's next action is the categorization of the facility into one of the three general risk categories. This categorization is based on several factors such as number of people exposed, type and degree of hazard of operation, criticality of the facility to defense readiness, and cost. This designation should be a direct reflection of the working group's concern regarding operational safety and health risks presented by the facility and its mission. The three general risk categories and typical system safety level of effort are listed below:

(1) "*Low*" risk facilities – examples: housing, warehouses, and administrative buildings. In these kinds of facilities, risks to building occupants are low and limited to those normally associated with everyday life. Accident experience with similar structures is acceptable and no additional hazards (for example, flammable liquids, toxic materials, and so forth) are to be introduced by the building occupant. Except in special cases, no further hazard analysis will be required.

(2) "*Medium*" risk facilities – examples: maintenance facilities, heating plants, and laboratories. These kinds of facilities present industrial type hazards to the building occupants. Accidents are generally more frequent and potentially more severe. A preliminary hazard analysis will normally be required of the designer. More sophisticated hazard analyses are normally not required. The engineering organization will actively participate in design reviews.

(3) "*High*" risk facilities – examples: explosives plants, chemical agent facilities, and high energy facilities. The SSPT should be heavily involved in the planning and design of this category of facility since it usually contains unique hazards of which only the user of a facility will have detailed knowledge. Because of this, it will often be appropriate for the user to specify preparation of additional special purpose system safety tasks during facility design. MIL-STD-882 should be used to identify the additional efforts required. The user will take an active role in the design review process.

d. Facility system safety cost estimation. For medium or high risk facilities where additional analyses are anticipated, include the analysis cost in estimates of overall project cost. Funding data for FASS efforts will be included in the DD Form 1391 package.

e. Provide data regarding facility intended use. Include in planning documents hazard data regarding development or procurement of any equipment intended to be installed, utilized or housed within the facility. Since the design and the construction of facilities often precedes the design and the manufacture of specialized equipment to be used in the facility, it is important to ensure that the facility can accommodate the equipment without compromising the safety or requiring modification of the facility. This is accomplished by defining equipment needs early in the planning process. The equipment needs criteria can include information such as dimensions, power requirements, weight, access requirements, clearance requirements, definitions of energy outputs (for example, noise, heat, fumes, and so forth.), energy shielding requirements and environmental requirements. Provide the engineering organization with updated information as necessary for use in facility design.

f. Project design review. The SSPT should participate in the design review process, reviewing and commenting on specification, design drawings and designer prepared hazard analyses.

g. Interface with lessons learned database. Where facility hazards are identified after occupancy, provide appropriate lessons learned data to the project lessons learned database.

6-4. Engineering organization responsibilities

a. Assist the user. Often, a user will request that the engineering organization assist in the development of facility planning documentation. The engineering organization's roles in assisting the user develop initial system safety planning documents (for example, PHL) should be limited to that of a facilitator. The active participation of the user community is critical to the process and the users intimate knowledge of the facility utilization is essential to the development of design planning documents.

b. Review user prepared system safety documentation. Conduct a thorough review of the user prepared PHL and any other safety data contained within the planning documents. Request clarification as necessary.

c. Prepare project System Safety Management Plan. This is a plan tailored to the specific project which establishes management policies and responsibilities for execution of the design system safety effort. It is based upon the PHL and

associated recommendations from the user regarding risk and design safety analysis needs. The following are the minimum elements of the SSMP:

(1) Designation of the engineering organization point of contact for system safety issues. This point of contact will be a military, civilian or contractor in an engineering series with training in system safety as defined in MIL-STD-882. The system safety POC will have oversight responsibility of the activity's system safety effort and report as appropriate within their organizational chain of command.

(2) Establish the project risk acceptance criteria based on consideration of the users recommendations. The acceptable level of risk in a facility is an expression of the severity and frequency of a mishap type that the using organization is willing to accept during the operational life of the facility. This is a function of the mission. For instance, the goal is to identify all hazards and to eliminate those exceeding the defined level of acceptable risk. While this is not always possible, the analysis conducted will provide the information upon which to base risk acceptance decisions.

(3) A specific listing of all tasks including hazard analyses which are a part of the design system safety effort. Designate the responsible parties or organizations for each task. The responsible parties for each task will be well qualified to perform the task as identified in MIL-STD-882. Optional tasks should be designated as such, listing conditions which would trigger these tasks.

(4) Establish the system safety milestone schedule, bearing in mind that the purpose of the hazard analysis is to beneficially impact design and that timely completion of the analysis is vital. The schedule for analysis completion must complement the overall design effort.

(5) State any special rules for government (engineering organization and user installation) and contractor interaction regarding the system safety effort.

(6) Establish procedures for hazard tracking and documenting residual risk and risk acceptance decisions. Hazard tracking systems are used in the FASS program in lieu of the SAR. The PHL should be used to create the initial list of hazards in the hazard tracking log. Initially, all hazards will remain open. New hazards identified throughout the design process are entered into the log. As the design progresses, corrective actions are included and hazards are eliminated or controlled. The statuses of these hazards are updated in the hazard tracking log. Hazards should be tracked throughout the facility life cycle. The hazard tracking log should be provided to the user when the facility is turned over for operation. Hazards should continue to be tracked by the user during the life of the facility. In many cases, these hazards will rely upon administrative controls such as SOP, limiting conditions of operation (LCO), and so forth.

(7) Identify method for incorporating lessons learned into the system safety effort. Outline procedures for documenting and submitting significant safety data as lessons learned.

(8) Establish procedures for evaluating proposed design changes for safety impact during the later stages of design after safety analysis is complete, or as a result of value engineering proposals, engineering change proposals, and so forth.

(9) Where equipment to be installed or utilized within the facility is being developed or procured separate from the facility design, establish a communication system that will provide timely equipment safety data to the designer. Of course, the SSMP must give consideration to overall project time constraints, manpower availability, and monetary resources. For example, the degree of system safety effort expended will depend on whether the project is replacing an existing facility, creating a new facility, involves new technology or is based on standard designs. The options for hazard analyses are many, and PMs will need to specify the design system safety tasks tailored to facilities acquisition in the SSMP.

d. Incorporate system safety requirements in contract documents. These requirements are structured from the project tailored SSMP. To provide an understanding of potential contractors system safety capabilities, candidate contractors will be requested to provide their proposed approach to the system safety requirements in their written or oral presentations to government contractor selection boards. Consider including the requirement for a system safety program plan (SSPP) in the statement of work. See paragraph 7-4 for the key elements of a SSPP.

e. Review and accept design hazard analyses submitted by the design/systems contractor. Assure the quality of the analyses required by the SSMP and the SSPP through a submittal review process.

f. Engineering change proposal analysis. Review each engineering change proposal for potential impact on project safety and verify that such impact is minimized by appropriate design measures.

g. Document risk acceptance decisions. In accordance with the SSMP, track hazard resolution and obtain and document residual risk acceptance decisions.

h. Construction quality assurance. During the construction phase, assure that design safety features are properly installed or constructed. Review any engineering changes after final design to minimize impact on FASS.

6-5. Design agent functions

a. Complete all system safety tasks as required by the SSMP and SSPP and/or contract documents. Utilize the output from hazard analysis as input to the design, developing, evaluating, and implementing appropriate hazard controls.

b. Review engineering change proposals before forwarding to the engineering organization for impact on facility system safety.

- c. Document residual hazards and initiate action to obtain risk acceptance decisions, as required.

6–6. Standard designs

- a. Facility system safety is an integral part of a standard design. Each standard design will include a set of standard FASS documents prepared using the requirements contained in this chapter.
- b. The effort required to complete the FASS program for a standard design should not be duplicated for each application of the design. Local analysis of the design application will be performed to identify specific hazards associated with the impact of the structure to/from its intended siting (for example, utilities, activities, adjacent structures, and so forth).
- c. For each application of the standard design, deviations from the standard design will be analyzed to identify any new hazards or increased risk introduced in the facility. This effort should be performed by the engineering organization responsible for the standard design and included with the standard FASS package for the design application.
- d. Standard designs will have a HTS, to include hazards associated with deviations from the standard design. Each standard design will include a lessons learned database. Any HTS or lessons learned database will be available to the users of the standard design.

6–7. Self-help projects

- a. Self-help projects consist of work that can be performed using Army training, materials, equipment, and supervision. These projects include minor maintenance (for example, painting a room), improvements (for example, landscaping and fencing), and troop sponsored projects (for example, renovation of barracks.)
- b. Self-help projects, if not properly managed, can increase the risk to a facility/project and/or personnel. For example, failure to use the appropriate fire retardant building materials or the construction of a wall in the hallway of a barracks building increases the risk of fire and injuries to personnel in the event of a fire
- c. Safety and occupational health personnel should provide input to the system safety POC at the engineering activity for the establishment of strict policies and procedures for the authorization and performance of self-help projects. These policies and procedures should address, as a minimum, scope of work/projects authorized to be performed, development of project proposals, selection and requisition of supplies and materials, training in use of equipment and procedures, supervision, and inspection/quality assurance.

6–8. Construction facility system safety

- a. *Safety features.* During the construction phase, two activities involving FASS will take place. Change orders will be reviewed to ensure changes do not degrade safety features already incorporated in the design. This is an area that will take considerable effort as configuration control has historically been poor in facility construction. Also, arrangement with the engineering organization may be made for site visits to check on the progress of the facility.
- b. *Occupancy inspection.* This inspection should take place immediately before the user takes over control of the facility. This inspection will verify the presence of critical safety features incorporated into the design. At this point, the HTS is important: Review of the tracking system will identify safety features that should be looked at during the inspection. The hazard tracking log should be used to generate a checklist for safety items that should be a part of the inspection.

6–9. Facility/project operation and maintenance

- a. *Procedure development.* After a facility/project design is completed, risks have been controlled and/or accepted, and the construction phase has begun, it is time to begin the process of developing facility/project operating, maintenance, and emergency procedures. The output of the design system safety effort should be used as the point of departure for procedure development. The primary focus should be on residual risks and assuring that critical safety features of the structure are included in maintenance plans. Plans to deal with natural and man made emergencies must also be developed at this time. In addition, necessary training programs for instructing building occupants in the use of these procedures and plans should commence.
- b. *Change analysis.* After building occupancy, any proposed building mission changes must be analyzed to detect changes that could introduce a new hazard or change the attributes or nature of an existing hazard or hazard control. A determination must be made of whether new mission tasks can be safely performed in the facility/project as originally designed and to identify any modifications necessary to insure the safety and occupational health of building occupants.
- c. *Facility/project/site maintenance and repairs.* Maintenance and repair of existing facilities or sites must comply with applicable standards and procedures. Maintenance is the work required to preserve and maintain a facility/project or site in such condition that it may be effectively used for its designated functional purpose. Maintenance includes cyclic work done to prevent damage, or work performed to sustain components. Repair is work performed to restore a project or facility. Repair may be overhaul, reprocessing, or replacement of deteriorated component parts or materials. All new work performed as repairs must meet new construction standards.

Chapter 7 Facility System Safety Program Contracting

7-1. General

The level of system safety effort for each program is tailored to ensure implementation of a cost-effective program based on the level of risk involved.

7-2. Contractor selection

To help develop an understanding of the potential contractors system safety capabilities and experience, candidate design contractors will be required to include their proposed approach to system safety requirements as extracted from the initial SSPP in their written and/or oral presentations to government contractor selection boards. Elements addressed will include the following:

- a. Qualifications of personnel to perform tasks.
- b. The procedures by which the contractor will integrate and coordinate system safety considerations into the design effort.
- c. The process through which contractor management decisions will be made, including timely notification of unacceptable risks, changes impacting safety, program deviations, and so forth.

7-3. Task selection

Commensurate with the SSMP, additional system safety tasks may be required of the design contractor. Tasks should be selected in accordance with the requirements contained in MIL-STD-882.

7-4. System Safety Program Plan

a. *General.* The purpose of the Facility SSPP is to bring together in one document the design agents plan for conducting the system safety program for a specific project from the concept design phase to the acceptance of the completed facility. Based on the FASS tailoring concept, the plan describes in detail how each applicable element of FASS is to be implemented.

b. *Program plan prerequisites.* The designer will require certain documents to write the facility SSPP. These documents include the following:

- (1) The PHL.
- (2) The contract documents.
- (3) The list of FASS tasks required.
- (4) The SOW.

c. *Timing of delivery.* Because the program plan is used to document the designers' plan for the system safety tasks required in the SOW, an initial SSPP must be completed for inclusion in the bid proposal. An update to the SSPP may be provided if required early in the design phase to allow for review, redrafting, and final approval without affecting the timeliness of safety input into the project.

d. *Team review.* Because the facility SSPP is used to describe the designers plan for meeting the system safety requirements specified in the contract, the engineering organization must review and accept the SSPP, ensuring a system safety approach consistent with contract specifications.

e. *Facility system safety program plan.* Each facility SSPP, regardless of level of system safety effort involved in the project, will address each area listed below. An approach will be provided for each area by the designer, or provide rationale as to why the area is not applicable, and will describe in detail the proposed approach to the requirement, the content, and format of the deliverables, and indicate the level of effort for each area. Each facility SSPP will be an individually tailored approach based on the contract-specified requirements, the anticipated hazards identified in the PHL, and the level of risk involved with the facility in question.

(1) *Program scope and objectives.* This section must describe the scope of the overall FASS project, the objectives and supporting tasks and activities of system safety management and engineering, and the interrelationships between FASS and other functional elements of the overall facility design, addressing as a minimum the four elements of an effective FASS program:

- (a) A defined set of objectives and supporting tasks.
- (b) A planned approach for objective/task accomplishment.
- (c) Qualifications of system safety personnel.
- (d) Authority to implement the system safety program through all levels of management.

(2) *System safety organization.* The program plan will describe:

- (a) The designers organization or functional alignment for accomplishing the system safety portion of the program.
- (b) The responsibility and authority of the designers system safety personnel, other contractor organizational elements involved in the FASS effort, and subcontractors. The program will identify the organizational unit responsible

for executing each task and the line of authority for the resolution of all identified hazards. The plan will also include the name, address, and telephone number of the individual responsible for system safety input.

(c) The staffing of the system safety effort for the duration of the contract, including manpower loading, control of resources, and the qualifications of key system safety personnel assigned.

(d) The procedures by which the designer will direct the FASS efforts, including assignment of FASS requirements to action organization and subcontractors, coordination of subcontractor system safety programs, integration of hazard analyses, program and design reviews, and program status reporting.

(e) The process through which management decisions will be made, including timely notification of unacceptable risks, changes to FASS or other safety and occupational health requirements, program deviations, and so forth.

(3) *System Safety Program Milestones.* The program plan will—

(a) Identify the system safety program milestones, including delivery dates as specified in the contract.

(b) Provide a program schedule of FASS tasks, including start and completion dates, reports, reviews, and estimated manpower loading in the scope of the overall program.

(c) In order to preclude duplication, identify integrated system activities (for example, design analyses, tests and demonstrations) applicable to the FASS program but specified in other facility engineering studies. This includes any required studies of user equipment to be installed in the facility.

(4) *General system safety requirements and criteria.* The program plan will describe—

(a) The general engineering requirements and design criteria for FASS, including FASS requirements for all appropriate phases for the life cycle up to and including disposal.

(b) The designers procedures to comply with the required FASS risk assessment, hazard control development/evaluation, and risk acceptance requirements. Also, any quantitative measures of safety to be used for risk assessment must be described and any system safety definitions used must be included.

(c) The procedures for addressing identified hazards, including those involving Government-provided equipment (GPE) and off-the-shelf equipment.

(5) *Hazard analyses.* The program plan will describe—

(a) The analyses needed to meet specified requirements.

(b) The degree to which each technique will be applied, including hazard identification associated with the facility, facility systems, subsystems, components, personnel, requirements and GPE.

(c) The integration of the overall system hazard analyses.

(d) Efforts to identify and control hazards associated with the facility during the facility's life cycle.

(e) The boundaries and key assumptions for hazard analyses and the limits of the analyses. These typically include hostile intentions, basic structural integrity, areas sufficiently covered by applicable codes and standards, and so forth. The analysis will have a limit of resolution. The limit is dependent on the facility and details of the hazard.

(6) *System safety data.* The program plan will—

(a) Describe the specific approach for researching, distributing, and analyzing pertinent historical hazard or mishap data, including lessons learned.

(b) Identify deliverable data.

(c) Identify non-deliverable system safety data and describe the procedures for accessibility and retention of data with historical value (lessons learned).

(7) *Safety verification.* The program plan will describe—

(a) The verification (test, analysis, inspection, and so forth) requirement for making sure that safety is adequately demonstrated. The plan will identify and certification requirements for safety devices or other special safety features.

(b) A procedure for making sure any safety information is transmitted for review and analysis.

(8) *Audit Program.* The program plan will describe the procedures to be employed by the contractor to make sure the objectives and requirements of the system safety program are being accomplished.

Appendix A References

Section I Required Publications

AR 70-1

Army Acquisition Policy (Cited in paras 3-5, 3-8, 4-9a.)

AR 385-10

The Army Safety Program (Cited in paras 1-1, 2-5e(2), app C.)

AR 602-1

Human Factors Engineering Program (Cited in paras 2-13b(3), 3-6a.)

AR 602-2

Manpower and Personnel Integration (Cited in paras 2-14b(5), 3-8c.)

MIL-STD-882

System Safety (MANPRINT) in the System Acquisition Process (Cited in paras 2-4, 2-5, 2-18, 6-3, 6-4, 7-3, and apps G, H, and I.) (Available at [//assist.daps.dla.mil/quicksearch/](http://assist.daps.dla.mil/quicksearch/))

Section II Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication. Military Standards, data items (DIs), and other publications are available at [//assist.daps.dla.mil/quicksearch/](http://assist.daps.dla.mil/quicksearch/).

AR 25-1

Army Knowledge Management and Information Technology

AR 25-55

The Department of the Army Freedom of Information Act Program

AR 40-5

Preventive Medicine

AR 40-10

Health Hazard Assessment Program in Support of the Army Acquisition Process

AR 71-9

Materiel Requirements

AR 73-1

Test and Evaluation Policy

AR 75-1

Malfunctions Involving Ammunition and Explosives

AR 95-1

Flight Regulations

AR 200-1

Environmental Protection and Enhancement

AR 385-63

Range Safety

AR 420-1

Army Facilities Management

AR 672-20

Incentive Awards

AR 700-127

Integrated Logistic Support

AR 750-6

Army Equipment Safety and Maintenance Notification System

DA Pam 385-1

Small Unit Safety Officer/NCO Guide

DA Pam 385-40

Army Accident Investigation and Reporting

DA Pam 750-8

The Army Maintenance Management System (TAMMS) Users Manual

DA Pam 738-751

Functional Users Manual for the Army Maintenance Management System-Aviation

FM 3-0

Operations

29 CFR 1910.119

Process Safety Management of Highly Hazardous Chemicals (Available at <http://www.osha.gov>.)

32 CFR 651

Environmental Analysis of Army Actions (Available at <http://www.gpoaccess.gov/cfr/index.html>.)

DI-ILSS-81495

Failure Modes, Effects, and Criticality Analysis Report

DI-MNTY-81600

Maintainability Program Plan

DI-QCIC-81722

Reliability Program Plan

DI-R-1730

Reliability Program Plan

DI-SAFT-80101B

System Safety Hazard Analysis Report (SSHA)

DI-SAFT-80102B

Safety Assessment Report (SAR)

DI-SAFT-80103A

Engineering Change Proposal System Safety Report

DI-SAFT-81626

System Safety Program Plan (SSPP)

DI-TMSS-81586A

Reliability Test Reports

DODD 5000.1

The Defense Acquisition System (Available at <http://www.dtic.mil/whs/directives/>)

DODI 5000.2

Operation of the Defense Acquisition System (Available at <http://www.dtic.mil/whs/directives/>)

DODI 6050.5

DOD Hazard Communication (HAZCOM) Program (Available at <http://www.dtic.mil/whs/directives/>)

EM 385-1-1

Safety and Health Requirements

MIL-HDBK-470A

Designing and Developing Maintainable Products and Systems, Vol. 1

MIL-STD-1472

Human Engineering

MIL-STD-1474

Noise Limits

MIL-STD-1522

Standard General Requirements for Safe Design and Operation of Pressurized Missile and Space Systems

Section III**Prescribed Forms**

This section contains no entries.

Section IV**Referenced Forms****DA Form 2397R-series**

Technical Report of U.S. Army Aircraft Accident

DA Form 2407

Maintenance Request

DA Form 2696

Operational Hazard Report

DA Form 3701-R

Product Improvement Management Information Report (PRIMIR)

DA Form 4755

Employee Report of Alleged Unsafe or Unhealthful Working Conditions

DD Form 1391

Military Construction Project Data

DD Form 1423

Contract Data Requirements List

SF 368

Product Quality Deficiency Report

Appendix B Preparation Guidance for a System Safety Working Group Charter

B-1. Purpose

Briefly describe the SSWG's purpose.

B-2. Scope

Describe the scope of the SSWG's activities.

B-3. Authorizations

The SSWG gains its authority through the PM by virtue of the program charter.

B-4. References

References will contain publications to be used in the charter.

B-5. Tasks

a. List the major tasks the SSWG should perform. These tasks will be broad in scope. Although the activities depicted in figures 2-5 through 2-8 are neither sequential nor complete, they can be used as a check against omission of important tasks.

b. Every charter will contain a task to develop a SSMP. The SSMP must contain the specific tasks necessary to accomplish the broad ones listed in the charter.

B-6. Operation

a. Membership. Membership should be divided into principal and advisory members. Membership is confined to organizations rather than individuals. Principal members must attend every meeting of the SSWG and advisory members only when required, see paragraph B-8.

b. Meetings. Frequency of meetings and composition of SSWG must be described.

c. Administration.

(1) Describe procedure for developing agendas, preparing minutes, and making formal recommendations to the PM.

(2) Forward minority opinions as well as consensus to the PM.

(3) Ensure provisions are made for updating the charter.

B-7. Term

Specify the period of time for which the SSWG is chartered.

B-8. Example of a System Safety Working Group Charter

a. Below is an example of a system safety working group charter:

(1) *Purpose.* To establish a technically qualified advisory group for the (system name) PM for system safety management as a means to enhance the design and safe operation effectiveness of the (system name).

(2) *Scope.* The (system name) SSWG will function as an element of program management to monitor the accomplishment of system safety tasks including—

(a) Validation of system safety tasks.

(b) Identification of system safety requirements to include crashworthiness and crash safety.

(c) Organizing and controlling those interfacing Government efforts that are directed toward the elimination or control of system hazards.

(d) Coordinating with other program elements.

(e) Analyzing and evaluating the contractor's system safety program to provide timely and effective recommendations for improving program effectiveness.

(3) *Authorizations.* Program charter, (system name), ACOMs/ASCC/DRUs.

(4) *References.* MIL-STD-882.

(5) *Tasks.* The (system name) SSWG will be responsible to the (system name) PM for the following:

(a) Review of (system name) requirements documents such as CDD and letters of agreement.

(b) Review and evaluation of the BTA.

(c) Recommendations to the (system name) PM for establishing new or revised requirement(s) based on existing system safety regulations.

(d) Response to requests from the (system name) PM for recommendations on program matters potentially influencing system safety.

(e) Coordination with other elements of the (system name) PM's office to identify and evaluate those areas in which safety implications exist.

- (f) Review of the (system name) RFP.
 - (g) Development of Source Selection Evaluation Board (SSEB) selection criteria for system safety.
 - (h) Evaluation of contractor proposals for system safety, to include crashworthiness.
 - (i) Development of a HTS to identify, eliminate if possible, rank, estimate a likelihood of occurrence, and track hazards throughout the life cycle of the system. Recommendation for corrective action will be provided to the (system name) PM, as appropriate.
 - (j) Development of an SSMP.
 - (k) Review and evaluation of the contractor's SSPP.
 - (l) Assistance to the (system name) PM during safety system safety analyses reviews at the contractor's facility. Comments or recommendations for corrective action should be provided to the (system name) PM as appropriate.
 - (m) Development of a PHL.
 - (n) Collection and evaluation of lessons learned pertaining to (system name) system safety.
- (6) *Operation.*
- (a) Membership.
 1. The principal voting members to be appointed from the MATDEV's organizations are—
 - a. (System name) PM's office.
 - b. Local safety office (LCMC Matrix Support).
 - c. Engineering representative.
 - d. CBTDEV safety representative.
 - e. MANPRINT representative.
 - f. Installation safety manager, if applicable.
 - g. Prime contractor's system safety manager, if appropriate.
 2. Advisory members will be appointed from the following organizations:
 - a. ACOMs/ASCCs/DRUs safety offices (LCMC, CBTDEV, and/or user).
 - b. User test organization.
 - c. Representatives from ACOMs/ASCCs/DRUs developing subsystems.
 - d. Technical test organization.
 - e. Developmental independent evaluator.
 - f. Operational independent evaluator.
 - g. ARLHRED.
 - h. DA observer (CRC).
 - i. Other organizations as required.
 3. Advisory members will be invited to attend meetings on an as-required basis when their expertise, opinions, or comments are required or solicited.
 4. The DA observer will be a representative from the CRC. The observer's responsibility will be to monitor the conduct of the SSWG by attending meetings. Any technical safety input will be provided to the SSWG through its chairman.
 5. Chairmanship is vested jointly in the (system name) PM's office member and the local safety office member.
 6. Changes in membership will be as required to fulfill the purpose of the (system name) SSWG. Such changes will be subject to approval of the chairmanship.
 - (b) Meetings of the (system name) SSWG will be held before safety reviews and at other times when required by the PM. Principal members will attend all meetings. Advisory members will attend meetings at the invitation of the chairmanship when their specialized expertise is required.
 - (c) Administration.
 1. The SSWG chairmen will establish the agenda for scheduled meetings no later than two (2) weeks prior to the meeting.
 2. Proposed agenda items may be submitted by any member of the SSWG.
 3. Minutes will be prepared for each meeting. A summary of action items, action agencies, and suspense dates will be prepared before the end of the meeting. Formal minutes of each meeting will be prepared and distributed by the PM's office.
 4. The SSWG does not have the authority to accept risks associated with identified hazards. All hazards identified by any source will be entered in the HTS and recommendations for their elimination or mitigation will be provided through the PM to the appropriate decision authority.
 5. SSWG recommendations to the PM will include any minority opinions.
 6. All items from previous meetings will be reviewed to determine that the action is closed or adequate progress is being made.
 7. Accident or incident experience will be reviewed at each meeting to identify trends and to monitor and evaluate the corrective actions taken.

8. Implementation of the provisions of this charter will be governed by the SSMP developed by the SSWG and approved by the PM.

9. This charter and the SSMP will be reviewed at least annually and updated or modified as required.

(7) *Term.* The (system name) SSWG will function during the life of the PM's office.

b. See paragraphs B-1 through B-7 for additional guidance.

Appendix C

System Safety Management Plan

C-1. General program requirements

a. Purpose.

b. References.

c. Scope.

d. Objectives. The objective of the system safety program, found in the SSWG charter, should be listed.

C-2. System safety organization

a. PMO.

b. Life Cycle Management Command Matrix Support Safety Office.

c. Integration of associated disciplines.

C-3. Tasks

The specific tasks to accomplish the objectives in paragraph C-8d, should be listed with the responsible action agency. The activities depicted in figures 2-5 through 2-8 can be tailored for use in the SSMP. It can also be used as a check against omission of important tasks.

C-4. Milestones

A milestone schedule that parallels the overall program schedule will be established. Specific start and completion dates should be developed for the activities/tasks above in paragraph C-3.

C-5. Mishap risk management

Procedures for hazard identification, categorization, tracking, and elimination must be discussed. The decision authority for action or inaction on a hazard and for acceptance of residual risk should be defined for this program. The decision authority matrix should be incorporated (see chap 2, sec I).

C-6. Administration

Administrative details not covered in the SSWG charter should be discussed in this section. Typical items include the details of the HTS and procedures for distribution of deliverable data from the contractor.

C-7. Resources

a. *Budget.* Specific budgets will be prepared annually. This section will cite funds available from the PM's office for accomplishment of the system safety program. It should also project future funding requirements to aid in preparation of annual budget requests.

b. *Manpower.* Manpower resources available to the PM to accomplish the system safety program objectives will be described.

c. *Authority.* The authority for implementation of the SSMP comes from the PM. Specific actions (For example, taskings, and so forth) will be conducted with the PM's approval.

Note. The sample SSMP in paragraph C-8 amplifies the preparation guidance provided in this appendix. It has been prepared for a generic major system and must be tailored before use as organizations and responsibilities will be different for each program.

C-8. Sample system safety management plan

General program requirements:

a. *Purpose.* This plan establishes management policies, objectives, and responsibilities for execution of a system safety program for the life cycle of (system name) system.

b. *References.*

(1) MIL-STD-882 and Issue D (Standard Practice for System Safety).

(2) Program charter, (system name), ACOM/ASCC/DRU.

c. *Scope.* This plan establishes ground rules for Government and contractor interaction with respect to system safety. It applies to the (system name) SSWG, functional areas within the ACOM supporting the (system name) program,

(system name) PMO, and (system name) contractors. The plan establishes the methodology by which the (system name) PM may oversee and evaluate the execution of contractor SSPPs.

d. Objectives.

(1) Assure all hazards associated with the (system name) system are identified and formally tracked and that risks associated with those hazards are properly managed.

(2) No hazard is accepted without formal documentation of associated risks.

(3) Historical safety data (lessons learned) is included in the (system name) system safety program.

(4) Safety consistent with mission requirements is included in the (system name) system safety program.

(5) Risk acceptance decisions are documented.

(6) Retrofit actions required to improve safety are minimized through the timely inclusion of safety features early in the life cycle of the (system name).

(7) Changes in design, configuration, or mission requirements are accomplished in a manner that maintains risk level acceptable to the decision authority.

(8) Significant safety data is documented as "lessons learned" and will be submitted to appropriate data banks (see para 2-14e) or as proposed changes to applicable design handbooks and specifications.

(9) Consideration is given in system design, production, and fielding to safety, ease of disposal, and demilitarization of any hazardous materials.

e. System safety organization integration of associated disciplines. The SSWG is the focal point for integration of other design and testing disciplines. The chairman of the SSWG will develop lines of communication and information exchange with the following:

(1) The (system name) MJWG and TIWG.

(2) ARLHRED and AEC to integrate the HFEA and the HHA into the (system name) system safety program.

(3) ATEC to obtain results of operational evaluations of the (system name) system and to ensure incorporation of key safety issues into the TEAM plan.

(4) Environmental considerations.

f. Tasks.

(1) *The PM will—*

(a) Charter and guide an SSWG.

(b) Designate the program system safety manager.

(c) Establish decision authority levels for the acceptance of residual risk associated with system hazards.

(d) Establish ground rules for Government and contractor interaction. Assure contracts stipulate these rules. Assure a SSWG representative attends appropriate (system name) system reviews (For example, mock-up reviews, preliminary design reviews, critical design reviews, and pre-first-flight reviews).

(e) Assign budget and manpower resources to accomplish system safety management tasks. (para C-7.)

(f) Establish and update system safety milestone schedule (see para C-4).

(g) Identify risk for residual hazards and provide recommendations of risk acceptance or resolution at each milestone review.

(h) Establish procedures for evaluation of product improvements for safety impact.

(i) Integrate hazards and safety issues identified by associated disciplines and input data into HTS.

(j) Prepare system safety risk assessment for each hazard. The SSRA will be sent to the CBTDEV for review no later than 60 days before each decision authority review. A copy of each SSRA requiring ASARC review will be forwarded to the CRC.

(k) Assure that adequate SSEB safety criteria are established to evaluate the contractor's proposals and Saps.

(l) Establish and maintain documentation of all risk acceptance decisions.

(m) Request a Health Hazard Assessment Report (HHAR) from The Surgeon General (TSG) (per AR 40-10) and provide to the DTC 60 days prior to the start of all testing.

(n) Sixty days prior to fielding, provide the gaining commands with all relevant system safety documentation developed during the acquisition process which provides supporting rationale for operational procedures, safety-critical maintenance and other support actions, and unit-level training requirements. As a minimum, these documents will include updated SARs, SSRAs, Hazard Classification Data, and Range Surface Danger Zones. As system fielding is expanded to other commands, update the system safety documentation with lessons learned by initial users. Provide hazard analyses and SSRAs to the combat developer as they are developed.

(2) *Local safety office.*

(a) Coordinate development of computerized HTS. System will be operational no later than (date or program milestone).

(b) Coordinate with test agencies to assure that system safety issues identified by the SSWG are included in test plans. As a minimum, have safety representation at the (system name) TIWG meetings to accomplish this task.

(c) Act as executive manager/agent for system safety for the PEO/PM/MATDEV.

- (d) Review procurement documentation for compliance with DOD and U.S. Army system safety policy.
- (e) Establish and maintain a system safety lessons-learned file for the (system name) system. Submit lessons learned on an annual basis (September) to CRC and DTIC throughout the system's life cycle. Make recommendations, as appropriate, for changes to military specifications and standards.
- (f) Review and comment on system safety portions of the (system name) request for proposal.
- (3) *PEO/PM/MATDEV/Life Cycle Management Command organizations.*
 - (a) Engineering. Provide description of hazards identified during development, production, and fielding to the SSWG. Include recommendations for controlling or eliminating the hazard.
 - (b) Product assurance. Provide description of hazards identified during development, production, and fielding to the SSWG. Include recommendations for controlling or eliminating the hazard.

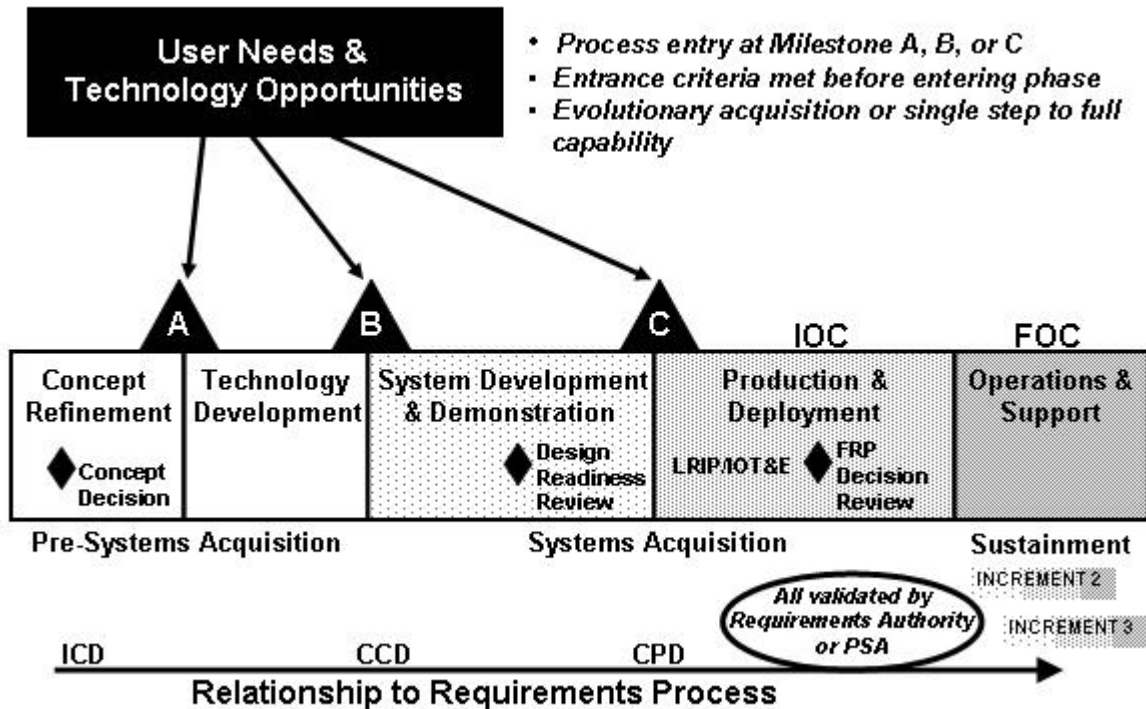


Figure C-1. Milestones

g. *Milestones.*

h. *Mishap risk management.*

(1) *Risk assessment.* The risk associated with a hazard is a function of its probability and severity. Therefore, all hazards will be evaluated by the SSWG to determine or verify probability and severity. (Specific definitions of these terms are in MIL-STD-882.) The matrix in table 2-1 and 2-2 will be used to assign a RAC to the hazard.

(2) *Risk resolution.*

(a) Once a hazard has been identified and a RAC assigned, the SSWG will identify the potential action(s)/methods of eliminating or controlling a hazard and the expected effectiveness of each option. Based on the RAC, not all hazards are severe enough or occur often enough to warrant the expenditures required to eliminate or control them. Regardless, the hazard will be tracked in the HTS. The SSWG will submit a written report to the PM stating risk assessment results and hazard control recommendations

1. Within 14 calendar days after each SSWG meeting.

2. Immediately when a high risk hazard is identified.

(b) The PM will comment in writing on the recommendations submitted by the SSWG. These comments will

constitute the basis upon which hazard resolution actions are to be taken and will serve as initial documentation for risk acceptance decisions. The risk decision matrix defines the command level to which each hazard must be reported and the decision authority for accepting the risk associated with each hazard.

(c) The consequences of risk acceptance of the proposed configuration and alternative actions will be expressed using projected costs due to deaths, injuries, and equipment damage. Information concerning application and projected costs will be obtained from the contractor by the SSWG. The SSWG will calculate personnel death and injury costs using AR 385-40, table D-1. The decision to accept the risk will also consider other factors such as impact on schedule and operational effectiveness. The CBTDEV will provide a recommendation as to which corrective measure will be taken and the impact of other alternative corrective measures.

(3) *Hazard tracking.*

(a) A HTS will be established jointly by the local safety office and the (system name) PM using the format in table 2-3.

(b) The status of a hazard will be listed as "closed" only if written approval from the appropriate decision authority has been given for acceptance of the residual risk. The hazard will be monitored even if closed so that accident data can be compared to the accepted RACs, to the projected deaths and injuries, or to the projected costs. The (system name) accident experience will be periodically compared to the projections to determine whether or not previous mishap risk management decisions should be reevaluated and other corrective measures proposed.

(4) *Preparation for ASARC.* The PM is responsible for preparation and presentation of an SSRA for each hazard that requires ASARC-level decision authority. The format guidance found in this document will be used for the SSRA. The HTL of the SSWG and the SAR by the contractor will be used to identify the appropriate hazards.

i. Administration. The PM's representative to the SSWG will accomplish the following:

(1) Prepare minutes for each SSWG meeting and distribute a copy of minutes to each SSWG principal member within 14 calendar days. The contractor will be responsible for preparing and distributing minutes of SSWG meetings held at contractor locations.

(2) Ensure distribution of contractor deliverable system safety documents to SSWG principal members within 14 calendar days of receipt by the PMO.

j. Resources. The PM is to maintain the following resource areas:

(1) Budget. To be established by PM.

(2) Manpower. To be established by PM.

(3) Authority. The (system name) PM is the authority for implementation of this plan. Taskings and requests for action to implement the system safety program will be forwarded to the PM for disposition.

Appendix D Preliminary Hazard List/Analysis

D-1. Definition

A PHL/PHA involves making a study during concept or early development of a system or facility to determine the hazards that could be present during operational use. The PHA should, as a minimum, identify the hazard, estimate its severity, provide the likelihood of occurrence, and recommend a means of control or correction. The PHL is only a list of the hazards. Resource constraints and data availability are the factors used to determine whether a PHL or a PHA would be appropriate. A PHL can be the basis for an analysis that becomes a PHA. A properly completed PHL/PHA has the following advantages:

a. Its results may help develop the guidelines and criteria to be followed in a system/facility design.

b. Since it indicates the principal hazards as they are known when the system is first conceived, it can be used to initiate actions for their elimination, minimization, and control almost from the start.

c. It can be used to designate management and technical responsibilities for safety tasks and be used as a checklist to ensure their accomplishment.

d. It can indicate the information that must be reviewed in codes, specifications, standards, and other documents governing precautions and safeguards to be taken for each hazard.

D-2. Basic elements

The PHL/PHA should include at least the following activities:

a. A review of pertinent historical safety experience and lessons learned databases. This involves discovering problems known through past experience on similar systems/facilities to determine whether they could also be present in the system or facility under development.

b. A categorized listing of basic energy sources.

c. An investigation of the various energy sources to determine provisions that have been developed for their control.

- d. Identification of the safety requirements and other regulations pertaining to personnel safety, environmental hazards, and toxic substances with which the system/facility will have to comply.
- e. Recommended corrective actions.

D-3. Sources of data

Obtain historical safety information from predecessor systems (see para 2-13c).

D-4. Preliminary hazard analysis chart

There are several formats that may be used when performing a PHA. See table D-1 for a sample format of a functional PHA.

Table D-1
Format of preliminary hazard analysis (typical)

Program:				
System:				
Part	Hazard	Cause	Hazard Effect	Corrective Category or Prevention Action

D-5. Instructions for completion of the preliminary hazard analysis

a. The following example outlines the procedure for completing a PHA. In this example, engine repair operations are a subsystem of a vehicle maintenance repair facility.

b. The first step in performing a PHA on this facility is to obtain all available information about the functional and operational requirements of the facility. This is also the time to obtain historical data on potential hazards at similar facilities from sources such as accident reports, equipment/operation maintenance logs, or inspection reports.

(1) *Facility.* The facility should then be broken down into subsystems or component operations. Once this is completed, the PHA chart may be completed.

(2) *Hazard.* Hazards are defined as conditions that are prerequisites to accidents; therefore, they have the potential for causing injury or damage. Hazards may be described as energy sources that generate this condition. For example, one hazard of engine repair operations in the vehicle repair facility would be carbon monoxide. Therefore, carbon monoxide is the energy source that generates the hazard. Proper hazard identification requires consideration of the following:

(a) Hazardous components that are energy sources such as fuels, propellants, lasers, explosives, toxic substances, hazardous construction materials, and pressure systems.

(b) Safety-related interface considerations among various elements of the system to include material compatibilities, electromagnetic interference, inadvertent activation, fire or explosion initiation, and hardware or software controls.

(c) Environmental constraints such as shock, vibration, extreme temperatures, noise, exposure to toxic substances, health hazards, fire, lightning, and radiation.

(d) Operating, test, maintenance, and emergency procedures such as HFE; human error analysis of operator functions, tasks, and requirements; effect of factors such as equipment layout, lighting requirements, potential exposures to toxic materials; effects of noise or radiation on human performance; life support requirements and their safety implications in manned systems; and crash safety, egress, rescue, survival, and salvage.

(e) Facilities and support equipment with appropriate training for proper use should be carefully examined. These could include provisions for storage, assembly, and testing hazardous systems and making sure personnel who will handle these systems or assemblies are properly trained.

(3) *Cause.* Cause factors are those items that create or significantly contribute to the existence of the hazard. In this case, failure to provide adequate exhaust ventilation is one potential cause factor. Another might be failure to control generation of carbon monoxide by running internal combustion engines or failure to provide work place monitoring to detect carbon monoxide levels.

(4) *Effect.* Potential effects are described in terms of the path or flow the energy takes between the source and the object that requires protection. The effect of personnel inhaling carbon monoxide, which enters the bloodstream and interferes with the delivery of oxygen to the tissues, can lead to death or serious injury.

(5) *Hazard category.* This is the assigned RAC, which is a determination of the hazard's severity and probability of occurrence. For this example, a RAC of 2A would be assigned based upon the high severity and probability factors associated with this hazard.

(6) *Corrective or preventive actions.* Recommendations on controlling the hazard should be prioritized by concentrating on the energy source first and then following points along the flow or path of the energy. In this way, last efforts are directed at the item or person requiring protection. This form of prioritizing might be reflected in the example by first recommending that internal combustion engines be replaced by electric motors, which remove the energy source (and hazard) altogether. Next, exhaust ventilation provided directly at the source through use of below-floor or overhead systems with hoses attached directly to vehicle exhausts could be installed to contain the energy source. Finally, carbon monoxide detection equipment could provide audio and visual alerting when carbon monoxide concentrations reach action level.

Appendix E System Safety Risk Assessment Preparation Guidance

E-1. Part I

- a. Item-system identification.
- b. Hazard topic.
- c. Hazard description and consequences of risk acceptance of the proposed configuration.
- d. Hazard classification (severity and probability according to MIL-STD-882).
- e. Source document reference.
- f. Alternative actions that could eliminate or control hazard level (include residual risk level for each action).

Note. The SSRA should be prepared as a stand-alone document.

E-2. Part II

The SSWG/safety manager recommendation regarding risk acceptance. (Include minority views and rationale.)

E-3. Part III

Recommendation by the CBTDEV.

E-4. Part IV

Recommendation by the LCMC.

E-5. Part V

Approval by the appropriate risk decision authority.

E-6. SSRA process

See figure 2-3 for the SSRA process.

Appendix F Safety Release Preparation Guidance

F-1. Purpose of this safety release

State the purpose of the safety release.

F-2. References

List appropriate references associated with the system.

F-3. System description

Give the name, type, model number, and mission of the system. If a component, name the parent system. State the specific test for which safety release is issued (for example, the number as it appears in the 5-year test program).

F-4. Requirements and background

- a. Requirements and procedures to conduct testing safely, including range safety fans (user test only).
- b. Background and testing (technical test only).
 - (1) If a SAR and HHA were provided for the system, it will be enclosed or referenced by the safety release, and if no SAR or HHA exists, so state.
 - (2) Summarize testing done or other basis, such as analyses or inspections, for safety release.
 - (3) State the results of testing, safety problems, and significant incidents.

(4) Define or enclose development data to assist in preparing range safety plans, requirements, and procedures.

F-5. Conclusions and recommendations

a. Indicate whether the system is completely safe for testing or whether it is safe for testing with exceptions. List hazards and any technical or operational limitations or precautions needed to prevent injury and property damage during testing.

b. Highlight any known safety problems that will require further investigation during testing.

F-6. Signature

Provide the signature of the appropriate release authority.

Appendix G

MANPRINT Joint Work Group System Safety Checklist

G-1. Coordination for the MANPRINT Joint Work Group system safety checklist process

a. The MJWG will meet to write the System MANPRINT Management Plan (SMMP).

b. The safety representative and the MJWG must ensure that the SMMP will be passed to the associated and interested safety officers for comments.

c. Ensure the appropriate CBTDEV's and MATDEV's system safety representative is a voting member and present at all MJWG meetings.

d. Ensure all MANPRINT safety issues brought to the MJWG are passed to the SSWG for evaluation and determination of a risk assessment per MIL-STD-882.

e. Coordinate with the MJWG health hazard/system health hazard representative to ensure health hazard issues are consistent.

G-2. System safety checklist items

a. The MJWG safety representative and reviewers of the SMMP should ensure certain system safety items are included in the document. This includes, but is not limited to the following:

(1) The system safety goals in Section 3, MANPRINT Strategy.

(2) A SSMP as part of Section 4, Data Sources/Availability, Planned Level of MANPRINT Analysis Effort.

(3) The data sources used by the developers of the lessons learned are included in Tab A (Data Sources).

(4) The established level of trade-off authority for all MANPRINT issues. This trade-off authority must be consistent with the risk acceptance decision authority established under the SSMP.

(5) List the SSWG and MJWG interface responsibilities in the SSPP and SMMP especially as related to obtaining and analyzing data to identify the hazard(s).

b. MJWG chairman will ensure the MANPRINT assessment is coordinated with the SSWG chairman.

Appendix H

Non-developmental Item System Safety Market Investigation/Survey Questions

H-1. Non-developmental item market investigation/survey questions

The following are some basic system safety questions extracted from MIL-STD-882 that should be included in any NDI market investigation/survey:

a. Has the system been designed and built to meet applicable/any safety standards?

b. Have any hazard analyses been performed? Request copies.

c. What is the accident history for the system? Request specifics.

d. Is any protective equipment or actions needed during operation, maintenance, storage, or transport of the system? Request specifics.

e. Does the system contain or use any hazardous materials (to include radioactive substances), have potentially hazardous emissions (such as from a laser), or generate hazardous waste?

f. Are special licenses or certificates required to own, store or use the system?

g. Is the system similar to previous military system? If so, what are the lessons learned from the previous system?

h. If the new system attempts to resolve problems with previous system, what are the new hazards created with the new system?

H-2. Guidelines

Guidelines are according to MIL-STD-882 unless Army requirements dictate otherwise.

Appendix I Independent Safety Assessment

I-1. Independent safety assessment format

a. The ISA is an evaluation of the existence, status, and impact of hazards on a system and the effectiveness of the system safety program for that system. The ISA is the formal document used to communicate SSP status and any significant hazards to the materiel decision authority during MADP review. The ISA will consist of a transmittal letter signed by the CRC Commander (for major materiel acquisition programs) or the ACOM Headquarters (or equivalent) Commander that provides matrix safety support (for MAISRC and non-major materiel acquisition programs) which summarizes the ISA and a technical report prepared by the safety office overseeing the program.

b. Draft ISAs will be prepared ten weeks prior to MADP review for initial review by CRC, PEO, PM, and the User/TSM. The purpose of this initial review is to provide appropriate program personnel with advance notification of the safety assessment and to allow for comment or additional supporting documentation to be gathered from these offices. Unless additional information is provided to prove the draft ISA is in error, the draft ISA will become the final ISA. Three weeks prior to MADP review, the safety office will submit the final ISA to the following:

- (1) ASARC/MAISRC Secretary (major acquisitions) or MDA (non-major acquisitions);
- (2) DASA(ESOH);
- (3) DCS, G-1;
- (4) DTC;
- (5) PEO;
- (6) PM;
- (7) TSM;
- (8) AMC Safety Office;
- (9) TRADOC Safety Office, and
- (10) Other agencies/services as required.

c. While the nature of the letter and the report will depend on the maturity of the system under review, they will conform to the following general format with the transmittal letter will consist of three sections: Purpose, Discussion, and Recommendations.

(1) *Purpose*. This section will describe the reason for submitting the ISA (for example, in support of Milestone I/II decision).

(2) *Discussion*. This section will provide an executive summary of concerns outlined in the technical report.

(3) *Recommendations*. The comments in this section will be formulated to ensure that all system safety concerns are addressed by the MDA.

I-2. Independent safety assessment technical report

The technical report will consist of four sections: Purpose, Methodology, Results, and Recommendations.

a. *Purpose*. This section will state the reason for submitting the ISA, which will be to present the current assessment of safety issues concerning the system. The objective of the assessment will be to evaluate the overall health of the system safety program and mishap risk management process, and to identify potential hazards to Army personnel or equipment.

b. *Methodology*. This section will describe procedures used for conducting the evaluation and completing the technical report. These procedures will include a review of all system documents, contact with program representatives, participation in working groups, design and program reviews, and, if possible, on site evaluation of the system. An appendix of pertinent references will be attached.

c. *Results*. This section will be subdivided into two sections.

(1) The first subsection, System Safety Program Management, will identify program attributes and/or deficiencies and assess the overall effectiveness of the SSP by evaluating the following elements:

- (a) SSMP;
- (b) SSWG Charter and participation;
- (c) System safety activities relative to life cycle phase;
- (d) Hazard identification and tracking process, to include review of lessons learned;
- (e) Mishap risk management process;
- (f) Integration with associated disciplines;
- (g) MANPRINT interface; and

(h) Contractor system safety program.

(2) The second subsection, System Safety Technical Issues, will provide a discussion of significant safety hazards, real or potential, and associated risks. System hazards will be classified according to potential severity and probability, as outlined in the SSMP or as in this DA Pam (if no SSMP exist). Proposed corrective actions, to include implementation and verification schedules, will be indicated, as well as any formal acceptance of risks.

d. Recommendations. This section will contain recommendations formulated to ensure that each system safety concern is properly documented and communicated to the decision authority and that risk acceptance or corrective actions for identify system hazards is formally recognized and recorded.

Glossary

Section I Abbreviations

AAE

Army Acquisition Executive

A/E

architect/engineer

ACAT

acquisition category

ACOM

Army Command

AEC

Army Environmental Center

AESMNS

Army Equipment Safety and Maintenance Notification System

AMC

U.S. Army Materiel Command

AMCOM

U.S. Army Aviation and Missile Command

AMSAA

U.S. Army Materiel Systems Analysis Activity

ANSI

American National Standards Institute

AR

Army Regulation

ARLHRED

Army Research Laboratory-Human Research and Engineering Directorate

ARNG

Army National Guard

AS

acquisition strategy

ASARC

Army Systems Acquisition Review Council

ASA (ALT)

Assistant Secretary of the Army for Acquisition, Logistics and Technology

ASC

U.S. Air Force Aeronautical Systems Center

ASCC

Army Service Component Command

ASME

American Society of Mechanical Engineers

BRAC

Base Realignment and Closure

BTA

best technical approach

C2E

continuous comprehensive evaluation

CDD

capabilities development document

CBTDEV

combat developer

COEA

cost and operational effectiveness analysis

CRC

U.S. Army Combat Readiness Center

DA

Department of the Army

DA Pam

Department of the Army Pamphlet

DASAF

Director of Army Safety

DCS, G-1

Deputy Chief of Staff, G-1

DCS, G-3/5/7

Deputy Chief of Staff, G-3/5/7

DCS, G-4

Deputy Chief of Staff, G-4

DEH

Directorate of Engineering and Housing

DOD

Department of Defense

DPW

Directorate of Public Works

DRU

Direct Reporting Unit

DT

developmental testing

DTC

Developmental Test Command

DTE

development testing and evaluation

DTIC

Defense Technical Information Center

ECP

engineering change proposal

EIR

equipment improvement report

EMA

engineering mitigation alternatives

EMD

engineering and manufacturing development

FASS

Facility System Safety

FMECA

failure modes, effects, and criticality analysis

FUDS

Formerly Used Defense Sites

GFE

Government-furnished equipment

GPE

Government-provided equipment

HFE

human factors engineering

HFEA

human factors engineering analysis

HHA

health hazard assessment

HQDA

Headquarters Department of the Army

HQ, USACE

Headquarters, US Army Corps of Engineers

HTL

hazard tracking list

HTS

hazard tracking system

ICD

initial capabilities document

ILS

integrated logistic support

ISA

independent safety assessment

LCO

limiting conditions of operation

LSA

logistic support analysis

LSAR

logistic support analysis record

MA

managing activity

MAA

mission area analysis

MADP

Materiel Acquisition Decision Process

MANPRINT

manpower and personnel integration

MATDEV

materiel developer

MCA

military construction authority

MILCON

military construction

MIL STD

military standard

MJWG

MANPRINT Joint Working Group

MOD

modification program

MTBF

mean time between failures

MTTR

mean time to repair

NDI

nondevelopmental item

ODCS, G-1

Office of the Deputy Chief of Staff, G-1

O&SHA

operating and support hazard analysis

OHR

operational hazard report

OT

operational testing and evaluation

PEO

program executive officer

PFTEA

post-fielding training effectiveness analysis

PHA

preliminary hazard analysis

PHL

preliminary hazard list

PM

program/project/product manager

PMA

procedural mitigation alternatives

PMO

program management office

POC

point of contact

PQDR

product quality deficiency report

PRIMIR

product improvement management information report

QDR

quality deficiency report

RAC

risk assessment code

RAM

reliability, availability, and maintainability

RDA

research development acquisition

RFP

request for proposal

SAR

safety assessment report

SFA

support facility analysis

SHA

system hazard analysis

SME

subject matter expert

SMMP

System MANPRINT Management Plan

SOF

safety-of-flight

SOP

standing operating procedure

SOW

statement of work

SSE

system safety engineering

SSEB

source selection evaluation board

SSHA

subsystem hazard analysis

SSMP

System Safety Management Plan

SSPP

System Safety Program Plan

SSPT

System Safety Product Team

SSRA

system safety risk assessment

SSWG

System Safety Working Group

TADSS

training aids, devices, simulators, and simulations

TEMP

Test and Evaluation Master Plan

TIWG

Test Integration Working Group

TOA

tradeoff analysis

TOD

tradeoff determination

TOP

test operations procedure

TRADOC

U.S. Army Training and Doctrine Command

TR

technical report

TSM

TRADOC System Manager

TSWG

Technology Safety Working Group

USACE

U.S. Army Corps of Engineers

USACHPPM

U.S. Army Center for Health Promotion and Preventive Medicine

USAMEDCOM

U.S. Army Medical Command

USAR

U.S. Army Reserve

WCNMA

warnings, cautions, and notes mitigation alternatives

Section II**Terms****Combat developer**

Command or agency that formulates doctrine, concepts, organization, materiel requirements, and objectives; represents the user community in the materiel acquisition process.

Equipment

See definition for System.

Evolutionary acquisition

The DOD's preferred rapid acquisition strategy. It delivers capability in increments, with the recognition that future improvements in capability will be needed. It is substantially dependent on the consistent and continuous definition of requirements and maturation of technologies that lead to disciplined development and production of systems that provide increasing capability towards a materiel concept.

Hazard

An actual or potential condition that can cause injury, illness, or death or personnel, damage to or loss of equipment, property or mission degradation. In order to effectively describe a hazard, the hazard statement must consist of three basic components: 1) a Source (an activity, condition, or environment where harm can occur), 2) a Mechanism (means by which a trigger or initiator event can cause the source to bring about harm), 3) an Outcome (the harm itself that might be suffered expressed as a severity).

Incremental development

An acquisition approach in which a desired capability is identified, an end-state requirement is known, and that requirement is met over time by development of several increments, each dependent on available mature technology.

Materiel developer (MATDEV)

The RDA command, agency, or office assigned responsibility for the system under development or being acquired. The term may be used generically to refer to the RDA community in the materiel acquisition process (counterpart to the generic use of CBTDEV).

Probability

A quantitative or qualitative measure of the most reasonable likelihood of occurrence of an individual event(s)/hazard(s) that might create a mishap.

Residual hazards

Hazards which cannot be eliminated by design will be considered residual hazards unless the managing activity agrees the design meets or exceeds all applicable consensus or military design standards (or is verified through testing, where standards do not exist) and that the environment in which it will operate is consistent with that envisioned by the design. Example: Any pressure vessel presents a hazard; however, if it has been designed to meet or exceed ASME,

ANSI, and MILSTD1522, and it is used in an environment appropriate to these standards, then it will not be considered a residual hazard.

Residual risk

An expression of severity and probability from hazards after controls have been put in place.

Risk assessment

An evaluation of risk in terms of mission loss should a hazard result in an accident.

Safety assessment report

A formal, comprehensive safety report summarizing the safety data that has been collected and evaluated during the life cycle before a test of an item. It expresses the considered judgment of the developing agency on the hazard potential of the item, and any actions or precautions that are recommended to minimize these hazards and to reduce the exposure of personnel and equipment to them.

Safety confirmation

A formal document that provides the MATDEV and the decision maker with the test agency's safety findings and conclusions, and states whether the specified safety requirements have been met. It includes a risk assessment for hazards not adequately controlled, lists any technical or operational limitations, and highlights any safety problems that require further testing. The safety confirmation is provided to decision makers prior to major milestone decisions, materiel release decisions, and fielding decisions. It is attached to the evaluator report. The safety confirmation may be issued to the MATDEV/PM for equipping decisions of equipment outside the traditional acquisition process. For aviation systems, an Airworthiness Release does not negate the need for a safety confirmation.

Safety deficiency report

The method by which an activity should record and transmit information concerning a defect in the design, specification, materiel, manufacturing or workmanship of a product used by the Government. Reports must be placed into Category I or II based on the possible outcomes of the deficiency and must include supporting documentation based on objective evidence, such as direct examination, test, procedural review, etc. PQDRs may be submitted online thru AEPS, electronically using SF 368 or e-mail format, or telephonically. See AR 702-7 for specific reporting requirements.

Safety release

A formal document issued before any hands-on testing, use, or maintenance by Soldiers. A Safety Release is issued for a specific event at a specified time and location under specific conditions. It is a standalone document that indicates the system is safe for use and maintenance by Soldiers and describes the specific hazards of the system based on test results, inspections, and system safety analysis. Operational limits and precautions are included. The Safety Release must be available prior to start of testing or Soldier familiarization events to include new equipment training.

Severity

An assessment of the results of the most reasonable credible outcome that could be caused by a specific event(s)/hazard(s).

Spiral development

An acquisition approach that develops and delivers a system in builds, but differs from the incremental approach by acknowledging that the user need is not fully formed at the beginning of development, so all requirements are not initially defined. The initial build delivers a system based on the requirements as they are known at the time development is initiated. The succeeding builds are delivered which meet additional requirements as they are identified, refined through experimentation and mishap risk management or requirements are refined as a result of continuous user feedback based on experience with the initial build, and technology maturation.

Life Cycle Management Command (LCMC)

Responsible for the logistics support of assigned materiel and the development, acquisition, and support of non-system and system TADSS. Manages assigned technology base. Provides matrix safety support to the PEOs and PMs for all acquisition and fielded systems to include input for any system safety risk assessments.

System

A composite, at any level of complexity, of trained personnel, procedures, materials, tools, equipment, facilities, and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific production, support, or mission requirement.

System-of-Systems

A combination of systems which must be fielded together, either independently, on a platform, or in combination on different platforms to ensure an effective warfighting capability. The elements of this composite, of required personnel, procedures, materials, tools, equipment, facilities, and software, are used together in the intended operational or support environment to perform a given task or achieve a specific production, support, or mission requirement.

System safety

The optimum degree of safety within the constraints of operational effectiveness, time, and cost attained through specific applications of system safety management and engineering principles, criteria, and techniques throughout the life cycle of the system.

System safety management plan (SSMP)

A management plan that defines the system safety program requirements of the Government. It ensures the planning, implementation, and accomplishment of system safety tasks and activities consistent with the overall program requirements.

System safety program plan (SSPP)

A description of planned methods to be used by the contractor to implement the tailored requirements of MIL-STD-882, including organizational responsibilities, resources, method of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems.

User test

A generic term that encompasses operational test, force development test and experimentation, and joint user tests.

Section III**Special Abbreviations and Terms**

This section contains no entries.

UNCLASSIFIED

PIN 062355-000

USAPD

ELECTRONIC PUBLISHING SYSTEM
OneCol FORMATTER WIN32 Version 253

PIN: 062355-000

DATE: 11-13-08

TIME: 10:41:18

PAGES SET: 66

DATA FILE: C:\wincomp\p385-16.fil

DOCUMENT: DA PAM 385-16

SECURITY: UNCLASSIFIED

DOC STATUS: REVISION