Department of the Army
Pamphlet 385–16

Safety

System Safety Management Guide

Headquarters
Department of the Army
Washington, DC
4 September 1987

UNCLASSIFIED

SUMMARY of CHANGE

DA PAM 385–16
System Safety Management Guide

This new pamphlet contains guidance for implementing procedures and conducting system safety programs.

o

o

Headquarters
Department of the Army
Washington, DC
4 September 1987

Department of the Army Pamphlet 385–16

Safety

System Safety Management Guide

By Order of the Secretary of the Army:

CARL E. VUONO
General, United States Army
Chief of Staff

Official:

R. L. DILWORTH
Brigadier General, United States Army
The Adjutant General

History. This UPDATE printing publishes a new DA pamphlet. This publication has been reorganized to make it compatible with Army electronic publishing database. No content has been changed.

Summary. This pamphlet contains guidance for implementing procedures and conducting system safety programs.

Applicability. This pamphlet applies to the Active Army, the U.S. Army Reserve, and the Army National Guard.

Proponent and exception authority. Not applicable.

Interim changes. Interim changes to this pamphlet are not official unless they are authenticated by The Adjutant General. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

Suggested Improvements. The proponent of this pamphlet is the Office of the Chief of Staff of the Army. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Commander, U.S. Army Safety Center, ATTN: PESC–SE, Fort Rucker, AL 36362–5363.

Distribution. Distribution of this publication is made in accordance with DA Form 12–9A–R requirements for DA Pam 385-series publications. The number of copies distributed to a given subscriber is the number of copies requested in Block 344 of the subscriber's DA Form 12–9A–R. DA Pam 385–16 distribution is D for Active Army, ARNG, and USAR. Existing account quantities will be adjusted and new account quantities will be established upon receipt of a signed DA Form 12–9U–R (Subscription for Army UPDATE Publications Requirements) from the publications account holder.

Contents (Listed by paragraph and page number)

Chapter 1
Fundamentals of System Safety Management, *page 1*

Section I
Introduction, page 1
Purpose • 1–1, *page 1*
References • 1–2, *page 1*
Explanation of abbreviations and terms • 1–3, *page 1*
Participants • 1–4, *page 1*
Program elements • 1–5, *page 1*

Section II
Hazard and Risk Management, page 1
General • 1–6, *page 1*
Hazard identification • 1–7, *page 1*
Hazard severity and probability • 1–8, *page 1*
Hazard Tracking • 1–9, *page 2*
Risk management • 1–10, *page 2*

Chapter 2
System Safety for Combat Developers, *page 3*

Section I
Principles, page 3
Introduction • 2–1, *page 4*
Combat development activities within the life cycle • 2–2, *page 4*

Section II
Procedures, page 4
Historical safety information • 2–3, *page 4*
System safety substudies • 2–4, *page 4*
User test issues and criteria • 2–5, *page 5*
Hazard control recommendations • 2–6, *page 5*
Mission changes • 2–7, *page 5*
Training • 2–8, *page 5*

Chapter 3
System Safety for Materiel Developers, *page 5*

Section I
System Safety Management Concept, page 5
General • 3–1, *page 5*
Adapting the system safety program • 3–2, *page 6*
Technical support • 3–3, *page 6*
System safety management plan • 3–4, *page 6*
System safety program plan • 3–5, *page 6*
Test and evaluation master plan • 3–6, *page 6*

Section II
System Safety Procedures, page 6
Program management activities within the life cycle • 3–7, *page 6*
Risk management • 3–8, *page 7*

Section III
Integration of Associated Disciplines, page 7
General • 3–9, *page 7*
Manpower and personnel integration • 3–10, *page 7*
Reliability, availability, and maintainability • 3–11, *page 7*
Quality engineering • 3–12, *page 7*
Integrated logistic support • 3–13, *page 8*
Combat survivability • 3–14, *page 8*
Human factors engineering • 3–15, *page 8*

UNCLASSIFIED

Contents—Continued

Health hazards • 3–16, *page 8*

Chapter 4
System Safety for Testers and Evaluators, *page 8*

Section I
Introduction, page 8
General • 4–1, *page 8*
Types of tests and evaluations • 4–2, *page 9*

Section II
Test Planning, page 9
Pretest • 4–3, *page 9*
Adaptation • 4–4, *page 9*
Checklists • 4–5, *page 9*
Test integration • 4–6, *page 9*

Section III
Conduct of Test, page 9
General • 4–7, *page 9*
Technical tests • 4–8, *page 9*
User tests • 4–9, *page 10*
Nondevelopmental item tests • 4–10, *page 10*

Section IV
Evaluations, page 10
Independent evaluators • 4–11, *page 10*
Continuous comprehensive evaluation • 4–12, *page 11*
USASC system safety evaluation • 4–13, *page 11*
Source documents • 4–14, *page 11*
Release information • 4–15, *page 11*

Chapter 5
System Safety for Users, *page 11*

Section I
Principles, page 11
General • 5–1, *page 11*
User involvement within the life cycle • 5–2, *page 11*
Role of the installation safety manager • 5–3, *page 11*
Interaction with DCD • 5–4, *page 12*
Preliminary hazard list for facilities • 5–5, *page 12*

Section II
System Safety After Deployment, page 12
Hazard identification • 5–6, *page 12*
Safety inspections • 5–7, *page 12*
Accident investigation and reporting • 5–8, *page 13*
Health hazard identification • 5–9, *page 13*
User hazard reports • 5–10, *page 13*

Section III
Reporting and Correcting System Safety Deficiencies, page 13
Quality deficiency report • 5–11, *page 13*
Produce improvement program • 5–12, *page 14*
Modification work orders • 5–13, *page 14*
Safety-of-use messages • 5–14, *page 15*
Safety-of-flight messages • 5–15, *page 15*
Training • 5–16, *page 15*

Appendixes

A. References, *page 16*

B. Preparation Guidance for a System Safety Working Group Charter, *page 18*

C. System Safety Program Plan, *page 21*

D. Preliminary Hazard List/Analysis, *page 27*

E. System Safety Management Plan, *page 29*

F. System Safety Risk Assessment Preparation Guidance(Reference AR 385–16), *page 33*

G. Safety Release Preparation Guidance, *page 33*

Glossary

Index

Chapter 1
Fundamentals of System Safety Management

Section I
Introduction

1–1. Purpose
This pamphlet is intended to provide combat developers (CBTDEV), materiel developers (MATDEV), testers, independent evaluators, and users with the information necessary to develop, initiate, and effectively manage a system safety program.

1–2. References
Required and related publications 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
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. The combat developer. The CBTDEV should incorporate system safety performance objectives into the concept formulation package. Accident potential should be considered in concept studies and tradeoff analyses. The CBTDEV—

(1) Develops user 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 risk management decisions at program reviews and milestone decision meetings.

b. The materiel developer. The MATDEV 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 MATDEV sets goals and establishes mechanisms to attain these goals. The first step is to charter and fund a system safety working group (SSWG) to provide the technical expertise needed to manage the system safety effort.The MATDEV ensures that a system safety management plan (SSMP) is prepared to outline the system safety activities throughout the system life cycle. (In some cases, a program, project, or product manager may be appointed to perform the functions described in this paragraph.)

c. The tester. The tester supports the hazard identification and tracking process by structuring the test based upon the independent evaluation plan (IEP) and the test design plan. Testing will provide data to the evaluator to assess the "fixes" made to previously identified hazards and may identify new hazards. Hazards identified by the tester should be provided to the MATDEV for incorporation into the hazard tracking system.

d. The independent evaluator. The evaluator consolidates test data from all available sources to address the technical and user test issues and requirements developed for a system. 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 an IEP, emphasis should be placed on both evaluation of the "fixes" made to previously identified hazards and identification of new hazards.

e. The user. Primary activity occurs during early concept exploration and user testing and after the system is fielded.The two major roles are—

(1) Identification of hazards in order to improve the safety of existing systems (by submitting an equipment improvement report (EIR), for example).

(2) Development of historical data that can be used by the CBTDEV and MATDEV to produce safer systems in the future.

1–5. Program elements
a. The creation of an 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 changes extremely costly.

b. The principles outlined in this pamphlet are consistent with but not mandated by regulations in all cases. Good management principles have been used in those areas that are not regulated. The system safety requirements of the references in appendix A have been incorporated into this pamphlet.

c. Table 1–1 (located after the last appendix of this regulation)contains a list of activities that should occur in a system safety program. When regulatory, the Army Regulation number is cited; also cited are pertinent paragraphs of this pamphlet. Note that all tasks are not required for every phase. Each system safety program should be tailored to fit the needs of the particular acquisition strategy.(See para 3–2.)

Section II
Hazard and Risk Management

1–6. General
a. The MATDEV must establish procedures to ensure that hazards will be identified and their severity and probability estimated and that they will be tracked throughout the life cycle of the system.The MATDEV will identify potential corrective actions for each hazard and project the total life cycle accident costs for each potential corrective measure.

b. The CBTDEV will make recommendations as to the operational suitability of each corrective measure. Decisions to apply or omit corrective action should be made after a thorough risk analysis and consideration by the appropriate decision authority. If a correction is made, the hazard should remain in the hazard tracking system to ensure the effectiveness of the correction and to provide a record of its disposition.

c. Testers should validate the appropriateness of the correction imposed. The user collects accident and failure data to be used by the user major Army command (MACOM) to verify the assumed severity and probability of occurrence and merit of the control or ignore decision.For a given system, independent evaluators will assess the completeness and effectiveness of the hazard and risk management process.

1–7. Hazard identification
Only the potential for injury or equipment damage need exist in order to justify inclusion of a condition in the hazard list. Contractor studies and Government testing are the principal sources for the identification of hazards, but all possible sources should be used. Several types of analyses (para C–6) usually performed by the contractor can contribute to the hazard list. In addition, the MATDEV and CBTDEV should perform safety studies as part of the tradeoff determination (TOD), tradeoff analysis (TOA), and cost and operational effectiveness analysis (COEA).Other related disciplines, such as those listed in chapter 3, section III, will identify hazards or other information that should be evaluated to identify hazards.

1–8. Hazard severity and probability
a. 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 and the categories defined as shown in table 1–2 (taken from MIL–STD–882B). To aid in classification, these probability definitions can be supplemented in terms of exposure (for example, 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–882B are shown in table 1–3.

b. 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 running may be categorized at a lower level than if the system were defined as the entire tank. If the engine also powers the brakes, the same hazard that caused the engine to stop running also could cause the brakes to fail, which could result in destruction of the tank. Thus the hazard severity would be categorized at a higher level. The system-level impact of a particular hazard is the appropriate measure of its severity.

c. The risk associated with a hazard is a function of its probability and severity. Table 1–4 provides 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 1×4 and 2×2)masks prioritization.

Table 1–2
Hazard probability definitions

Description: Frequent
Level: A
Individual item: Likely to occur frequently
Fleet or inventory: Continuously experienced

Description: Probable
Level: B
Individual item: Will occur several times in life of item
Fleet or inventory: Will occur frequently

Description: Occasional
Level: C
Individual item: Likely to occur sometime in life of item
Fleet or inventory: Will occur several times

Description: Remote
Level: D
Individual item: Unlikely but possible to occur in life of item
Fleet or inventory: Unlikely but can reasonably be expected to occur

Description: Improbable
Level: E
Individual item: So unlikely it can be assumed occurrence may not be experienced
Fleet or inventory: Unlikely to occur but possible

Table 1–3
Hazard severity definitions

Description: Catastrophic
Category: 1
Mishap definition: Death or system loss

Description: Critical
Category: 2
Mishap definition: Severe injury, severe occupational illness, or major system damage

Description: Marginal
Category: 3
Mishap definition: Minor injury, minor occupational illness, or minor system damage

Description: Negligible
Category: 4
Mishap definition: Less than minor injury, occupational illness, or system damage

Table 1–4
Risk assessment codes

Probability of occurrence: A (frequent)
Severity category 1-Catastrophic: 1A
Severity category 2-Critical: 2A
Severity category 3-Marginal: 3A
Severity category 4-Negligible: 4A

Probability of occurrence: B (probable)
Severity category 1-Catastrophic: 1B
Severity category 2-Critical: 2B
Severity category 3-Marginal: 3B
Severity category 4-Negligible: 4B

Probability of occurrence: C (occasional)
Severity category 1-Catastrophic: 1C
Severity category 2-Critical: 2C
Severity category 3-Marginal: 3C
Severity category 4-Negligible: 4C

Probability of occurrence: D (remote)
Severity category 1-Catastrophic: 1D
Severity category 2-Critical: 2D
Severity category 3-Marginal: 3D
Severity category 4-Negligible: 4D

Probability of occurrence: E (improbable)
Severity category 1-Catastrophic: 1E
Severity category 2-Critical: 2E
Severity category 3-Marginal: 3E
Severity category 4-Negligible: 4E

1–9. Hazard Tracking

a. A system for tracking hazards should be initiated by the PM during the concept exploration phase and maintained throughout the life cycle of the system. A preliminary hazard list and analysis should be performed and then used as the basis for establishing the hazard tracking system. (See app D.) The hazard tracking system should list—

(1) The hazard.
(2) The RAC.
(3) Projected life cycle accident cost.
(4) Projected life cycle accident deaths.
(5) Projected corrective measures (with their RACs, application costs, and projected effects.
(6) Status of the correction.

b. The status should 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 tracking system during the useful life of the hardware and successor systems.The PM should ensure that a system safety risk assessment (SSRA) is performed, coordinated with the CBTDEV, and kept on file for each hazard. (See app F.) (See fig 1–1 for sample format for a hazard tracking system.) Since thousands of hazards may be identified over the life of a system, automation of the hazard tracking system is essential.

1–10. Risk management

a. Once a hazard has been identified and a RAC assigned, a determination should then be made as to what action should be taken to remedy the hazard. Based on the RAC, not all hazards are severe enough or occur often enough to justify the cost of lessening or eliminating them. Risk management involves—

(1) Identifying potential methods of controlling a hazard and the expected effectiveness of each method.

(2) Determining which method will be applied given the program's resource constraints.

b. The following methods are in order of precedence for controlling an identified hazard:

(1) Design for minimum risk.
(2) Incorporate safety devices.
(3) Provide warning devices.

(4) Develop procedures and training.

c. Determining which method should be applied is important;the decision to accept risk should be at a level appropriate to the priority of the hazard. From a safety standpoint, the goal should be to achieve the lowest level of residual risk. The hazard control methods in *b* above are listed in their order of effectiveness at reducing 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 identification is essential. Caution should be taken when relying on procedures or training as corrective measures. (See para 2–7.)

d. A single decision authority cannot review every hazard identified in a particular system; therefore, the PM should establish criteria to select the decision authority for each hazard. The selection of appropriate decision authority is based on both the type of materiel acquisition program and the level of risk that will be accepted. (See AR 70–1 for guidance on management levels for program decisions.)The decision authority for the highest level of risk is determined by using table 1–5; successive lower decision levels are then selected for the lower risk levels. After selecting the decision authority appropriate for the program, the PM should then create a table such as the example in table 1–6. After creating this decision authority matrix, the PM should include it in the SSMP. (See app E.)

Table 1–5
Management levels for risk acceptance

Type of program: DOD major **Management level:** Army acquisition executive
Type of program: Designated acquisition **Management level:** Army acquisition executive
Type of program: DA IPR **Management level:** DCSRDA
Type of program: IPR **Management level:** Commander of materiel development command
Type of program: Systems managed at a level below IPR **Management level:** Commander having procurement authority for the system

Table 1–6
Example decision authority matrix*

Hazard RAC: 1A, 1B, 1C, 2A, 2B, 3A **Decision authority:** Risk acceptance by Army acquisition executive
Hazard RAC: 1D, 2C, 2D, 3B, 3C **Decision authority:** Risk acceptance by MATDEV MACOM commander
Hazard RAC: 1E, 2E, 3D, 3E, 4A, 4B **Decision authority:** Risk acceptance by MATDEV MACOM subordinate commander
Hazard RAC: 4C, 4D, 4E **Decision authority:** Risk acceptance by PM (or MATDEV)

Legend for Table 1-6;
* DOD major or designated acquisition programs.

Hazard

RAC

Corrective measure

Residual RAC

Projected life cycle cost (deaths/injuries/damage/program delay

Cost to apply

Status

Figure 1-1. Sample for a hazard tracking system

e. The hazard RACs in table 1–6 refer to the residual risk remaining after corrective action. For example, a hazard is identified and assigned a RAC of 1A. The PM allocates additional funds for the contractor to apply an engineering "fix" to the system, which would reduce the RAC to 4A. The cost to further reduce the risk is prohibitive in the judgement of the PM; however, given the matrix in table 1–6, his or her commander must decide whether or not to accept the risk for this hazard. If the decision authority decides that the residual risk is acceptable, then the engineering "fix" should be applied and tested. In another example, a 1A hazard is identified, but the PM's recommended engineering "fix" will only reduce the RAC to 2B.The PM cannot accept that level of residual risk; therefore, the Army acquisition executive at the Army Systems Acquisition Review Council(ASARC) must decide on risk acceptability. If the decision authority decides that 2B is an unacceptable level, then the PM will have to take necessary action to reduce the risk.

f. The decision authority should receive an SSRA for each hazard. (See app F.) This is particularly important for hazards with a lower decision authority. Cost data should be used to supplement the RACs. Each potential corrective measure should be identified, and the residual risk, if it is applied, should be projected. The consequences of risk acceptance of the hazard and of each alternative corrective measure should be expressed using projected costs in terms of deaths, injuries, system damage, and program delay. Information on projected costs for application and residual risk of alternative corrective measures should be obtained from the contractor. Personnel death and injury costs can be calculated using AR 385–40, table E–1.

g. Test operating procedure (TOP) 10–2–508 (Test and Evaluation Command (TECOM)), AR 40–10, and AR 70–61 provide guidance on risk"acceptability." Since this guidance does not consider other factors such as impact on schedule and operational effectiveness, it should be used only for prioritization of hazard corrections. AR 385–16 requires that the CBTDEV provide a recommendation on the SSRA as to which corrective measure should be taken and the impact of alternative corrective measures.(See para 2–6.) These factors must be evaluated fairly, which is the principal reason a risk acceptance decision at an appropriate level should be made for every hazard. (See fig 1–2 for summary of this process.) Risk acceptance without input by the user, CBTDEV, and operational evaluator is unacceptable. Although their involvement is regulatory at the ASARC level, the PM should ensure in the SSMP that their participation is assured at lower decision levels.

h. The status of the hazard may be listed as closed only if a redesign has been completed, implemented, and verified as being completely effective in eliminating the hazard, or if approval has been given by the appropriate authority as defined in table 1–5 for acceptance of the residual risk. The hazard should be monitored, even if closed, so that accident data can be compared to the accepted RACs, to projected deaths or injuries, or to projected costs. Each system's accident experience should be periodically compared to the projections to determine whether or not previous risk management decisions should be reevaluated and other corrective measures proposed.

Chapter 2
System Safety for Combat Developers

Section I
Principles

2–1. Introduction

a. The CBTDEV has a vital role in the success of any system safety effort. As the concept for the system is developing, the CTBDEV should ensure that system safety is considered an integral component. The need for improvements in the safety of a system should be evident as early as the mission area analysis (MAA).As soon as it is determined that a new system is the appropriate solution to deficiencies identified during the MAA, the CBTDEV should seek system safety expertise. Some CBTDEVs have system safety expertise within their organizations; however, for those who do not, the principal sources of help are at the installation safety office and the CBTDEV's MACOM safety office. The CBTDEV is the integrator of system safety until a PM is chartered, usually after Milestone I. (See DA Pam 11–25.)

b. The principal system 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.

2–2. Combat development activities within the life cycle

a. Research and exploratory development phase. The CBTDEV should assemble historical system safety information on similiar predecessor systems. The CBTDEV's manpower and personnel integration (MANPRINT) joint working group (MJWG) should coordinate its system MANPRINT management plan with the SSWG to assure compatibility with the SSMP. (For more information on the MJWG, see AR 602–2.)The CBTDEV should determine the maximum allowable accident rate consistent with system availability. The tone for future system safety activity should be set by incorporating system safety objectives into all documents prepared by the CBTDEV such as the operational and organizational (O&O) plan.

b. Concept exploration phase. The CBTDEV should develop system and evaluation issues and criteria for user tests.Safety substudies should be conducted as part of the TOA and COEA to identify the impact of system safety on operational effectiveness.

c. Demonstration and validation phase. The CBTDEV should evaluate the impact of increased risk on operational effectiveness as tradeoffs are made for cost, weight, or schedule purposes.Mission-oriented safety requirements should be incorporated into requirements documents such as the required operational capability (ROC).

d. Full-scale development phase. The CBTDEV should attend design and program reviews to provide immediate user recommendations for risk-management decisions. Training and technical manuals should be reviewed to ensure inclusion of safety. Manuals must be very specific about what an item of equipment can and cannot do.

e. Production and deployment phase. Performance objectives should be made available to the user to provide criteria by which to evaluate the system. (See para 5–7*b*(2).)If accident severity or probability exceeds accepted residual risk, a product improvement should be initiated by the CBTDEV.(See para 1–10*h*.) Product improvement proposal (PIP)risk assessments should be reviewed and the user recommendation on acceptability of residual risk incorporated into the PIP package.Mission changes should be formally coordinated with the MATDEV and the user to ensure that system capabilities are not exceeded.The PIP process is described in paragraph 5–12.

Section II
Procedures

2–3. Historical safety information

a. Historical safety information on predecessor systems and the application of lessons learned are critical to the development of a safe system. The CBTDEV should begin to collect this information soon after approval of the justification of major system new start(JMSNS) or the O&O plan.

b. Historical safety information is available from the following sources:

(1) The U.S. Army Safety Center (USASC) maintains a computerized data base containing accident information. Safety lessons learned are also available. (Commander, USASC, PESC–D, Fort Rucker, AL 36362–5363.)

(2) The Human Engineering Laboratory (HEL) develops lessons learned in the area of human factors. (HEL, AMXHE–DA, Aberdeen Proving Ground, MD 21005–5001.)

(3) The Materiel Readiness Support Activity (MRSA) maintains the maintenance data base, integrated logistic support (ILS) lessons learned, and has recently established the MANPRINT data base. Also, MRSA is in the process of developing a health hazard assessment data base. (MRSA, AMXMD–EI, Lexington, KY 40511–5105.)

(4) The Air Force maintains a lessons learned data base, All lessons learned (including safety) are consolidated at the Air Force Acquisition Logistics Center (AFALC) by the Directorate of Lessons Learned. (AFALC, AFALC/PTL, Wright-Patterson AFB, OH 45433.)

(5) The Navy maintains computerized safety lessons learned and accident data. (Naval Safety Center, Code 90, Naval Air Station, Norfolk, VA 23511.)

(6) 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. (AMSAA, AMXSY–L, Aberdeen Proving Grounds, MD 21005–5071.)

(7) The materiel proponent maintains safety-of-flight, safety-of-use, equipment improvement, and quality deficiency reports.(See AR 95–18, AR 750–10, DA Pam 738–750, and DA Pam 738–751.)

(8) The Defense Technical Information Center (DTIC) can provide information on research being planned, research currently being performed, and results of completed research. (DTIC, DTIC–DDR–1, Cameron Station, Alexandria, VA 22314.)

(9) Users of predecessor systems maintain historical safety information. User MACOM safety offices can provide system safety input.

2–4. System safety substudies

a. The CBTDEV should 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 should be considered. Care must be taken in specifying accident rates, since testing is impractical. An early accident rate projection can serve the CBTDEV as a basis of comparison for accident rates projected for specific candidates. Also, an early accident rate projection is useful in defining crashworthiness levels and other 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 Deputy Chief of Staff for Operations and Plans (DCSOPS) must allow for attrition due to accidents. The Deputy Chief of Staff for Logistics(DCSLOG) assists in determining the attrition rate. The CBTDEV should coordinate with the DCSLOG and the DCSOPS to ensure consistency between the attrition rate and the maximum allowable accident rate.

b. The CBTDEV should review the MATDEV's TOD safety substudy(if conducted) to ensure user safety issues are addressed. (See para 3–7*b*.) The purpose of the TOD safety substudy is to identify desirable safety design features. Safety design features fall into two categories:

(1) 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.

(2) Design features that contribute to the systems's ability to prevent or reduce injury once an accident occurs.

c. A safety substudy should also be conducted by the CBTDEV as a part of the TOA. Any historical safety information not examined during the TOD should be studied. The safety design features identified during the TOD should be reexamined and tradeoffs made within the context of overall system effectiveness. The purpose of this substudy is to identify mission-oriented safety requirements that should be incorporated into any requirements documents. (See para 5–4.)Requirements documents should not specify a particular design, but should provide the designer with statements that define what the system should be able to do. 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.

d. The effectiveness of the safety design features in each candidate should be determined and each candidate's life-cycle accident costs should be estimated during a safety substudy conducted as part of the COEA. The life cycle accident costs should be incorporated into the overall COEA. Estimates of life cycle accident costs are made based on the accident history of predecessor systems. The USASC can assist in the development of an appropriate methodology for a particular system.

e. The CBTDEV should prepare input to the human factors engineering analysis (HFEA). He or she should 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 HEL. (See AR 602–1.)

2–5. User test issues and criteria

a. CBTDEV participation in the test integration working group (TIWG) is essential. Safety test issues and criteria in *b*and *c* below should be developed and incorporated into the test and evaluation master plan (TEMP). (See para 3–6.)

b. The quality of the user test in the area of safety depends on the development of safety issues. During the substudies described in paragraph 2–4, the CBTDEV should be alert for potential safety test issues.

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

2–6. Hazard control recommendations

a. Developmental systems. In coordination with the user, the CBTDEV should make a recommendation on acceptability of residual risk associated with proposed corrective alternatives.(See para 1–10.) This recommendation is part of the SSRA for each hazard. (See app F.) It should be forwarded to the appropriate decision authority as defined by table 1–6. If engineering change proposals (ECPs) are submitted, the CBTDEV should assess their impact and develop the user position regarding acceptability.

b. Fielded systems. The CBTDEV's recommendation on the acceptability of residual risk should be incorporated into any PIP. (See para 5–12.) The CBTDEV's recommendation, made in coordination with the user, should be provided to the materiel proponent, the USASC, and the DCSOPS.

2–7. Mission changes

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 should coordinate with the MATDEV and the user to determine the impact of that mission change. The MATDEV should determine if there are adverse impacts (such as performance limitations or MANPRINT factors)on the system. If hazards are identified, the risk management process described in chapter 1 should be used to resolve them. The CBTDEV, in coordination with the user, should also review modifications of doctrine and tactics for safety impact. A copy of this review should be provided to the DCSOPS.

2–8. Training

a. Safety should be included 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 so as 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.

b. The CBTDEV and the training developer should maintain a list of hazards controlled by training or procedure modifications.Training or procedure modifications are a last-resort control measure used when funding is critical. (See para 1–10*b*.) 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. (See para 2–5.)

c. The safety of training equipment and devices should 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 should examine the degree to which the devices emulate the actual system. As more reliance is placed on training with these devices rather than with actual equipment, the "realism"of the devices becomes a safety issue.

Chapter 3
System Safety for Materiel Developers

Section I
System Safety Management Concept

3–1. General

a. The principal objective of a system safety program is to make sure that safety, consistent with mission requirements, is designed into systems, subsystems, equipment, facilities, and their interfaces. The degree of safety achieved in a system depends directly on management emphasis; therefore, the PM must provide personal leadership and direction. A formal safety program that stresses early hazard identification and resolution through elimination or reduction to an acceptable level is essential.

b. The PM is responsible for integrating system safety into the acquisition strategy for his or her system. System safety is not an end in itself; it must be a part of the overall system's effectiveness. AR 70–17 requires the PM to ensure that, at all stages of system development—

(1) System safety engineering requirements are taken into account.

(2) System safety planning and analyses proceed in phase with the procurement effort.

c. To fulfill these integration responsibilities, the PM must ensure that hazards associated with every component of the system, whether or not he or she is responsible for their development, are identified, tracked, and resolved. The PM must also be alert for hazards that may be introduced into the system when subsystems, components, or equipment are added. Subsystem PMs should coordinate known or assumed hazards with the system PM. For example, if a PM is required to incorporate into his or her system an item of government-furnished equipment (GFE)that has a previously identified hazard, then the PM is responsible either for resolving the hazard or ensuring that the appropriate decision authority accepts the risk for it.

3–2. Adapting the system safety program

A successful system safety effort requires adaptation in order to fit the particular materiel acquisition program. This is particularly true for nondevelopmental items (NDIs) and other programs with an accelerated acquisition cycle. A summary of actions that typically should be performed by the PM during a system's life cycle is covered in paragraph 3–7. Table 1–1 may be used as a checklist, but each activity need not be performed for every system. The PM's system safety advisor should recommend activities that are necessary for his or her system. (See para 3–3.) The selected activities should then be included in the SSMP. (See para 3–4.)

3–3. Technical support

a. Major and designated acquisition programs. AR 385–16 requires the establishment of an SSWG for major acquisition programs. The purpose of the SSWG is to provide program management with system safety expertise and to ensure communication among all participants. The SSWG is officially formed and its authority defined by the PM through the SSWG charter. A sample SSWG charter is at appendix B.

(1) 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. The PM should appoint an individual within his or her office to serve as chairman of the SSWG. This individual also serves 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 engineer from an appropriate local safety office as co-chairman. A USASC representative will attend SSWG meetings for major systems as a Department of the Army (DA) observer.(See AR 385–16.)

(2) The frequency of SSWG meetings should 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; reliability, availability, and maintainability (RAM); human factors; and test and evaluation reports.

(e) Review of individual system safety hazards (old and new) and system safety engineering reports.

(f) Review of documents supporting safety such as test plans, budgets, contracts, and system safety program plans (SSPPs).

(g) Assignment of actions and reports resulting from requests for action.

(h) Preparation and approval of draft SSWG minutes.

b. Other programs. Funding and the required level of system safety effort may make an SSWG impractical for less-than-major acquisitions and NDIs. For these system safety programs, a different approach is necessary. The PM should formally request the support of a dedicated system safety engineer from an appropriate safety office. The PM should then ensure that communication takes place between the PM's office, the system safety engineer, and representatives of the various related disciplines.The PM should task the system safety engineer with the development of an SSMP, which serves two purposes:

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

(2) It serves as a tasking agreement between the PM's office and the safety office as to the level of effort required in terms of manhours.

3–4. System safety management plan

a. 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—

(1) Apply system safety requirements to a particular program.

(2) Designate the Government program system safety manager.

(3) Set forth a plan or action for the SSWG.

(4) Establish ground rules for Government and contractor interaction.

(5) Assign tasks, financial requirements, training requirements, schedules, data, and personnel.

(6) Designate which safety analyses and trade studies are required and when they should be performed.

b. The SSMP should be written so 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 E.

3–5. System safety program plan

a. An SSPP is required for all systems. The PM should require delivery of the SSPP as part of the contractor proposal.This plan should be required of each integrating contractor and prime contractors. (The Government is considered the integrating contractor when one is not named.)

b. 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 statement of work (SOW) within the request for proposal (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. (The Government will prepare the SSPP for in-house development projects.)

3–6. Test and evaluation master plan

The TEMP provides the basis for all testing and evaluation during the system life cycle. It integrates the activities of the test and evaluation community with the MATDEV. (See chap 4.) The PM normally forms a TIWG to prepare the TEMP. The PM should ensure adequate safety representation in the TIWG; ideally, these representatives should also serve on the SSWG. Tests should be planned to ensure that systems operate as planned or required. The CBTDEV may provide safety issues and criteria for both technical and user testing.(See para 2–5.) The safety representatives in the TIWG should ensure that safety design features are adequately tested during development and user testing. (See paras 4–8 and 4–9.)

Section II
System Safety Procedures

3–7. Program management activities within the life cycle

a. Research and exploratory development phase. A system safety program strategy should be formulated shortly after assignment of a PM. (The PM is normally not appointed until after a successful Milestone I decision; this reference to the PM is intended to include the management of the program if a PM has not been designated.) Upon appointment, the PM should ascertain whether the following tasks have been accomplished and if not, that they are done as soon as possible. A SSWG should be chartered (see app B) and tasked to accomplish, at a minimum, the following:

(1) Prepare an SSMP. (See app E.) The SSMP should then become a part of the PM's overall management plan. Preparation of the SSMP should be coordinated with the CBTDEV's system MANPRINT management plan. (See para 2–2*a*.)

(2) Coordinate with the CBTDEV for collection of historical safety data from the sources listed in paragraph 2–3.

b. Concept exploration phase.

(1) A preliminary hazard analysis/list, including a study of similar systems based on the historical safety data collected above,

should be completed to identify any desirable safety design features. This is best accomplished as part of the TOD. Any desirable safety design features identified during the TOD should be incorporated into the best technical approach (BTA) and the RFP.

(2) The TEMP is prepared and maintained by the MATDEV, with the assistance of the TIWG, and safety performance issues should be included. The tests should be planned to prove systems operate as advertised or required. The SSWG should be fully functional by this time. A hazard tracking system should be put into effect using information from the preliminary hazard analysis/list.

(3) An initial safety assessment report (SAR) should be prepared. The PM should ensure that selected members of the SSWG aid in preparation of the RFP. (See app C.) Key inputs include the SOW and safety design and evaluation criteria. The PM should 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.

c. Demonstration and validation phase. 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 SSMP and the TEMP should be updated. The preliminary hazard analysis and the SAR should be reviewed and updated.

d. Full-scale development (FSD) phase. During the FSD phase, the PM will closely monitor the contractor's effort and require the SSWG to perform at least a quarterly contractor performance appraisal. Safety issues should be thoroughly evaluated and brought to the attention of the PM. Identification of safety failures in FSD models is preferred to those in production models.Early identification of safety failures allows timely corrective action. The PM should ensure maintenance and operational hazard analysis results are reflected in maintenance and operator technical publications.

e. Production and development phase.

(1) *Production phase.* During this phase, numerous PIPs and ECPs will be submitted. The safety impact of each proposal should be carefully evaluated and documented. The PM should ensure that all PIPs 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) *Deployment phase.* Invariably, unanticipated hazards will be discovered during this phase. Adverse safety trends identified by mishap and safety deficiency reporting will have to be addressed. Maintenance of the hazard tracking system is essential. Previously identified hazards will have to be tracked to ensure the criteria associated with the accepted risk has not changed. If the accident probability or severity is worse than anticipated, the CBTDEV should be notified so that a product improvement can be initiated. (See para 1–10*h*.)

3–8. Risk management

a. The PM should ensure the preparation of an SSRA for each hazard. The PM should establish criteria to select the appropriate decision authority for each hazard as described in paragraph 1–10*d*.From the hazard tracking system, the SSWG should provide the PM a list of hazards that meet the above criteria. The PM should then select a recommended corrective action on the SSRA. Each SSRA should be coordinated with the CBTDEV, who should subsequently coordinate with the user. The appropriate decision authority should be presented with a completed SSRA (see app F) for each hazard requiring a decision.

b. For major and designated systems, the PM is also responsible for a presentation to the ASARC on system safety. This presentation should include a brief description of each hazard 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 should be presented to this group to ensure adequate agenda time.

c. The independent evaluators will prepare reports for materiel acquisition decision process (MADP) reviews. (See chap 4, sec II.) The SSWG should verify that the independent evaluators have copies of the appropriate documents listed in table 4–1 in time for evaluation prior to the MADP review date.

Section III
Integration of Associated Disciplines

3–9. General

Associated disciplines should be integrated into the system safety program by the PM through the SSWG. This integration can be extremely beneficial to the safety effort since hazards may be 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. The areas discussed in this section should be considered associated disciplines, and their representatives should be participants in the system safety program.

3–10. Manpower and personnel integration

MANPRINT is a process oriented toward integrating human factors engineering, manpower, personnel, training, system safety, and health hazard considerations into the materiel acquisition process.Every effort should be made to provide system safety input to the overall MANPRINT effort. The HFEA is the principal MANPRINT assessment document. Data from the various MANPRINT disciplines is collected by the HEL for inclusion in the HFEA prior to each MADP review. For major systems, the USASC provides input in coordination with appropriate local safety offices. For other programs, the local safety offices provide direct input to HEL and furnish a copy to the USASC.

3–11. Reliability, availability, and maintainability

A RAM program is required for most systems per AR 702–3.

a. Availability is the percentage of time an item is in a mission-committable status expressed as inherent, achieved, or operational availability.

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 failure (MTBF). The requirement for a reliability program plan (DI–R–1730) is normally incorporated into the RFP.

(1) A failure modes, effects, and criticality analysis(FMECA) report (DI–R–1734) will normally be required as a part of the reliability program. The contractor's integration of the results of the FMECA into his or system safety program should be established as criteria for the SSPP evaluation during source selection in those cases where the FMECA is required.

(2) Provisions should be made for the SSWG to examine reliability reports (DI–R–1731) 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. Maintainability is a measure of the ease with which an item may be maintained and repaired. It is usually stated as a mean time to repair (MTTR). A maintainability program will normally be required per MIL–STD–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). (For more information on the O&SHA, see para C–6*e*(4).) This exchange of information should be reflected in the maintainability program plan (DI–R–1740).

3–12. Quality engineering

One 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 should ensure that the SSWG monitors the critical items and service life surveillance programs. The PM should also ensure contractor integration of those programs into the contractor's system safety program by requiring a quality program plan (DI–R–1710) in the RFP and establishing it as evaluation criteria for the SSPP and for the quality program plan during source selection.

3–13. Integrated logistic support

As one of its primary tools, ILS employs a management science application termed logistic support analysis (LSA).

a. A LSA is required for all acquisition programs by AR 700–127 and should be established per MIL–STD–13881A. The logistic support analysis record (LSAR) (MIL–STD–13882A) is a manual and/or automated data base 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 technical manuals 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).

b. Normally, 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 technical manuals.

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.

3–14. Combat survivability

Survivability is a general term used to describe a system's ability to avoid and/or withstand manmade 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 features.

b. Survivability design features will affect both crashworthiness and emergency egress.

3–15. Human factors engineering

a. Data produced by the human factors engineering program per AR 602–1 is useful to the safety engineer and vice versa.

(1) The human factors organization should be placed on distribution for the preliminary hazard analysis/list, the O&SHA, and the SAR.

(2) The PM should ensure that the deliverable human factors engineering data item list is reviewed by the SSWG to determine which data items will be placed on distribution to the safety office.

(3) Coordination between the human factors engineering and system safety activities must be established to generate efficient output from each program.

(4) The system safety engineer and the human factors engineer must confer when potential program overlaps exist; addenda to data items should be prepared to account for these potential overlaps.

b. Human factors engineering personnel are responsible for conduct of the HFEA. The HFEA should be initiated prior to each milestone by the PM or, if no PM is chartered, by the CBTDEV.The content and purpose of the HFEA is discussed in AR 602–1.

3–16. Health hazards

a. The Office of the Surgeon General (TSG) is the proponent for Army programs to identify health-related hazards through the use of health-hazard assessment during system acquisition. AR 40–10 provides the policy for conduct of these health-hazard assessments.The PM will ensure that the SSWG is placed on distribution for these reports. The point of contact within the TSG office is the Preventive Medicine Consultants Division, HQDA (DASG–PSP), 511 Leesburg Pike, Falls Church, VA 22041–3258.

b. Health hazards are also considered safety hazards;therefore, a large overlap exists between the two disciplines.The assessment of health hazards is the responsibility of TSG.Examples include the following:

(1) Acoustical energy from steady-state and impulse noise as well as blast overpressure.

(2) Biological substances, to include micro-organisms, that cause disease, plus sanitation issues.

(3) Chemical substances, to include weapon and engine combustion products and other toxic materials.

(4) Oxygen deficiency in crew or confined spaces or caused by high altitude.

(5) Radiation energy from ionizing and nonionizing energy to include light and lasers.

(6) Shock due to rapid acceleration and deceleration.

(7) Temperature extremes and humidity resulting in heat and cold injury.

(8) Trauma resulting from blunt or sharp impact or musculoskeletal injury.

(9) Vibration affecting the entire body or specific body parts.

c. The SSWG must be prepared to support TSG in the area of hazard identification and to develop a coordinated effort for resolution of identified hazards. Hazard analyses are a primary means of health-hazard identification. The PM should ensure the RFP requires health-hazard assessments from the contractor.

Chapter 4
System Safety for Testers and Evaluators

Section I
Introduction

4–1. General

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

(1) To help the MATDEV uncover system problems for correction.

(2) To help the decision authority determine whether development is progressing satisfactorily and whether the system is likely to meet operational needs.

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. (See para 3–6.)The major effort of safety testing should be directed

toward identifying, evaluating, and tracking hazards. (See chap 1, sec II.) Hazard resolution will be accomplished by the MATDEV. System safety evaluations should focus on deficiencies in the system safety program as well as hazards.

4–2. Types of tests and evaluations

a. Distinctions are made in this pamphlet between testing and evaluation and between technical testing and evaluation (DT&E)and user test and evaluation, which includes operational test and evaluation (OT&E).

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

c. User testing of materiel systems is conducted with representative operators, maintainers, crews, and units under realistic combat conditions. The operational 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 tactics, doctrine, organization, and training.

d. 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. Pretest

a. During pretest planning, the tester should request a copy of the hazard tracking file from the PM. Test directives and test design plans for all tests should provide for an independent assessment of hazards and ensure that the results of these safety evaluations are included in all reports. The independent evaluator and the tester can then evaluate the hazards. Emphasis should be placed on checking hazards that have "fixes" applied and identifying those uncorrected hazards about which the tester should be warned. If the PM has not established a hazard tracking system, the tester should ensure his or test reports are complete enough to serve as a basis for starting a tracking system.

b. Precautions are taken to protect personnel and equipment during tests. Safety assessment reports (DI–SAFT–80102) and safety releases (app G) are used to integrate safety into test planning and procedures and for shipping and handling of the system.

(1) Prior to development testing—

(a) An SAR is received from the contractor, reviewed, and accepted by the MATDEV. The SAR is a formal, comprehensive safety report that summarizes the safety data that has been collected and evaluated during the life cycle. (See para C–7*d*(1).) 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 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 MATDEV should prepare the SAR.

(2) No testing involving troops will begin until a safety release has been issued to the test organization (such as Training and Doctrine Command (TRADOC) boards and government laboratories).(See AR 70–10.) Safety releases are provided to user test organizations by the MACOM responsible for user testing (for example, TRADOC and Health Services Command).

(3) For technical and Operational Test and Evaluation Agency(OTEA)-conducted tests, the safety release is prepared by the MATDEV.When the CBTDEV is the designated user tester, the MATDEV provides safety release recommendations to the CBTDEV for preparation of the safety release. The safety release will 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 G. The test agency or command will ensure that test objectives can be met within the limits stated in the release.

4–4. Adaptation

a. A successful system safety effort requires adaptation in order to fit the particular test. Not every test need be performed for every system. The test agency may consult the SSWG on which tests are necessary for a particular system. (See para 3–3.) The selected tests or assessments should then be included in the TEMP (para 3–6)and the safety subsection of the test design plan or detailed test plan.

b. During technical testing, specific safety tests should be performed on critical devices or components to determine the nature and extent of materiel hazards. Particular attention should be given to identifying and evaluating special safety and health hazards listed in paragraph 3–16*b*. Attention should also be given to evaluating the adequacy of hazard warning labels on equipment and warnings, precautions, and control procedures in equipment publications.

4–5. Checklists

The TECOM has published a series of safety test operations procedures(TOPs) that can be used as checklists for safety tests and evaluations.

4–6. Test integration

Tests for system safety should be incorporated into tests required for other disciplines. This can be accomplished through the TIWG.The PM should ensure adequate safety representation in this group.

Section III
Conduct of Test

4–7. General

a. Many organizations responsible for testing do not have system safety engineers on their staffs. This results in reluctance to conduct safety testing. There are some tradeoffs 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. (See para 4–3.)

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 equipments, and design objectives.

4–8. Technical tests

a. Technical testing is 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 MATDEV.Therefore, technical testing of safety is characterized by systematic testing of materiel using highly technical equipment and instrumentation under laboratory or other rigorously controlled conditions.

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

c. Specific safety tests are also performed on critical devices or components to determine the nature and extent of hazards presented by the materiel. Requirements for such tests will be found in the TEMP (para 3–16) and are usually performed during technical testing when contractor testing and data are not sufficient to make a hazard assessment.

4–9. 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, operational testing of safety issues is less systematic and less technical than that conducted during technical testing. It is common, however, for unanticipated hazards to occur when a system is placed in the hands of soldiers and put to use, so user test planning must include disciplined observation and other data collection procedures to ensure that such hazards are identified. As always, these hazards must be reported and added to the hazard tracking list.

b. Hazards identified in previous technical tests 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 operational testing is whether any safety release restrictions imposed upon the use of or training with the system are so confining that the user's training needs cannot be met or that an adequate user test cannot be conducted.

4–10. Nondevelopmental item tests

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

b. NDIs 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. Safety assessment reports and safety releases are required for NDI testing. (See para 4–3.)

Section IV
Evaluations

4–11. Independent evaluators

a. The two principal evaluation organizations for major acquisitions are the AMSAA and OTEA. AMSAA focuses its evaluation on how well a system has met performance specifications. OTEA evaluates the system's potential operational effectiveness and suitability in a combat environment.

b. For certain designated acquisition programs, TECOM is the technical independent evaluator. TRADOC performs the role of operational independent evaluator for those programs.

c. 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.

d. One element of analysis that is common to all independent evaluations is system safety. A system safety evaluation is an assessment of the existence, status, and impact of hazards on the system and the effectiveness of the system safety program for that system. The evaluation focuses on the impact of any hazards or program deficiencies in terms of the system's overall effectiveness. The documents listed in table 4–1 should be evaluated.

Table 4–1
Documents necessary for a system safety evaluation

Document: Program Manager's Charter. **Preparer:** MATDEV.
Document: Operational and Organizational (O&O) Plan. **Preparer:** CBTDEV.
Document: System MANPRINT Management Plan. **Preparer:** CBTDEV.
Document: SSWG Charter. **Preparer:** MATDEV.
Document: System Safety Management Plan. **Preparer:** MATDEV.
Document: Tradeoff Determination Safety Substudy. **Preparer:** MATDEV.
Document: Best Technical Approach (BTA). **Preparer:** MATDEV.
Document: Tradeoff Analysis Safety Substudy. **Preparer:** CBTDEV.
Document: Human Factors Engineering Analysis. **Preparer:** MATDEV.
Document: Health Hazard Assessment. **Preparer:** HQDA (DASG–PSP).
Document: Hazard List From Hazard Tracking System. **Preparer:** MATDEV.
Document: Test and Evaluation Master Plan (TEMP). **Preparer:** MATDEV.
Document: Integrated Logistic Support (ILS) Plan. **Preparer:** MATDEV.
Document: Required Operational Capability (ROC). **Preparer:** CBTDEV.
Document: Statement of Work (SOW). **Preparer:** MATDEV.
Document: Request for Proposal (RFP). **Preparer:** MATDEV.
Document: Contractor Safety Assessment Reports. **Preparer:** MATDEV.
Document: System Assessments and Disciplined Review Reports. **Preparer:** MATDEV.
Document: Physical Teardown and Logistics Demonstration Report. **Preparer:** MATDEV.
Document: Operator and Maintenance Manuals. **Preparer:** MATDEV.
Document: Safety Releases. **Preparer:** MATDEV.
Document: Technical Test Plans and Reports. **Preparer:** MATDEV.
Document: User Test Plans and Reports. **Preparer:** User Test Organization.
Document: AMSAA Independent Evaluation Report. **Preparer:** MATDEV.
Document: Independent Evaluation Report. **Preparer:** User Test Organization.
Document: Force Modernization Review Report. **Preparer:** HQDA (DAMO–FM).
Document: Follow-On Evaluation Reports. **Preparer:** MATDEV.

4–12. Continuous comprehensive evaluation

a. OTEA is responsible for providing a comprehensive evaluation of the system by integrating reports and analyses of the individual test and evaluation organizations. OTEA also plays the role of spokesman for test and evaluation organizations before the MADP review body.

b. As explained in AR 71–3, OTEA has developed a methodology known as Continuous Comprehensive Evaluation (C^2E) to achieve the evaluation integration responsibilities outlined above.C^2E focuses on evaluating major system acquisitions, evaluating the system's progress in reaching its operational effectiveness objectives over its entire development cycle, and utilizing all available information in the evaluation process. A test, evaluation, analysis, and modeling (TEAM) plan is prepared to—

(1) Identify the resources to be used in the evaluation process.

(2) Outline evaluation strategy.

(3) Provide the schedule of C^2E events.

(4) Contain the coordinated support agreements between OTEA and other commands.

c. System safety issues enter the C^2E process through continual dialogue among the MATDEV, CBTDEV, technical and operational testers and evaluators, and other members of the acquisition team. Key activities for input of system safety issues to C^2E are the development of the TEMP issues and criteria. The forum for coordination of acquisition team activities is the TIWG. The SSWG should ensure that the updated SSMP is used throughout the development process by the TIWG for each update of the TEMP and by OTEA for each update of the TEAM plan.

4–13. USASC system safety evaluation

A system safety evaluation is prepared by the USASC and provided to the Deputy Chief of Staff for Personnel (DCSPER) for each major milestone review. The USASC evaluation assesses the status of the system safety program and any significant hazards that require attention at the MADP review. In addition to the DCSPER, the USASC evaluation is provided to OTEA for the reason discussed in 4–12 above and, in coordination with input from the appropriate local safety office, provided to the HEL for incorporation into the HFEA.

4–14. Source documents

The accuracy of the system safety evaluation is a function of the quantity and quality of the source documents used in its preparation-.Document selection for the evaluation depends on the point in the life cycle at which the evaluation is being performed. The documents listed in table 4–1 are candidates that may be available to the evaluator for review.

4–15. Release information

Documents listed in table 4–1 and any other documents or materials generated for system safety purposes are intended for use within official DOD channels; they are not intended for routine release to the public.Requests for such material under the Freedom of Information Act will be forwarded for release determination to the Commander, USASC, ATTN:PESC–SE, Fort Rucker, AL 36362–5363, together with a copy of the requested material.

Chapter 5
System Safety for Users

Section I
Principles

5–1. General

a. The requirements for developing and implementing a system safety program are set forth in AR 385–16. It emphasizes the establishment of system safety early in the system's life cycle through the efforts of CBTDEVs, MATDEVs, and testers and evaluators who design and implement hazard control measures for various systems. The users of the system also should be involved in the system safety effort.

b. The intent of this chapter is to provide users with information on administering and implementing a system safety program, stressing early hazard identification, and elimination or reduction of associated risk to an acceptable level.

5–2. User involvement within the life cycle

a. Introduction. Other than the few soldiers who are involved in testing, the user is first introduced to a new system during the deployment phase when the system becomes operational at unit level. This is the critical time for safety personnel to monitor field failures or accidents to identify hazards and begin the correction process. However, corrective efforts at this late phase in the life cycle will be costly and difficult to implement.After all, it is easier and less costly to make a change on the drafting board than after hardware has been manufactured. In addition, lessons learned from the past should be incorporated into future designs. Major cost savings can be realized on any system if system safety is emphasized in the early phases of the life cycle.

b. Concept exploration phase. Installation safety personnel should assist CBTDEVs as they collect historical safety information and as studies are conducted to point out critical safety-related operational requirements. A preliminary hazard list should be developed by the installation safety office for new facilities or facility modifications. (See para 5–5.) When requested, installation safety offices should provide field experience and user safety requirements to the CBTDEV for inclusion in requirements documents.

c. Deployment phase. This phase of the life cycle begins when the system becomes operational and is fielded for use.System safety concerns are now directed toward evaluating any hardware or procedural changes that may have occurred.

(1) Operational activities should be reviewed to ensure that maintenance procedures are not hazardous or cause other hazards.

(2) Installation of modification work orders (MWOs) must be monitored to ensure timely installation.

(3) Emergency procedures and any training programs should be evaluated to ensure that proper safety standards exist.

(4) Any problems, incidents, or accidents that occur during this time must be investigated to determine the cause.

(5) Hazards identified by the user should be reported.The user must ensure the system is used in accordance with published procedures. The user should also inform the CBTDEV when the system no longer matches the mission or purpose for which it was intended.

(6) Other specific tasks that safety personnel perform or monitor during the deployment phase will be addressed in section II.

5–3. Role of the installation safety manager

a. AR 385–16 addresses the role of the user, specifically the installation commander's responsibilities. However, evidence suggests that not all requirements of AR 385–16 are being fulfilled.Possible reasons for this include lack of specific tasks and directives for accomplishing the specified guidelines in AR 385–16 and the inability to identify and work with people who interface within system safety concerns. These problems and appropriate methods for correcting such deficiencies should be the focus of the installation safety manager since he or she is the user's principal local source of system safety information.

b. The user MACOM safety office should develop procedures for implementation of a system safety program within the MACOM.The installation safety manager should make use of the system safety expertise in the user MACOM safety office. The user MACOM safety office should conduct surveys to ensure that installation system safety programs are functional.

c. The installation safety manager's role is particularly important at installations having a Directorate of Combat Developments(DCD). Installation safety personnel can play a proactive role

in system development by providing input early in the life cycle through the CBTDEV.

5–4. Interaction with DCD

a. Within each DCD, an office or individual will be tasked with system safety responsibility. One method of achieving early involvement in the system life cycle is for the installation safety office and the user MACOM safety office to develop active working relations with this office or individual. The practical safety expertise contributed by the installation safety office and user MACOM is invaluable. With this type of coordination, safety can be incorporated into a system more effectively and in the earliest possible phase of the life cycle.

b. A major function of the DCD is to develop the required operational capabilities for any proposed new system. The ROC is prepared by the CBTDEV in conjunction with the MATDEV, logistician, and manpower and personnel planner. It concisely states the essential operational, technical, MANPRINT, training, logistical, and cost information to start full-scale development or procurement of a materiel system. Installation safety managers should take the initiative to work with DCD personnel and provide them with specific system safety data. Quite often, ROCs are written with only a vague statement that the system will comply with the applicable safety standards.With assistance from the safety office, qualitative safety standards that address specific requirements can be written into the ROC.

5–5. Preliminary hazard list for facilities

a. Another opportunity for early user involvement in the life cycle is during requirements development for new facilities.This represents the concept phase for construction of a new structure.

b. During this phase, installation safety office personnel have a responsibility to develop a preliminary hazard list (PHL)to identify specific hazards related to that type of facility. (See AR 385–16.) The PHL is the initial hazard analysis during the system design phase. The purpose of this analysis is not to effect control of hazards but to fully recognize the hazardous states with all accompanying system implications. Safety personnel should interface with installation engineers in reviewing any proposed concepts to ensure that potential hazards are identified. Details for completing a PHL are at appendix D.

c. Once completed, the PHL should be attached to DD Form 1391 (Military Construction Project Data) (see AR 415–15) and forwarded to the area corps of engineer district where it can be used during facility design reviews. The benefit of this list is to identify hazards so facility developers can design out most of the potential accident causes before construction begins. To ensure safety offices are aware of proposed new construction and facilities renovations, a safety official should be a member of this Installation Planning Board and the New Work Review Board.

Section II
System Safety After Deployment

5–6. Hazard identification

Once a system is fielded, efforts should be focused on discovering safety deficiencies. Safety personnel as well as users must be aware of the known hazards of the system. In addition, other hazards are discovered during wide use of the system. The primary effort in this continuing examination is to ensure that hazards are identified.Once identified, they can be evaluated and then ultimately controlled or risk accepted. Hazard identification methods are described in this section.

5–7. Safety inspections

The purpose of the safety inspection is to eliminate accident causes through procedures designed to detect unsafe conditions and unsafe practices. Specifically, safety inspections are concerned with the condition of the system or facility, condition of the work area, personnel practices, and job procedures. To be successful, safety inspections require—

a. Competent inspection personnel.

(1) By virtue of his or her duties and experience, the installation safety specialist should be one of the most qualified individuals to perform safety inspections. However, with the variety of operational systems and facilities on any installation, it is quite difficult for safety personnel to become authorities on all systems, especially those that are newly fielded. Therefore, installation safety personnel should take advantage of local expertise and coordinate safety inspections with personnel who are knowledgeable and familiar with the system.

(2) Success of these inspections depends on unit safety personnel. Proper safety training for unit safety personnel is essential. Inspection results should be collected and analyzed for trends at installation level.

b. Definite schedules regarding what to inspect and how frequently.

(1) AR 385–10 sets forth the requirement for annual installation-level inspections of all facilities. However, facilities and operations involving special hazards will be inspected more frequently as determined by the designated safety and occupational health official. Special hazards are those that are likely to produce high probability or high severity personnel injuries, high dollar losses, or losses likely to produce significant legal action or discredit to the Army.

(2) With newly fielded systems, which are normally under a warranty or guarantee period for the first year of use, extra effort should be made to observe the system carefully to ascertain that it is meeting its performance objectives. When such systems are being fielded by the Army, the manufacturer will usually have technical representatives on location to—

(a) Work with safety personnel when problem areas are identified.

(b) Coordinate warranty actions.

(c) Guard against potential accidents or incidents.

(3) Special inspections should be conducted to ensure that no additional hazards will be created by changes introduced into the system. These inspections should cover establishment of new procedures, relocation or revision of operations, and other modifications.

(4) In addition to the annual facilities inspection mentioned in(1) above, the installation safety manager should inspect the safety program of each unit, activity, and agency on the installation.One element of this inspection should be the adequacy of the system safety effort.

c. Adequate systematic procedures.

(1) A methodical approach to any safety inspection can best be achieved through the use of a checklist. Examples of safety inspection checklists may be found in DA Pam 385–1 and the "Guide to Aviation Resources Management for Aircraft Mishap Prevention, "available from USASC, ATTN: PESC–M, Fort Rucker, AL 36362–5363.

(2) Checklists for new systems can be found in the dash–10 operators manual. This manual provides a brief description of major parts and features of the system. It also includes preventive maintenance checks and services and provides specific instructions on inspecting the system. Also, a list of safety warnings included in the front of the manual points out potential hazards and appropriate controls.

d. Proper maintenance of inspection records. Unsafe conditions and practices revealed by the inspection should be recorded along with recommendations for correcting these deficiencies. During the program inspection discussed in paragraph *b*(4) above, installation safety personnel should ensure that the recommendations for correcting deficiencies are being passed to the appropriate agency for action. Over a period of time, these inspections should uncover fewer unsafe conditions as countermeasures are initiated.However, recurring problems often are indicative of deficiencies within the system's materiel. By maintaining a file of reports on all inspections, safety personnel can readily detect these persistent problem areas.

5–8. Accident investigation and reporting

a. Investigation. Despite all design efforts made in the development of a system, accidents will occur. While some of these may be predicted, others cannot be foreseen due to unpredictable aspects of use or environment.

(1) Installation safety office personnel should participate in accident investigations to identify the system elements that caused or permitted the accident to occur. These system elements include task errors made by man, failures or malfunction of materiel, or environmental influences.

(2) Once the investigation is complete, the proponent activities responsible for each inadequate system element can be formally notified of deficiencies to determine feasible corrective actions.

(3) Procedures for conducting thorough accident investigations for aircraft mishaps are described in DA Pam 385–95. AR 385–40 provides information on investigation requirements for ground accidents.

b. Reporting. Properly completed DA Forms 285(U.S. Army Accident Investigation Report) and DA Forms 2397–R-series (Technical Report of U.S. Army Aircraft Accident)are essential sources of accident data. Safety personnel should collect and analyze accident data to determine recurring system inadequacies. Only when hazards are discovered can resolutions be implemented. Even if the hazard cannot be promptly corrected due to procedural and economic constraints, the problem, if revealed to the CBTDEVs (see para 2–3), can be designed out of future replacement systems. Although accident investigation and reporting is an after-the-fact reaction, the lessons learned from a present system can be used in a proactive approach when developing future systems.

5–9. Health hazard identification

a. Preventive medicine program. The authority for determining occupational health hazards belongs to the occupational health function of the preventive medicine program. Several people support preventive medicine efforts; however, the installation's industrial hygienist plays an integral role in the occupational safety and health program. The hygienist is responsible for performing all industrial hygiene surveys to identify specific work-related health hazards. These surveys are known as the health hazard inventory(HHI) module of the Occupational Health Management Information System-;they are required by AR 40–5, paragraph 5–3*e*.

b. Health hazard inventory.

(1) Information contained in the HHI includes—

(a) Type of facility or activity surveyed.

(b) Operation involved.

(c) Hazards or exposures detected.

(d) Number of people exposed.

(e) Methods of control, including personal proactive equipment, engineering methods, administrative controls, or warnings.

(2) The installation safety manager, who is the designated installation occupational safety and health official, should be provided a copy of the installation HHI quarterly by the industrial hygienist. The HHI is an excellent source of hazard data. By interfacing with the industrial hygienist, safety personnel can become aware of health hazards existing on the installation and then can concentrate their efforts on monitoring the effectiveness of control methods.

(3) Health hazards can be controlled by "designing"them out of the system; by substitution, isolation, or enclosure of the hazardous material; or by ventilation. When reviewing designs for proposed new systems that may have potential health hazards, the SSWG should ensure that these types of controls are included.Users should be prepared to respond to MATDEV requests for recommended health hazard control measures for proposed new systems.

5–10. User hazard reports

a. Reports by Army personnel or others who actually use Army systems are an important means of detecting hazards that may lead to accidents. These reports are handled at the operating level to ensure prompt, efficient processing.

(1) *Operational hazard report (OHR).* DA Form 2696–R (Operational Hazard Report) is used by the aviation community to record information about hazardous acts or conditions before mishaps occur. An operational hazard is any condition, action, or set of circumstances that compromises the safety of Army aircraft, personnel, or equipment. OHRs document materiel misuse and maintenance practices that are hazardous to safe flight.

(a) OHRs are routed to the unit's aviation safety officer, who is responsible for investigating the hazard promptly and recommending corrective actions to the commander.

(b) OHRs can be forwarded to the next higher command when corrective actions exceed the capabilities of the receiving unit.

(c) Although the installation safety office is not included in the routing requirements, installation safety personnel should monitor each unit's OHR log to identify possible system inadequacies.

(d) Information pertinent to OHRs is in AR 385–95.

(2) *Employee reports of unsafe or unhealthful working conditions.* DA Form 4755 (Employee Report of Alleged Unsafe or Unhealthful Working Conditions) serves the same purpose for ground-related hazards as an OHR for aviation hazards. These reports are handled at the operating level to ensure prompt, efficient processing. However, procedures exist to allow these reports to be submitted directly to the installation safety office. In such cases, safety personnel should investigate the hazard and implement necessary corrective actions. The procedure for submitting DA Form 4755 can be found in AR 385–10.

b. The installation safety office should actively promote the use of OHRs and reports of unsafe or unhealthful conditions by all personnel. These reports can benefit system safety efforts by providing a means for users to bring hazards to the attention of those who have the authority to implement corrective actions.Safety personnel who fail to monitor these reports are neglecting their responsibility to add valuable user input concerning the safety of Army systems.

Section III
Reporting and Correcting System Safety Deficiencies

5–11. Quality deficiency report

a. Any time an accident involves materiel failure, malfunction, or design, the proponent activity responsible for the equipment must be notified. The mechanism for making this notification is SF 368 (Product Quality Deficiency Report (QDR)). The purpose of submitting a QDR is to—

(1) Report conditions that are the result of below-standard workmanship (such as materiel that does not conform to design specifications).

(2) Report materiel faults in design, operations, or manufacture with the purpose of initiating early and effective corrective action or to recommend improvements.

b. Any user of Army materiel who discovers a defect or has an equipment improvement recommendation is responsible for reporting it to the sponsoring agency; for example, U.S. Army Materiel Command (AMC) or other MATDEV commands. This includes actual users as well as safety personnel. Information on completing and addressing QDR/EIRs is contained in DA Pam 738–750. Reports should be submitted without delay even if an item has been repaired or replaced locally.A record of the failure is important to the proponent activity in determining possible wide-use problems. Direct contact between the sponsoring agency and the QDR/EIR originator is encouraged to exchange ideas and gather feedback.

c. Quality defects and equipment improvement recommendations fall into two categories:

(1) Category I involves deficiencies that will or may affect life or limb of personnel or impair the combat capabilities of the using organization or individual. Deficiencies that affect operational capability to the extent that mission accomplishment is jeopardized fall within this definition. Category I deficiency reports should be sent to the proper command in message format within 48 hours after the discovery of the defect or problem. They may be phoned in or brought in, but must be followed up with a message. The message should be priority and unclassified.

(2) Category II involves deficiencies that do not meet criteria set forth in category I. For all other defective materiel conditions or recommendations for improvement (category II), a properly completed SF 368 should be sent to the proper command within 5 working days after discovery of the defect. Details on completing the SF 368 and where to send it are included in DA Pam 738–750.

d. Commands that receive SF 368 should acknowledge receipt of the QDR within 7 days. They should investigate the reports and ensure that the disclosed deficiencies are corrected. This often is a time-consuming process since any proposed engineering changes must be approved by the configuration control board. Once a change is approved, it can be processed by one of the following methods:

(1) Through the product improvement cycle.

(2) As a minor alteration (making it optional in the field and mandatory in the depot).

(3) As a component modernization by attrition.

(4) As a component modernization by obsolescence.

e. Since the user is responsible for reporting equipment deficiencies, the installation safety office should be actively involved in monitoring the submission of QDR/EIRs. Installation commanders, through their safety staff, should review all locally-initiated EIRs for impact on safety and to ensure their proper classification as category I or II. The installation safety office must instill the value of these reports to all units and stress their importance in contributing to system safety input.Such reports not only provide a means for correcting present deficiencies, but also allow the problems to be designed out of future replacement systems.

f. One way to provide an incentive for QDR/EIR submission from the field is to recommend that users also submit ideas on equipment improvements as suggestions per AR 672–20. If the improvement is adopted as a result of a suggestion, the user may receive a monetary award.

5–12. Produce improvement program

a. A product improvement is a configuration change to an existing system or piece of equipment in response to a user-validated need. The improvement requires testing to assure that it accomplishes what is intended without jeopardy to any interfacing system and is installed as a modification kit in the field. The objective of product improvement is to extend the useful life or improve the capability of existing materiel rather than acquiring or developing entirely new equipment. A product improvement is used as the means by which materiel is reconfigured to—

(1) Increase the safety of personnel or reduce damage to equipment during use.

(2) Improve operational capability in response to user needs.

(3) Reduce the cost of production or operational support.

(4) Improve reliability, availability, and maintainability.

(5) Correct performance deficiencies.

(6) Improve rationalization, standardization, and interoperability(-RSI) compatibility or simplification.

(7) Comply with legislative requirements.

(8) Conserve energy.

b. The CBTDEV identifies the need for a product improvement and prepares user requirements documents. The DCSRDA has main Army General Staff responsibility for Army product improvements. The MATDEV programs and budgets funds to carry out the product improvement and evaluates and prepares the PIP, which provides the means for processing the product improvement.

c. To submit a PIP for approval, a PIP package must be prepared. It contains documents that clearly describe and fully justify all aspects of the proposed improvement. The documents include the following:

(1) DA Form 3701–R (Product Improvement Management Information Report (PRIMIR)), which is the basic document used to report on a PIP. The PRIMIR should contain a risk assessment for those PIPs coded safety and those PIPs whose primary purpose is other than safety but that include safety benefits. (See para 3–7.)

(2) An operating and support cost impact.

(3) A COEA or economic analysis/cost analysis.

(4) A test and evaluation master plan.

(5) A life-cycle cost analysis.

(6) A detailed technical description.

(7) An RSI and/or ILS impact statement.

(8) A modification application plan.

(9) Environmental documentation (AR 200–2).

(10) A detailed milestone plan.

(11) A statement of user representative concurrence. (See para 2–5.)

d. After an extensive review process, the PIP may be approved and funded by HQDA. To speed this process, a justification code is assigned to each PIP. The justification code is related to the reason for the PIP. "S" is the justification code for safety-related PIPs.

e. Once approved, a product improvement is completed in three phases.

(1) *Phase I, Engineering.* Actions include making an acquisition plan, estimating costs, planning tests, assembling a prototype, preparing a safety statement, planning new equipment training, and preparing a fielding plan.

(2) *Phase II, Procurement.* Actions include updating tasks in phase I, awarding a manufacturing contract or issuing a task order for in-house manufacturing, and procuring the modification kits needed to make the improvement.

(3) *Phase III, Application.* Actions include finalizing the materiel fielding plan, publishing the MWO, issuing the MWO kit to the field, and applying it to the equipment.

5–13. Modification work orders

a. The MWO, which is issued by the proponent of the system, prescribes the technical requirements along with the needed hardware for making the modification. The kits can be applied by a government contractor or by field units themselves; however, the proponent has ultimate responsibility for the satisfactory installation of the modification kits on the Army's inventory. All urgent MWOs must be applied on receipt of the kits since the equipment cannot be operated until the modification is complete. Limited-urgent MWOs will be applied as soon as possible, but not later than the time specified in the MWO.

b. The MWO, which provides the means for implementing a PIP, can be classified as follows:

(1) *Urgent.* Urgent MWOs receive the highest priority in the modification program; they immediately deadline all equipment affected until stated deficiencies are corrected.A modification (as well as a PIP) is classified as urgent when continued operation of the equipment will cause personnel injury, equipment damage, or security compromise.

(2) *Limited urgent.* Limited-urgent MWOs receive the second highest priority in the modification program. As in an urgent modification, continued operation of the equipment may result in injury or damage. However, the equipment may continue to be operated under predetermined restrictions for not more than 180 days after the MWO effective date.

(3) *Normal.* Normal MWOs are the third highest priority; they are issued for conditions that present no safety problems if left uncorrected.

c. Once the MWO kit is installed, the PIP proponent will collect and analyze data on its performance to verify that the improvement is working as intended. The SSWG should monitor these improvements to ensure that they do not inadvertently compromise safety. AR 385–16 also requires active involvement by the installation safety office to—

(1) Ensure that all urgent and limited-urgent MWOs are complied with in a timely manner. To accomplish this task, the safety office must maintain close liaison with the installation's MWO coordinator. The MWO coordinator usually works within the post's Directorate of Industrial Operations. Arrangements should be made for copies of all urgent and limited-urgent MWOs to be sent to the installation safety office for tracking purposes.

(2) Evaluate each MWO (or similar work request) to ensure precautions previously identified by the MATDEV are taken while the work is being done. To accomplish this task, unit safety personnel

must make an effort to inspect or observe the actual modification operation. The operation should be performed according to the modification procedure outlined in the MWO. This description explicitly defines the procedure and includes appropriate cautions and warnings about potential hazards. It is imperative that safety personnel ensure that these procedures are closely followed.

(3) Ensure through unit safety officers timely reporting of all urgent and limited-urgent MWOs. Once an MWO has been completed, it must be recorded on DA Form 2407 (Maintenance Request). This form is used to report applied MWOs can can also be used to request that a needed MWO be applied by support or contractor personnel.Unit safety personnel should ensure that these reports, and others prescribed in the MWO, are completed. These reports provide necessary documentation to verify that an MWO has been properly performed.The guidelines for reporting MWO applications for ground systems are found in DA Pam 738–750; aircraft systems are covered in DA Pam 738–751.

5–14. Safety-of-use messages

a. As required by AR 750–10, any unit or agency discovering an unsafe condition with Army equipment is responsible for notifying the commander of the proponent of the system. It is the proponent's responsibility to assess the situation to determine whether the unsafe condition is of an operational, technical, one-time inspection, or advisory nature. Once determined, the appropriate message is released.

b. The proponent will issue safety-of-use messages through the MACOM down to all users of the hardware, directing them to immediately check the equipment. These messages are of the following types:

(1) *Operational.* These messages are used to change operating procedures or impose limits on equipment users.

(2) *Technical.* These are sent to deadline equipment because of materiel or maintenance deficiencies. This type of message will require modification of the equipment or its parts or components.It must be published later as an urgent MWO.

(3) *One-time inspection.* This message immediately deadlines specified equipment. It directs that a procedure inspection of the equipment or its parts be done before its next use. The deadline period is usually that required for inspection. Equipment found to be deficient will remain deadlined until corrected. The original message will state corrections required or they will be published later as safety-of-use, one-time inspection, or technical messages.

(4) *Advisory.* The advisory message contains new operational or technical maintenance information essential for equipment operators or maintenance activities. Advisory messages neither deadline equipment nor direct the immediate accomplishment of a task.

c. Each installation safety office must ensure that it is on distribution to receive all safety-of-use messages that arrive on the installation. The safety office must monitor organizations that are affected by a message to ensure they are in compliance.With messages requiring a one-time inspection, the procedures and guidelines must be followed closely and documented appropriately before the equipment may be used again.

5–15. Safety-of-flight messages

a. Safety-of-flight (SOF) messages are similar to safety-of-use messages but apply to the aviation community. These messages are sent by the U.S. Army Aviation Systems Command to aircraft users to report any defect or hazardous condition, actual or potential, that can cause personal injury or damage to aircraft components.

b. SOF messages are classified as follows:

(1) *Emergency.* An emergency message immediately grounds a fleet of aircraft or a designated portion of a fleet of aircraft when a hazardous condition exists that has the potential to cause a catastrophic accident resulting in death of personnel or destruction of aircraft. These messages are for grounding purposes only. They will always be followed by another SOF message, urgent MWO, or urgent technical bulletin.

(2) *Operational.* This message may ground an aircraft for operational reasons, other than emergency, to correct hazardous conditions pertaining to aircraft operations. These may include flight procedures, operating limitations, or operational policy.

(3) *Technical.* A technical message may be issued to effect noncatastrophic grounding for materiel or maintenance conditions. This message can be an independent or a follow-up to an emergency SOF message. Required corrective action must be completed within the timeframe designated.

(4) *Maintenance mandatory.* This message will not ground aircraft, but it may require accomplishment of a task and require a report of completion of findings.

c. The installation safety office should monitor these messages in the same manner as safety-of-use messages to ensure compliance by aviation units that are affected.

5–16. Training

a. EIRs, PIPs, MWOs, and SOF and safety-of-use messages are used to either notify commands or initiate corrective actions to problems with Army materiel. Although a large part of system safety efforts concentrate on the actual hardware involved in a system or facility, emphasis must also be directed toward properly training personnel to operate and maintain these systems safely.

b. MATDEVs are responsible for collecting technical safety and health data throughout the life cycle of the system. This data, which provides basic knowledge of the system with its associated hazards, is used by the CBTDEV and the training developer in establishing training requirements. These requirements, which are incorporated into training circulars, plans, bulletins, and field manuals, are useful in training personnel to avoid the occurrence of hazards later in operation and maintenance. The development of operator and maintenance manuals (see para 3–13) also requires that the personnel interfacing with the system clearly identify and recognize potentially hazardous situations.

c. The safety of the system is intimately linked to the effectiveness of safety-related training and education.

(1) The installation safety office is responsible for monitoring training programs to ensure that they meet the user's needs. Such programs should include provisions for emergency training associated with handling the most critical or catastrophic hazards.

(2) Proper safety training requires units to train user personnel in how to handle emergency conditions using methods that have been established by the training developer. This type of training and practice may bring about changes that will enhance the system of handling both routine and emergency situations. If inadequate, the training developer should be informed.

Appendix A
References

Section I
Required Publications

AR 70–1
System Acquisition Policy and Procedures. (Cited in paras 1–10*d*, and 4–10*a*.)

AR 385–16
System Safety Engineering and Management. (Cited in paras 1–10*g*, 3–3*a*, 5–1*a*, 5–3*a*,5–5*b*, and 5–13*c*, and apps B and E.)

DA Pam 11–25
Life Cycle Management Model for Army Systems. (Cited in para 2–1*a* and app C.)

MIL–STD–882B
System Safety Program Requirements. (Cited in para 1–8*a*and apps B, C, E, and F.)

Section II
Related Publications

A related publication is merely a source of additional information.The user does not have to read it to understand this regulation.

AR 15–14
Systems Acquisition Review Council Procedures

AR 40–5
Preventive Medicine

AR 40–10
Health Hazard Assessment Program in Support of the Army Materiel Acquisition Decision Process

AR 70–9
Army Research Information Systems and Reports

AR 70–10
Test and Evaluation During Development and Acquisition of Materiel

AR 70–17
System/Program/Project/Product Management

AR 70–61
Type Classification of Army Materiel

AR 71–3
User Testing

AR 71–9
Materiel Objectives and Requirements

AR 95–18
Aviation Safety-of-Flight Messages

AR 200–2
Environmental Effects of Army Actions

AR 385–10
Army Safety Program

AR 385–40
Accident Reporting and Records

AR 385–62
Regulations for Firing Guided Missiles and Heavy Rockets for Training, Target Practice and Combat

AR 385–63
Policies and Procedures for Firing Ammunition for Training, Target Practice and Combat

AR 385–95
Army Aviation Accident Prevention

AR 415–15
Military Construction Army (MCA) Program Development

AR 602–1
Human Factors Engineering Program

AR 602–2
Manpower and Personnel Integration

AR 672–20
Incentive Awards

AR 700–51
Army Data Management Program

AR 700–127
Integrated Logistic Support

AR 702–3
Army Materiel Systems Reliability, Availability, and Maintainability(RAM)

AR 715–6
Proposal Evaluation and Source Selection

AR 750–10
Modification of Material and Issuing Safety-of-Use Messages

DA Pam 385–1
Unit Safety Management

DA Pam 385–95
Aircraft Accident Investigation and Reporting

DA Pam 738–750
Functional Users Manual for the Army Maintenance Management System

DA Pam 738–751
Functional Users Manual for the Army Maintenance Management System—Aviation

DI–A–3027A
Data Accession List/Internal Data

DI–H–1327A
Surface Danger Area Data

DI–H–1332A
Radioactive Material Data

DI–H–1336
Noise Measurement Report

DI–R–1710
Quality Program Plan

DI–R–1730
Reliability Program Plan

DI–R–1731
Reliability Reports

DI–R–1734
Reliability Failure Modes, Effects, and Criticality Analyses Report

DI–R–1740
Maintainability Program Plan

DI–R–1741
Maintainability Report

DI–R–7039
Report, Failed Item Analysis

DI–SAFT–80100
System Safety Program Plan

DI–SAFT–80101
System Safety Hazard Analysis Report

DI–SAFT–80102
Safety Assessment Report

DI–SAFT–80103
System Safety Engineering Report

Data Item (DI) publications may be obtained from the Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, PA 19120.

DODI 5000.36
System Safety Engineering and Management

MIL–STD–470A
Maintainability Program for Systems and Equipment

MIL–STD–490
Specification Practices

MIL–STD–1294
Acoustical Noise Limits in Helicopters

MIL–STD–1474B
Noise Limits for Army Materiel

MIL–STD–13881A
Logistic Support Analysis

MIL–STD–13882A
Requirements for a Logistic Support Analysis Record

System Safety Analysis Techniques, Safety Engineering Bulletin No. 3–A, Nov 1983
This bulletin may be obtained from the Electronic Industries Association, Engineering Department, 2001 Eye Street, N.W., Washington, DC 20006.

Technical Report ASSAC–TR, System Safety Procedures for Nondevelopmental Item (NDI) Acquisitions, U.S. Army Armament Research and Development Center, August 1985
This report may be obtained from U.S. Army Armament Research and Development Center, Dover, NJ 07801–5001.

Guide to Aviation Resources Management for Aircraft Mishap Prevention
This guide may be obtained from U.S. Army Safety Center, ATTN:PESC–M, Fort Rucker, AL 36362–5363.

TECOM TOP 10–2–508
Safety and Health Hazard Evaluation—General Equipment

Section III
Referenced Forms

DA Form 285
U.S. Army Accident Investigation Report

DA Form 2397–R–series
Technical Report of U.S. Army Aircraft Accident

DA Form 2407
Maintenance Request

DA Form 2696–R
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 should be broad in scope. Although the list provided in table 1–1 is neither sequential nor complete, it can be used as a check against omission of important tasks.

b. Every charter should contain a task to develop a System Safety Management Plan. The SSMP should contain the specific tasks necessary to accomplish the broad ones listed in the charter. (See fig B–1.)

B–6. Operation
a. Membership. Membership should be divided into principal and advisory members. Membership should be confined to organizations rather than individuals. Principal members should attend every meeting of the SSWG and advisory members only when invited.

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

c. Administration. Describe procedure for developing agendas, preparing minutes, and making formal recommendations to the PM. Minority opinions as well as consensus should be forwarded to the PM. Provisions should be made for updating the charter.

B–7. Time period
Specify the period of time for which the SSWG is chartered.

System Safety Working Group Charter

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

2. Scope. The *(system name)* System Safety Working Group 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), (MACOM).*4. References.

a. AR 385–16: System Safety Engineering and Management, 3 Sep 85.

b. MIL–STD–882B: System Safety Program Requirements, 30 Mar 84.

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 ROC and letters of agreement.

b. Review and evaluation of the best technical approach.

c. Recommendations to the *(system name)* PM for establishing new or revised requirement in light of existing system safety.

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)* Request for Proposal.

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 hazard tracking system to identify, eliminate if possible, rank, estimate a likelihood of occurrence, and track hazards throughout the life cycle of the program. Recommendation for corrective action should 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 (or representative)during safety reviews at the contractor's facility, in the review of system safety analyses generated by the requirements of the *(system name)* system safety program. Comments or recommendations for corrective action should be provided to the *(system name)*PM as appropriate.

m. Development of a preliminary hazard list.

n. Collection and evaluation of lessons learned pertaining to *(system name)* system safety.

6. Operation.

a. Membership.

(1) Principal members will be appointed from the following organizations:

(a) *(System name)* PM's office.

(b) Local safety office.

(c) Engineering representative.

(d) *(MACOM safety offices (MATDEV, CBTDEV, and/or user)).*

(e) CBTDEV safety representative.

(f) MANPRINT representative.

(g) Installation safety manager, if applicable.

(h) Prime contractor's system safety manager.

(2) Advisory members will be appointed from the following organizations:

(a) User test organization.

(b) *Representatives from MACOMs developing subsystems.*

(c) *(Technical test organization.)*

(d) *(Developmental independent evaluator.)*

(e) *(Operational independent evaluator.)*

(f) *(U.S. Army Human Engineering Laboratory.)*

Figure B-1. Sample of a system safety working group charter—Continued

(g) *(Other organizations as may be necessary.)*

(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 U.S.Army Safety Center. 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. 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 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 hazard tracking system and recommendations for their elimination or mitigation will be provided to the PM.

(5) SSWG recommendations to the PM will include minority opinions as applicable.

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

Figure B-1. Sample of a system safety working group charter

Appendix C
System Safety Program Plan

C–1. Introduction

a. This appendix contains detailed guidance for evaluating a system safety program plan or preparing a requirement for an SSPP in a request for proposal. It provides guidance for defining what data should be placed in each section of the SSPP.

b. The format and content of an SSPP, dictated by Data Item Description (DI–SAFT–80100), is shown in table C–1. Paragraphs C–2 through C–12 correspond to and describe these eleven sections. Each section contains information to supplement MIL–STD–882B and DI–SAFT–80100.

Table C–1
System safety program plan format per DI–SAFT–80100

Section number: 1 **Title:** General Program Requirements
Section number: 2 **Title:** System Safety Organization
Section number: 3 **Title:** System Safety Program Milestones
Section number: 4 **Title:** System Safety Requirements
Section number: 5 **Title:** Hazard Analyses
Section number: 6 **Title:** System Safety Data
Section number: 7 **Title:** Safety Testing
Section number: 8 **Title:** Training
Section number: 9 **Title:** Audit Program
Section number: 10 **Title:** Mishap Reporting and Investigation
Section number: 11 **Title:** System Safety Interfaces

c. The SSPP is a detailed description of both system safety management and engineering tasks necessary to address system-related hazards. The requirement for an SSPP is valid for both in-house developmental items and efforts that are contracted out. The responsibility for having an SSPP prepared will be the organization that is responsible for overall project development.

(1) The SSPP is normally valid for a specified period of time. This time period is associated with a particular phase of the Army system life cycle because separate contracts are awarded as development of equipment proceeds through each phase of the life cycle. For example, a contract is awarded to develop a prototype during the validation phase, another contract is awarded to develop hardware and software during full-scale engineering development, and still another contract is awarded when the equipment enters the production phase.

(2) As development progresses from one phase of the life cycle to the next, the new contract may specify that the SSPP prepared from the former contract simply be revised to meet the requirements of the new contract.

d. The requirement for the SSPP is outlined in the RFP and will be designed to require the contractor to prepare the SSPP and deliver it to the Government as a part of the contractor's proposal.

(1) Specifically, this early preparation and delivery of the SSPP is accomplished by the contracting officer inserting the requirement into the "Instructions to Offerers" section of the RFP.This approach is recommended because competition among contractors at this point results in the best possible SSPP and because this document will be available for program evaluation and approval during source selection.

(2) DI–SAFT–80100 should be listed in the contractor data requirements list (CDRL) to provide formal guidelines to the contractor.Provisions for updates to the SSPP after contract award should also be included in the CDRL, since preparation and delivery of the SSPP is recommended prior to actual contract award.

(3) All instructions involving preparation and delivery of the SSPP must be clearly stated in the RFP. Major system safety tasks can be required of the contractor by listing the desired tasks in the RFP. The MATDEV should tailor the list of tasks in MIL–STD–882B based on recommendations from his or her SSWG.

(4) The SSPP should be delivered to the Government by the contractor with his or her proposal and should be made contractually binding. This is accomplished by placing the SSPP as a line item in section B of the contract. Each proposal should be evaluated for this requirement.

C–2. General program requirements

a. Scope.

(1) Requirements in MIL–STD–882B are designed to be tailored for each life-cycle phase of every system under development. The actual tailoring of MIL–STD–882B should be accomplished in this section.If specific tasks from MIL–STD–882B were required in the RFP, the SSPP should be checked to ensure those requirements were incorporated into the contractor's system safety program.

(2) Another item that should be included in this section is to provide for revision of the SSPP. The SSPP cannot be allowed to stagnate. The design requirements and schedule of the system being developed can be expected to change because of continuous assessment of the threat and innovations and handicaps involving technology.The SSPP must be periodically reviewed and revised accordingly.

(3) The SSPP need not repeat portions of a program documented elsewhere, either in a proposal or a contract. Conversely, the SSPP must be closely coordinated with many other program elements for it to be effective. To ensure completeness and foster the usefulness of an SSPP, a cross-reference system should be included in the documentation.Some companies make a practice of listing all paragraph numbers from the RFP and then list the corresponding paragraphs in their proposal that answer each RFP requirement. An extension of this practice will also include in the SSPP a cross-reference section that lists other portions of the documentation having system safety implications.

b. Purpose. The basic purpose of a system safety program is to ensure that the system safety concept is effectively integrated into the total design and that maximum performance of the system is realized without degradation in system safety. The system safety program must have a reasonable prospect of achieving tangible benefits in the development project. Every provision in the SSPP must be related to some beneficial aspect of the overall program. The SSPP is a basis of understanding between the contractor and the MATDEV as to how the system safety effort will be accomplished.

c. Objective. Objectives are not included in the RFP but may be listed in the contractor-prepared SSPP. These objectives must be modified to be consistent with specific system development program features. The contractor is responsible for further refinement and modification of these objectives to fit the specific activities of the system safety program.

d. Definitions. The definitions in MIL–STD–882B are normally placed verbatim by the contractor in the SSPP. However, the contractor may use different definitions. In this event, the MATDEV should review these definitions.

e. Referenced documents.

(1) A list of all documents referenced in the safety portion of the statement of work must be provided to the organization preparing the RFP. The safety documents will be included in a comprehensive list of all documents referenced in the SOW. (See MIL–STD–490.)

(2) Occasionally, internal company documents are used as references for an SSPP. Care must be taken that internal company documents do not replace Government specifications and standards unless a statement is included indicating that specifications in company documents meet or exceed all specifications in required Government documents. In such cases, the company documents should be furnished to the Government for review.

C–3. System safety organization

a. Safety organization.

(1) A special effort must be made in depicting the system safety organization in the SSPP to illustrate how that organization actually integrates into the company's overall development program.This is particularly important because every program activity must involve system safety.

(2) Often a contractor organizes the system safety effort as a component of another discipline. Placing system safety with reliability, for example, is common. When this is done by a contractor, the job of the MATDEV becomes more difficult because of the problem of verifying that resources dedicated to safety by the contractor will indeed be applied to system safety. (See para C–12 for additional comments.)

(3) The contractor's safety engineering organization may be responsible for the system safety effort on several contracts.For this reason, the RFP should contain a requirement that a list of all functions for which the contractor's system safety organization is responsible be placed in the SSPP. If the system safety organization is responsible for other safety efforts or other disciplines (such as human factors and reliability), then a bookkeeping system must be established by the contractor to ensure that this project is provided with the level of effort indicated in the proposed SSPP.

(4) If all effort is concentrated in the program/project element, this may be an indication that the system safety effort is being organized only in response to RFP requirements and is intended to interface with well established company procedures only to the minimum extent possible. One acceptable procedure to preclude this is to provide a working group for system safety within the design engineering element and have this group receive program direction and control from the program engineering managers. The contractor's system safety group's functions, responsibilities, and authority must be clearly defined.

(5) An SSWG composed of Government and contractor personnel participating in various safety-related activities for a major development effort may be organized by the Government. This SSWG is recognized through a charter issued by the PM's office. Each member of the SSWG will be placed on distribution for the hazard analyses prepared by the contractor and be notified of all major design reviews. The SSWG, which is organized by the Government, is discussed in this section because industry participation in this group is vital for its success.

(6) The terms used to describe the organization and its functions must be consistent and accurate. For example, industry often refers to a design engineering group as merely "design." Such terminology is confusing because it is not always clear whether a function or organizational element is being discussed.

b. Personnel qualifications. Specific minimum qualifications are provided in MIL–STD–882B, Task 108. The RFP should not require the contractor to incorporate personnel qualifications as part of the SSPP, but an important evaluation item is whether the contractor's personnel are qualified to do the job they propose. The qualifications of safety managers should be carefully evaluated, particularly if the system safety effort is managed as a component of another discipline.If the contractor provides personnel qualifications, they should be placed in supporting documentation, not in the SSPP, since personnel and qualifications change.

c. Safety organizations interface. Safety organization interface within corporate organization.

(1) The methodology that the contractor will use to integrate and coordinate system safety efforts should be evaluated. This evaluation should include—

(a) Distribution of the system safety requirements to action organizations and subcontractors.

(b) Coordination of subcontractor's system safety programs.

(c) Integration of hazard analyses.

(d) Program and design reviews.

(e) Program status reporting.

(f) Contractor system safety groups.

(2) The "chain of command" for contractor management decisions should be identified and evaluated. The final authority within the contractor's organization for hazard closure and risk acceptance should be identified. This authority should be given to one individual at a sufficiently high level within the organization to authorize funding for hazard resolution activities.

(3) Subcontractor interface is discussed in paragraph C–12 below and in Task 102 of MIL–STD–882B.

C–4. System safety program milestones

a. Milestone identification. Milestones are formally designated points in a program that are chosen for their prominence.Overall program milestones will likely be specified by the Government in an RFP. System safety milestones should be established to permit evaluation of the effectiveness of the system safety effort. Specific items to be checked for are start and completion dates and manloading.Manloading is of particular importance because it contractually binds the contractor to a specific level of system safety effort if the SSPP is approved.

b. Safety task schedule.

(1) In this section of the SSPP, the contractor documents the detailed tasks and their sequence necessary to implement the system safety program. Any task that is performed in a system safety program must be related to overall program activities and milestones. There must be a valid reason to perform each task, and the sequence must reflect a logical progression of activities that result in program milestones being attained.

(2) Historically, this part of an SSPP has been one of the weakest because tasks have not been defined in detail, and their sequencing has been unrealistic or unrelated to accomplishment of overall program milestones. If system safety tasks are not related to other essential program activities, the system safety program cannot be a coordinated, integrated effort.

(3) The Government will stipulate requirements for a system safety program in an RFP in as much detail as possible. There will be some requirements included that can even be classified as tasks, which the contractor must include in the SSPP. However, the contractor is not limited to just those tasks that may be prescribed by the Government.The contractor must fully develop his or her own system safety program to the extent that additional tasks are defined, completely and logically establishing the activities of the overall program.

(4) Many safety activities in the past have been characterized by an over-generalized approach to the solution of safety problems.The only way to solve the complex problems of accident prevention is to analyze the basic details of the situation and work out the problems at that level.

(5) Dealing effectively with this much detail in a development program demands that a systematic and coordinated procedure be developed.The tasks established for a system safety program must reflect this mandatory detail and scope.

(6) DA Pamphlet 11–25 lists many activities to be conducted during the various phases of a system life cycle. In addition, table 1–1 of this pamphlet contains a list of Government tasks. While the list is neither all-inclusive nor sequential, nor are all the items shown applicable for every program, the list serves as a check against omission of important program tasks.

(7) As system concepts and functions are identified, safety studies will be performed to determine the adequacy of design concepts to meet the essential safety characteristics of the system. These studies also will—

(a) Evaluate technical approaches to system safety design features.

(b) Identify possible safety interface problems.

(c) Highlight special areas of safety consideration, such as system limitations, risks, and man-rating requirements.

(d) Define areas requiring further safety investigation, and describe safety tests on data needed from exploratory or advanced development activities.

C–5. System safety requirements

a. Standards and specifications list. All safety design requirements contained in the RFP should be listed in this section of the SSPP. The contractor's safety personnel should be aware of all safety-related design requirements. Safety design standards and specifications with which the contractor intends to comply should also be listed. This is a critical SSPP evaluation area. One of the major goals of the contractor's program should be to incorporate safety design features; this section of the SSPP outlines how this is to be done.

b. Hazard risk indexing procedures. Risk indexing procedures are outlined in detail in paragraph 1–9 and in MIL–STD–882B.The MATDEV should ensure the contractor plans to derive a hazard risk index based on both severity and probability.

c. Hazard resolution procedures.

(1) The description of control and closed-loop procedures to ensure hazard resolution is one of the most important parts of the SSPP. Recommended action on identified hazards are provided in MIL–STD–882B; however, the methodology outlined in chapter 1, section II, of this pamphlet should be reviewed.

(2) The contractor needs to outline a similar procedure for hazard resolution and risk management in the SSPP. A hazard tracking system should be established. In evaluating the contractor's method, it is most important to check whether the contractor intends to attempt to resolve all hazards or only those of a certain risk level. For example, a contractor may propose to attempt hazard resolution activities only on hazards categorized as critical or catastrophic. Risk reduction and resolution activities should occur on every hazard. The format shown in appendix F is recommended for use as a record of the risk resolution process. The final approval authority identified in section 2 of the SSPP should be the last signatory.

C–6. Hazard analysis

a. Development of hazard analysis requirements in the RFP is an important function. Hazard analyses are the single most important activity performed by system safety personnel because they are the principal means of hazard identification. Most of the elements of the contractor's system safety program will eventually be reflected in the quality of hazard analysis reports.

(1) Various analyses exist that may or may not be appropriate for a particular system. A common shortcoming is to allow one type of analysis to exceed the scope and purpose for which it was designed-.No single analytical technique will satisfy all system safety requirements.

(2) Guidance for selection of hazard analyses is included in this paragraph and in MIL–STD–882B, Tasks 202 through 205. If checklists are to be used by the contractor, they should be listed in section 1 of the SSPP under "Referenced Documents" and approved by the Government.

b. Hazard analyses are normally scheduled to be delivered to the Government in relation to program milestones and not calendar dates. Program milestones are often delayed because of technology or cost problems encountered. Tying delivery of hazard analyses to program milestones will—

(1) Make available to the contractor's safety personnel the latest design data for the hazard analyses.

(2) Preclude premature submission of a safety report to the Government.

c. From the contractor's point of view, hazard analyses are due a given number of days prior to program milestones. Normally, informal suspense placed on the contractor's safety engineer is another 30 days so that the analyses may be typed and coordinated. Of course, the contractor's safety engineer must complete the hazard evaluation at least a week prior to the internal suspense so data may be reviewed and placed in the proper format. Therefore, a 10-week period is encountered between the conclusion of the safety evaluation and the program milestone.This time period is excessive. The Government system safety manager should recognize this problem and deal with it on a case-by-case basis.

(1) Government audits to ensure that the contractor's safety engineer has current design data for the hazard analyses should be conducted.

(2) Should the audit reveal that design scheduling will not permit an adequate hazard evaluation, the delivery of the hazard analyses can be delayed by request of the Government system safety manager through the contracting officer and/or the PM.

d. Another problem that may be encountered is a ceiling imposed on the number of data items that may be required in a contract.The PM or the contracting officer may establish a quota on the number of data items that each support group may request in order to meet the limitation. Under these special conditions, a safety assessment report (DI–SAFT–80102) can be used to summarize hazard analyses or as the only formal documentation of safety program activities/ hazard assessment. (See para C–7*d*(1).)

e. Types of hazard analyses.

(1) *Preliminary hazard analysis (PHA).* A PHA or PHL identifies anticipated hazardous components or operations for the total system. The use of historical safety performance data from similar systems is important. Several data sources for PHAs and PHLs are listed in paragraph 2–3.

(a) 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. The PHA or PHL should provide the basis for the hazard tracking system used by the SSWG.

(b) The contractor should be required in the RFP to perform a PHA on the proposed design. The PHA, when required, will be the first hazard analysis performed by the contractor, and it should be delivered to the Government per DI–SAFT–80101. The PHA is not necessary during full-scale development that was preceded by development of a prototype that had a system safety program that included deliverable hazard analyses.

(c) Delivery of the PHA may be established for some time period after contract award (for example, 60 days after contract award), or delivery may be required prior to a predesignated program milestone (for example, 30 days before the preliminary design review).The MATDEV will select the method that best integrates into its system safety program.

(2) *Subsystem hazard analysis (SSHA).* Subsystem hazard analyses are performed on each subsystem of the overall system. They are the most detailed analyses performed on the components of the system.

(a) Each SSHA must be conducted in close coordination with the design effort of each subsystem; therefore, analysis of the subsystems is usually specified in the RFP and performed by the contractor.

(b) Delivery of both the initial and final SSHAs should be scheduled relative to pre-established program milestones so delivery will be automatically adjusted to program slippage. When the preliminary design is revised, the affected portion of the SSHA must be updated accordingly.

(c) By the time all SSHA tasks have been completed, every part of the system will have been considered individually. The subsystem breakdown will be at the contractor's option. The MATDEV may wish to list the subsystems to be analyzed to ensure subsystem breakdown is functionally organized. Instructions on when they should be performed are contained in data item descriptions (DIDs), the AMC System Safety Engineering Handbook, and the Electronic Industries Association's Guide.

(d) Following are examples of the types of SSHAs that are possible:

1. Fault hazard analysis—detailed investigation of the subsystem to determine component hazard modes, causes, and effects.

2. Fault tree analysis—analysis of all events, faults, and occurrences and all their combinations that could cause or contribute to

the occurrence of defined undesired events. The Fault tree analysis is performed by the contractor and is quite manpower intensive due to the complexity of the analysis technique. If deemed necessary, it should be required in the RFP.

3. Sneak circuit analysis—identification of latent electrical, hydraulic, or other control system conditions that could cause undesired functions or inhibit desired functions. This analysis is also manpower intensive and performed by the contractor when required in the RFP.

4. Software safety analysis—examination of the critical functions of a computerized system to ensure that a deviation from proper routine or an improper routine will not result in a hazard.

5. Safety requirements analysis—used to identify and ensure compliance with safety design requirement codes, specifications, or standards.

(3) *System hazard analysis (SHA).* This analysis examines subsystem interfaces to determine the effect of failure and normal operating modes on safe system operation.

(a) The SHA identifies hazards that surface during integration of the subsystems. Examples of such hazards include contact of incompatible metal when subsystems are brought together, electromagnetic interference, transportability, and electrical grounding. The SHA will also identify hazards associated with the total system. Hazards relating to stability and control of a mobile system is an example.The format for the SHA may be similar to the fault hazard analysis.Delivery of the SHA should be relative to program milestones so delivery dates will be automatically adjusted when program schedules are slipped.

(b) Analytical techniques available for conducting an SHA are the fault hazard analysis, fault tree analysis, or sneak circuit analysis. They are powerful tools for uncovering problems with the interface between subsystems.

(4) *Operating and support hazard analysis.* The O&SHA identifies hazards relating to the operation and maintenance of the system. The O&SHA will list hazards to personnel who must be included as part of the system and addresses system hazards induced by personnel actions. Examples of hazards that could be included in the O&SHA are refueling operations, nonionizing radiation, and electrical capacitance. (See para 3–15 for a discussion on human factors interface with system safety.)

(5) *Maintenance analysis.* The maintenance analysis used by the maintainability program is an excellent source of input for the O&SHA. The output of the maintenance analysis, reported using the Maintainability Report (DI–R–1741), can be used as direct input to the O&SHA.

(a) Delivery of the preliminary O&SHA should be scheduled prior to the first system test.

(b) Delivery of the final O&SHA should be scheduled prior to publication of equipment manuals but not before completion of the maintenance analysis.

(c) Copies of the report should be furnished to the testing activities, the office preparing the manuals, the organization responsible for new equipment training, and the human factors engineering organization. (See para 3–15 for additional comments.)

(6) *Failure modes and effects criticality analysis.* The FMECA, performed by reliability engineering, can be used to satisfy that part of the SSHA dealing with equipment failures.However, it is inadequate for the identification of hazards resulting from personnel error and environmental and procedural deficiencies.The use of FMECA is only partially adequate for the identification of hazards resulting from design characteristics. The FMECA should not be scheduled for delivery prior to the SSHA.

(7) *Safety trend and deficiency analysis.* Accident and incident data, failure reports, QDRs, and EIRs are analyzed in developing engineering change proposals or product improvement proposals. (See chap 5, section III.)

C–7. System safety data

a. Historical data. Contractor intentions to use historical data should be evaluated. Data sources are listed in paragraph 2–3.

b. Deliverable data. Each contract requiring data contains a CDRL, which lists the data the contractor will be required to deliver (excluding Federal Acquisition Regulation clauses).

(1) The CDRL is the only contractual authority for delivery of data. Therefore, the requirement for submission of data is not placed in the work statement specifications. The CDRL will be completed per AR 700–51.

(2) After each interested office responds to the "data call" with its required data items, duplicate or overlapping data requirements are eliminated by the Data Requirements Review Board.A safety representative should serve on this board. A data call will be issued to begin preparation of the RFP for a given project.

(3) When the PM determines that system safety data should be a part of the contractual effort, the following two actions are required:

(a) Preparing DD Form 1423 (Contract Data Requirements List) for incorporation into the CDRL.

(b) Checking appropriateness of data using a "specification tree." The purpose of the specification tree is to limit the scope of work through a tailoring process. It is set up like a flow chart.Place specifications that the contractor is required to comply with on the branches of the tree. For example, the contractor may be required to comply with paragraph 9a of MIL–STD–XXXX; but, paragraph 9a may reference two other specifications. These two specifications should then be listed on the secondary branches of the tree and so on. This process identifies inappropriate requirements that may be placed on the contractor through specifications that are"hidden" inside other specifications.

c. Non-deliverable data.

(1) All safety data not delivered to the Government will be maintained by the contractor. Often a contractor uses in-house work sheets to perform the hazard assessment and then uses portions of this data to develop the report for the deliverable data item.The MATDEV will require that the contractor make in-house data available to Government personnel during on-site visits or audits.From a management point of view, access to all data is the only method to ensure the contractor is providing the required level of effort. From a technical point of view, hazard analyses sometimes include only identified hazards and do not include areas not considered a hazard. The Government needs to be assured that the contractor has considered all areas and can identify those that had no hazards.Such concerns may be resolved through—

(a) Audits of the contractor's non-deliverable data.

(b) Participation by the Government system safety manager in the design review.

(c) Active involvement and interface between an SSWG and the contractor.

(2) The Government system safety manager should inspect the RFP for the Data Accession List/Internal Data (DI–A–3027).The contractor publishes in this list all actions with which he or she is involved for a period of time. Non-deliverable data are itemized on this list. If the system safety manager is aware of non-deliverable safety-related data, he or she must ensure that the SSPP allows for Government inspection of the non-deliverable data.

d. Safety reports. In addition to hazard analysis reports (para C–6*e*), the following special reports are usually required of the contractor.

(1) *Safety Assessment Report, DI–SAFT–80102.* This report is a comprehensive evaluation of the safety risks being assumed prior to test or operation of the system or at contract completion. It identifies—

(a) All safety features of hardware and system design.

(b) Procedural hazards that may be present in the system being acquired.

(c) Specific procedural controls and precautions that should be followed. (See para 4–3.)

(2) *System Safety Engineering Report, DI–SAFT–80103.* This report addresses safety impact in an ECP, background information for waivers, and progress reports on the contractor's system safety program. The requirement for the progress report is often deleted when the SSPP includes sufficient audits and information exchanges to monitor the contractor's safety effort.

(3) *Surface Danger Area Data, DI–H–1327A.* This data item is required when guns, rockets, or lasers are to be used during system test.A copy of the report will be forwarded to the test activity. The delivery of the report will be scheduled prior to government tests. The data item is not adequate for most cases. Basically the contractor should provide data so test ranges can be established, but also so that training ranges may be established later during the program. Requirements for training ranges are included in AR 385–62 and AR 385–63.

(4) *Radioactive Material Data, DI–H–1332A.* This data item is required for systems that contain radioactive material and is a feeder document for type classification actions. Delivery is normally 90 days after contract award with updates as necessary.

(5) *Noise measurement Report, DI–H–1336.* The noise limits will be listed in a clause in the RFP. (See MIL–STD–1474B or MIL–STD–1294.)The data item is used to ensure the system complies with established design requirements.

C–8. Safety testing

a. Evaluations of the safety and health characteristics of each item and system should be conducted throughout all contractor testing, technical testing, and user testing. The testing will provide determinations or assessments of personnel and equipment hazards inherent in the system and associated operation and maintenance hazards.

b. Evaluation of the SSPP should focus on the adequacy of contractor testing and on contractor support available to the Government during technical and user testing conducted by the Government.

c. Pertinent data from all tests should be used as the basis for evaluating safety and health characteristics. In addition, specific safety tests will be performed on critical devices or components to determine the nature and extent of hazards presented by the materiel.

(1) Particular attention should be given to identifying and evaluating special safety and health hazards presented in paragraph 3–16*b*.

(2) Attention should also be given to evaluating the adequacy of hazard warning labels on equipment, and warnings, precautions, and control procedures in equipment publications. Although not normally included during system tests, identification of hazards that result from failure of the operator to follow the operators manual is useful information.

d. Data from the O&SHA can be used to develop test requirements in the technical and user test plan. Conversely the test and incident reports from technical and user testing can be used as input into updates of the O&SHA that will be beneficial in preparing operators manuals and identifying warnings and cautions for system manuals.

C–9. Training

a. This portion of the SSPP contains the contractor's plan for using the results of the system safety program in various training areas. Often hazards that relate to training are identified in the SAR or the O&SHA. Consequently, these two reports should be furnished to the office preparing the new equipment training plans.

b. The system safety program will produce results that should be applied in training operator, maintenance, and test personnel. This training should be continuous, conducted both formally and informally as the program progresses. Such training—

(1) Will be applied initially to contractor personnel engaged in the development program.

(2) Should be continued in contractor training of military personnel in the latter stages of development and early in the deployment phases.

(3) Provide useful input to training programs conducted by the military and the training of technical representatives working with military agencies.

c. The SSPP should also address training devices. The system safety program should monitor the effect of design changes on system maintenance trainers, flight simulators, and mission training simulators.

d. Two potential pitfalls in preparing this section of an SSPP should be pointed out. Since the subject of training is so broad, care must be exercised to restrict this paragraph to only the essential elements of training related to the SSPP. If more elaborate or detailed documentation is deemed appropriate, it should be included as an appendix to the SSPP or provided as a separate document. The tendency to include many industrial safety aspects in this paragraph should also be avoided.

C–10. Audit program

The contractor will describe techniques and procedures for ensuring accomplishment of the objectives and requirements of the system safety program. Specific elements of an audit program by the prime contractor should include on-site inspection of subcontractors, an accurate man-hour accounting system, and traceability of hazards.

C–11. Accident reporting and investigation

a. The contractor should be required to notify the Government immediately in case of an accident. The details and timing of the notification process should be addressed.

b. The SSPP should define the time or circumstances under which the Government assumes primary responsibility for accident investigation. The support provided by the contractor to government investigators should be addressed.

c. The process by which the Government will be notified of the results of contractor accident investigations should be spelled out. Provisions should be made for a Government observer to be present for contractor investigations.

C–12. System safety interfaces

a. Integration of associated disciplines. Since the conduct of a system safety program will eventually touch on virtually every other element of a system development program, a concerted effort must be made to effectively integrate support activities. Each engineering and management discipline often pursues its own objectives independently, or at best, in coordination only with mainstream program activities such as design engineering and testing. (See chap 3, section III, for comments on system safety interface with various support activities.)

b. Integration with other major systems.

(1) *Subcontractor/vendor/supplier system safety programs.* To ensure that the system safety program for a development program is comprehensive, the contractor must impose requirements on subcontractors and suppliers that are consistent with and contribute to the overall system safety program.This part of the SSPP must show the contractor's procedures for accomplishing this task. The prime contractor must evaluate variations and specify clear requirements tailored to the needs of the system safety program.

(a) These requirements will range from minor system safety activities(such as for a vendor supplying nuts and bolts according to a well-established military specification) to the preparation and implementation of a full system safety program for a major subsystem.

(b) Variations will depend on the degree of complexity involved and the amount of actual design effort required of the subcontractor.

(2) *Integration of other system safety programs.* Occasionally, the Government procures subsystems or components under separate contracts to be integrated into an overall system. Each subsystem contract should include implementation of a system safety program.

(a) The integration of these programs into the overall system safety program is normally the responsibility of the prime contractor for the overall system. When the prime contractor is to be responsible for this integration, it must be called out specifically in the RFP. This subparagraph of the SSPP should indicate how the prime contractor plans to effect this integration and what procedures will be followed in the event of conflict.

(b) The Government system safety manager should be aware that the prime contractor is not always responsible for integration of the

system safety program. For example, in some major system developments, the Government is the system safety program integrator for several associate contractors.

c. Miscellaneous system safety activities. The following items are not covered elsewhere in the SSPP; the contractor must adapt this list to the particular requirements of the system safety program:

(1) Ground handling.

(2) Storage.

(3) Servicing.

(4) Transportation.

(5) Facilities.

(6) Support requirements.

(7) Government-furnished equipment. When GFE is involved, Government policy states that the GFE will be used only on contractor "premises."Contractor premises should be defined in section H of the contract.

Appendix D
Preliminary Hazard List/Analysis

D–1. General

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 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. This involves discovering problems known through past experience on similar systems 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 will have to comply.

e. Recommended corrective actions.

Program: _____

System: _____

Part	Hazard	Cause	Effect	Hazard Category	Corrective or Preventive Action

Figure D-1. Format of preliminary hazard analysis (typical)

D–3. Sources of data

Historical safety information can be obtained from predecessor systems.(See para 2–3.)

D–4. PHA chart

There are several formats that may be used when performing a PHA. Figure D–1 typifies a functional PHA format.

D–5. Instructions for completion of the PHA

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.

a. 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.

b. The facility should then be broken down into subsystems or component operations. Once this is completed, the PHA chart may be completed.

(1) *Hazard.* Hazards are defined as conditions that are prerequisites to mishaps; 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, noises, exposure to toxic substances, health hazards, fire, lightning, and radiation.

(d) Operating, test, maintenance, and emergency procedures such as human factors engineering; human error analysis of operator functions, tasks, and requirements; effect of factors such as equipment layout, lighting requirements, potential exposures to toxic materials; 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.

(2) *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 workplace monitoring to detect carbon monoxide levels.

(3) *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.

(4) *Hazard category.* This is the assigned risk assessment code, which is a determination of the hazard's severity and probability of occurrence. (See para 1–9.) For this example, a RAC of 2A would

be assigned based upon the high severity and probability factors associated with this hazard.

(5) *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 Management Plan

E–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.

E–2. System safety organization (see fig E–2)

a. Program management office.

b. Integration of associated disciplines.

E–3. Tasks

The specific tasks to accomplish the objectives in figure E–1, paragraph 1d, should be listed with the responsible action agency. The task list provided in table 1–1 can be tailored for use in the SSMP. It can also be used as a check against omission of important tasks.

E–4. Milestones

A milestone schedule that parallels the overall program schedule should be established. Specific start and completion dates should be developed for the tasks listed in paragraph E–3. (Figure E–3 shows a sample of system safety milestones.)

E–5. Risk management

Procedures for hazard identification, categorization, tracking, and elimination should 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 1, sec II.)

E–6. Administration

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

E–7. Resources

a. Budget. Specific budgets should be prepared annually.This section should 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 should be described.

c. Authority. The authority for implementation of the SSMP comes from the PM. Specific actions such as taskings should be conducted with the PM's approval.

d. Sample SSMP. The sample SSMP in figure E–1 amplifies the preparation guidance provided in this appendix. It has been prepared for a generic major system and must be tailored before use. For example, organizations and responsibilities will be different for each program.

System Safety Management Plan

1. 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) AR 385–16, 3 September 1985.

(2) MIL–STD–882B, 30 March 1984.

(3) DA Pam 385–16.

(4) Program charter, *(system name), (MACOM).*

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 *(MACOM supporting the (system name) program,) (system name)* Program Management Office (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 defined in table 1–6, DA Pam 385–16.

(8) Significant safety data are documented as “lessons learned”and will be submitted to appropriate data banks (see para 3b(5)) 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.

2. System safety organization

a. Organization. *(For the organization of a PMO, see figure E–2.)*

b. Integration of associated disciplines. The SSWG is the focal point for the 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)* MANPRINT joint working group and test integration working group.

(2) The HEL and TSG to integrate the HFEA and the health hazard assessment into the *(system name)* system safety program.

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

3. Tasks

a. Program manager. The PM will—

(1) Charter and guide an SSWG per AR 385–16.

(2) Designate the program system safety manager.

(3) Establish decision authority levels for the acceptance of residual risk associated with system hazards. *(See table 1–6 DA Pam 385–16.)*

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

(5) Assign budget and manpower resources to accomplish system safety management tasks. *(See para E–7.)*

(6) Establish and update system safety milestone schedule. *(See para E–4.)*

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

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

(9) Integrate hazards and safety issues identified by associated disciplines and input data into hazard tracking system.

(10) 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 USASC.

Figure E-1. Sample of a system safety management plan—Continued

(11) Participate in Source Selection Evaluation Boards. Assure adequate SSEB criteria is established for evaluation of contractor SSPPs.

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

(13) Request TSG perform a health-hazard analysis of the *(system name)* (per AR 40–10) and provide a copy to the technical test agency 60 days before the start of the technical test.

b. Local safety office.

(1) Coordinate development of computerized hazard tracking system.System will be operational no later than *(date of program milestone).*

(2) 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.

(3) Act as executive manager for system safety for the MATDEV.

(4) Review procurement documentation for compliance with DOD system safety policy.

(5) Establish and maintain a system safety lessons-learned file for the *(system name)* system. Submit lessons learned on an annual basis (September) to USASC and DTIC until the system is fielded. Make recommendations, as appropriate, for changes to military specifications and standards.

(6) Review and comment on system safety portions of the *(system name)* request for proposal.

c. MATDEV organizations.

(1) Engineering. Provide description of hazards identified during development, production, and fielding to the SSWG. Include recommendations for controlling or eliminating the hazard.

(2) Product assurance. Provide description of hazards identified during development, production, and fielding to the SSWG. Include recommendations for controlling or eliminating the hazard.

4. Milestones

(For system safety milestones, see figure E–3.)

5. Risk management

a. 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. Probability will be categorized as frequent, probable, occasional, remote, and improbable. The categories for severity will be catastrophic, critical, marginal, and negligible. *(Specific definitions of these terms are in MIL–STD–882B.) (The matrix in table 1–4 will be used to assign a RAC to the hazard.)*

b. Risk resolution.

(1) Once a hazard has been identified and a RAC assigned, a determination should be made as to what action, if any, should be taken to remedy the hazard. Based on the RAC, not all hazards are severe enough or occur often enough to warrant the expenditures required to eliminate or control them. The SSWG will identify the potential methods of controlling or eliminating a hazard and the expected effectiveness of each option. The SSWG will submit a written report to the PM stating risk assessment results and hazard control recommendations—

(a) Within 14 calendar days after each SSWG meeting.

(b) Immediately when a Category 1A, 1B, 1C, 2A, 2B, or 3A hazard is identified.

(2) 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. *Table 1–6 defines the command level to which each hazard must be reported and the decision authority for accepting the risk associated with each hazard.*

(3) 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 E–1. The decision to accept the risk will also consider other factors such as impact on schedule and operational effectiveness. Per AR 385–16, the CBTDEV will provide a recommendation as to which corrective measure should be taken and the impact of other alternative corrective measures.

c. Hazard tracking.

(1) *(A hazard tracking system will be established jointly by the local safety office and the (system name) PM using the format in figure 1–1.)*

(2) The status of a hazard will be listed as “closed” only if written approval from the appropriate decision authority *(see table 1–6 DA Pam 385–16)* has been given for acceptance of the residual risk. The hazard will be monitored even if closed so that the mishap data can be compared to the accepted RACs, to the projected deaths and injuries, or to the projected costs. The *(system name)*mishap experience will be periodically compared to the projections to determine whether or not previous risk management decisions should be reevaluated and other corrective measures proposed.

d. Preparation for Army System Acquisition Review Council. The PM is responsible for preparation and presentation of an SSRA for each hazard that requires ASARC-level decision authority. The format found in AR 385–16 will be used for the SSRA. The hazard tracking list of the SSWG and the SAR by the contractor will be used to identify the appropriate hazards.

6. Administration

Figure E-1. Sample of a system safety management plan—Continued

The PM representative to the SSWG will accomplish the following:

a. 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.

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

7. Resources

a. Budget. *(To be established by PM.) (See para 3a(5) above.)*

b. Manpower. *(To be established by PM.) (See para 3a(5) above.)*

c. 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.

Figure E-1. Sample of a system safety management plan

Appendix F
System Safety Risk Assessment Preparation Guidance(Reference AR 385–16)

F–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–882B).

e. Source document reference.

f. Alternative actions that could reduce hazard level (include residual risk level for each action).

F–2. Part II

System safety working group/safety manager recommendation regarding risk acceptance. (Include minority views and rationale.)

F–3. Part III

Recommendation by the materiel developer (the PM, if chartered).

F–4. Part IV

Recommendation by the combat developer.

F–5. Part V

Approval by the appropriate decision authority.

Appendix G
Safety Release Preparation Guidance

G–1. Purpose of this safety release.

G–2. References.

G–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).

G–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 an SAR was provided for the system, it will be enclosed or referenced by the safety release. If no SAR 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 fans, requirements, and procedures.

G–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.

G–6. Signature of appropriate release authority.

Table 1–1
Government system safety timetable (typical)

System safety task	Phase				Reference
	CE	D&V	FSD	PRD	
Charter system safety working group (para 3–3)	X				AR 385–16
Develop system safety management plan (para 3–4)	X	O	O	O	
Develop preliminary hazard list (app D)	X				AR 385–16
Review requirements and program documents	X	X	X	X	
Assemble lessons learned and historical safety data (para 2–3)	X	O	O		AR 385–16
Review and approve request for proposal (para 3–5)	X	X	X	X	AR 385–16
Review contractor system safety program plan (para 3–5)	X	X	X	X	AR 385–16
Establish and maintain hazard tracking system (para 1–9)	X	O	O	O	AR 385–16
Safety input to test and evaluation master plan (para 3–6)	X	O	O	O	AR 385–16
Prepare system safety risk assessments (para 3–8)	X	X	X	X	AR 70–1AR 385–16
Conduct safety substudies (para 2–4)	X				AR 385–16
Prepare safety assessment report (para 4–3)	X	O	O	O	AR 385–16
Coordinate equipment design with facility design (para 3–16)	X				AR 385–16
Participate in source selection (para 3–7)		X	X		
Participate in design reviews (para 2–2)	X	X	X		AR 385–16
Identify hazards (para 1–7)	X	X	X	X	AR 385–16
Manage hazard risk (para 1–10)	X	X	X	X	AR 385–16
Review health hazard assessments (para 3–16)		X	X		AR 70–1AR 385–16
Evaluate training publications and programs (paras 2–8 and 5–16)		X			AR 385–16
Evaluate technical publications (para 3–7)			X		AR 385–16
Type classification reviews and other materiel release actions	X	X	X	X	AR 70–61AR 385–16
Accident/mishap investigation (para 5–8)	X	X	X	X	AR 385–40
Development and review of PIPs, ECPs, and QDRs (paras 2–5,5–11, and 5–12)				X	AR 385–16AR 71–9
Post-fielding system assessments (para 4–13)				X	AR 385–40

Legend for Table 1-1:
CE—concept exploration
D&V—demonstration and validation
FSD—full-scale development
PRD—production and deployment
X—initial
O—update
Blanks in phase columns indicate that the task is not applicable

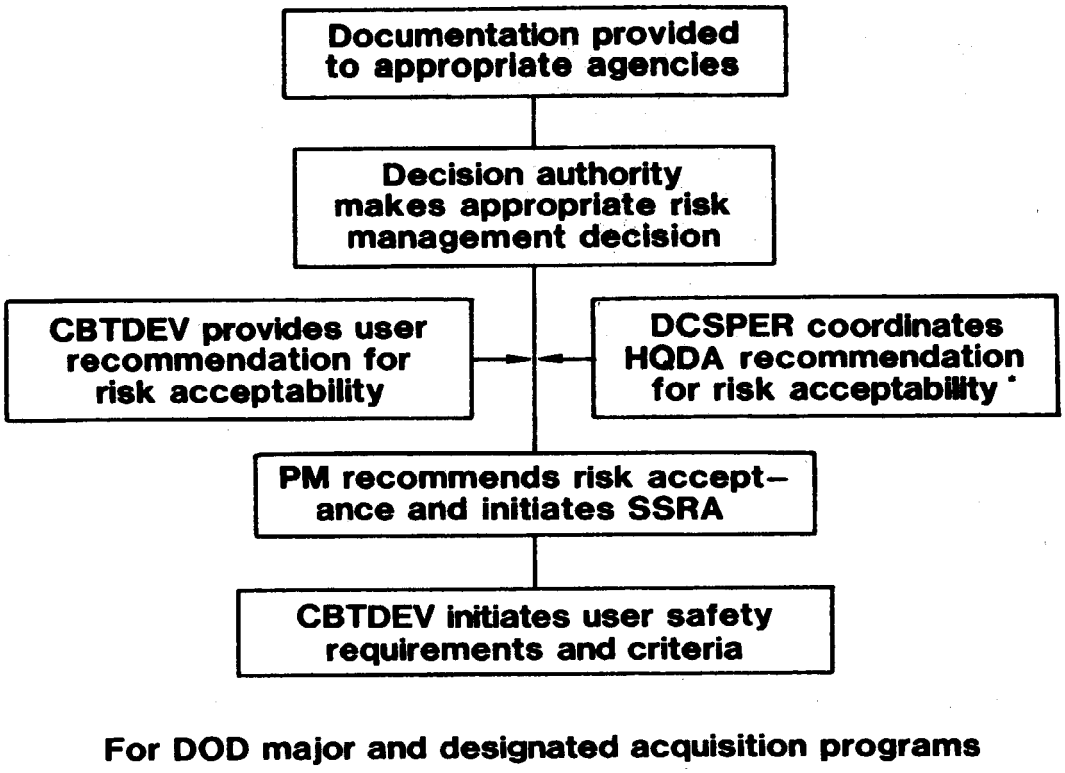

Figure 1-2. Risk management process

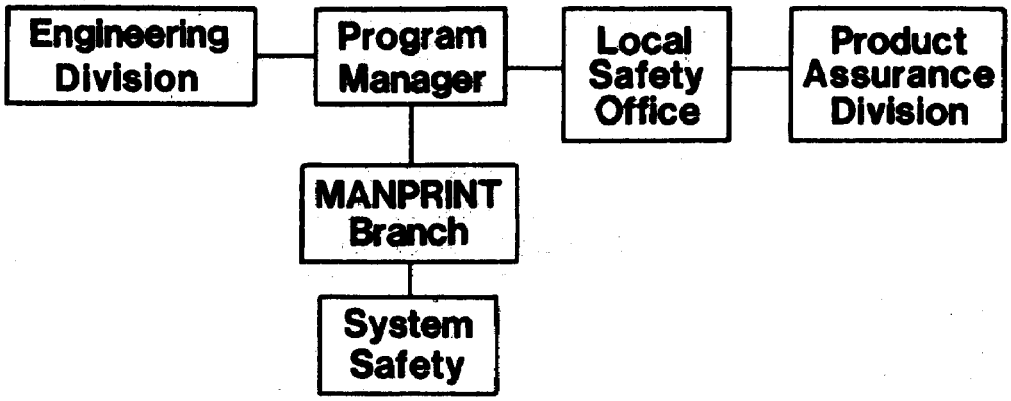

Figure E-2. Sample of a system safety organization

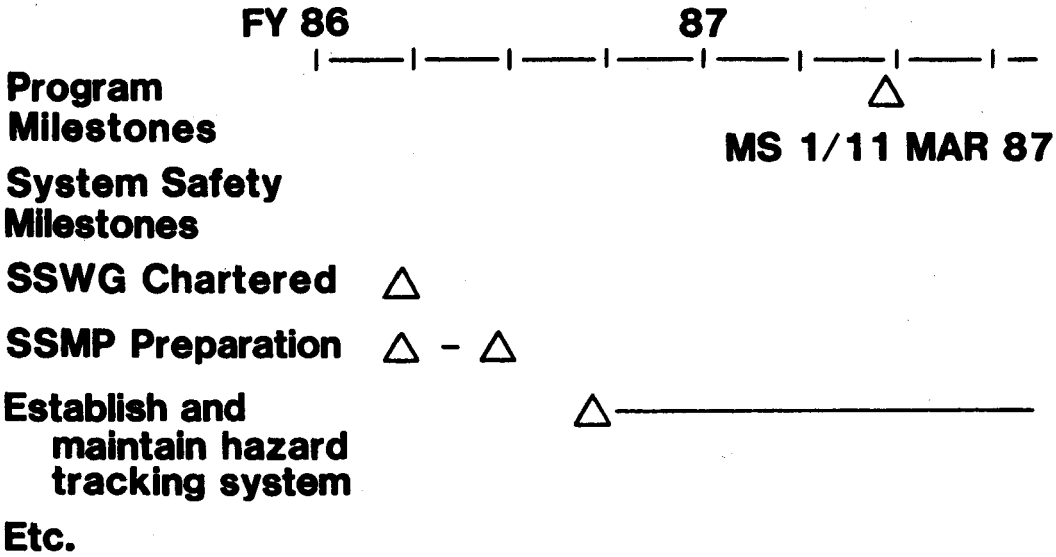

Figure E-3. Sample of system safety milestones

Glossary

Section I
Abbreviations

AFALC
U.S. Air Force Acquisition Logistics Center

AMC
U.S. Army Materiel Command

AMSAA
U.S. Army Materiel Systems Analysis Activity

ARNG
Army National Guard

ASARC
Army Systems Acquisition Review Council

BTA
best technical approach

CBTDEV
combat developer

CDRL
contractor data requirements list

COEA
cost and operational effectiveness analysis

DA
Department of the Army

DCD
directorate of combat development

DCSLOG
Deputy Chief of Staff for Logistics

DCSOPS
Deputy Chief of Staff for Operations and Plans

DCSPER
Deputy of Staff for Personnel

DCSRDA
Deputy Chief of Staff for Research, Development, and Acquisition

DI
data items

DID
data item description

DT&E
development testing and evaluation

DTIC
Defense Technical Information Center

ECP
engineering change proposal

EIR
equipment improvement report

FMECA
failure modes, effects, and criticality analysis

FSD
full-scale development

GFE
Government-furnished equipment

HEL
U.S. Army Human Engineering Laboratory

HFEA
human factors engineering analysis

HHI
health hazard inventory

IEP
independent evaluation plan

ILS
integrated logistic support

IPR
in-progress review

JMSNS
justification of major system new start

LSA
logistic support analysis

LSAR
logistic support analysis record

MAA
mission area analysis

MACOM
major Army command

MADP
materiel acquisition decision process

MANPRINT
manpower and personnel integration

MATDEV
materiel developer

MJWG
MANPRINT joint working group

MRSA
Materiel Readiness Support Activity

MTBF
mean time between failures

MTTR
meant time to repair

MWO
modification work order

NDI
nondevelopmental item

O&O
operational and organizational

O&SHA
operating and support hazard analysis

OHR
operational hazard report

OT&E
operational testing and evaluation

OTEA
U.S. Army Operation Test and Evaluation Agency

PHA
preliminary hazard analysis

PHL
preliminary hazard list

PIP
product improvement proposal

PM
program/project/product manager

PMO
Program Management Office

PRIMIR
product improvement management information report

QDR
quality deficiency report

RAC
risk assessment code

RAM
reliability, availability, and maintainability

RFP
request for proposal

ROC
required operational capability

RSI
rationalization, standardization, and interoperability

SAR
safety assessment report

SHA
system hazard analysis

SOF
safety-of-flight

SOW
statement of work

SSEB
source selection evaluation board

SSHA
subsystem hazard analysis

SSMP
system safety management plan

SSPP
system safety program plan

SSRA
system safety risk assessment

SSWG
system safety working group

TEAM
test, evaluation, analysis, and modeling

TECOM
U.S. Army Test and Evaluation Command

TEMP
test and evaluation master plan

TIWG
test integration working group

TOA
tradeoffs analysis

TOD
tradeoff determination

TOPS
test operations procedure

TRADOC
U.S. Army Training and Doctrine Command

TSG
The Surgeon General

USAR
U.S. Army Reserve

USASC
U.S. Army Safety Center

Section II
Terms

Terms

Army acquisition executive
Principal advisor and staff assistant to the Secretary of the Army for acquisition of Army systems; the assistant Secretary of the Army (Research, Development, and Acquisition) responsible for overall management of RDA programs.

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

Hazard
A condition that is a prerequisite for an accident.

Materiel developer
Command or agency responsible for research, development, and production of a system in response to approved requirements.

Residual risk
An expression of probable loss from hazards that have not been eliminated by design.

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

Safety release
A formal document issued to test organizations before any hands-on use or maintenance by troops. The safety release indicates the system is safe for use and maintenance by typical user troops and describes the specific hazards of the system or item based on test results, inspections, and system safety analysis. Operational limits and precautions are included. The test agency uses the data to integrate safety into test controls and procedures and to determine if the test objectives can be met within these limits.

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.

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 throughout the life cycle of the system.

System safety management plan
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
A description of planned methods to be used by the contractor to implement the tailored requirements of MIL–STD–882B, 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
There are no special terms.

Index

This index is organized alphabetically by topic and subtopic. Topics and subtopics are identified by paragraph number.

Accident investigation, 1–5, 5–8
Adaptation, 3–2, 4–4
Army acquisition executive, 1–10
Army materiel systems analysis activity, 4–11, 4–14

Best technical approach, 3–7, 4–14

Continuous comprehensive evaluation, 4–12
Cost and operational effectiveness analysis, 1–7, 2–2, 2–4, 5–12
Combat developer, 1–4, 2–1, 2–5, 2–6, 2–7, 5–2, 5–4, 5–8

Defense Technical Information Center, 2–3, appendix E

Engineering change proposal, 1–5, 2–6, 3–7
Equipment improvement report, 5–11

Failure modes and effects criticality analysis, C–6

Government-furnished equipment, 3–1, appendix C

Hazards
Probability of, 1–8
Identification of, 1–5, 1–7, 4–3, 5–6
Severity of, 1–8
Tracking of, 1–5, 1–9, 3–7, 4–8, 4–14
Health hazard assessments
Review of, 1–5, 4–14
Responsibility for, 3–16, 5–9
Human factors engineering, 2–4, 3–15
Human factors engineering analysis, 2–4, 3–10, 3–15, 4–12, 4–13, 4–14

Installation safety office, 2–1, 5–2, 5–10, 5–11, 5–13, 5–14, 5–15, 5–16
Integrated logistic support, 3–13, 4–14

Logistic support analysis, 3–13

MANPRINT
Elements of, 2–7, 3–10
Incorporation into ROC, 5–4
Joint working group, 2–2
Management plan, 2–2, 3–7, 4–14
Materiel acquisition decision process review, 3–8, 3–10, 4–12
Materiel developer, 1–1, 1–4, 1–6, 1–7, 2–7, 3–6, 4–3, 5–1, 5–4, 5–12, appendix C, F–3

Mission area analysis, 2–1, 2–4
Modification work order, 5–2, 5–13, 5–15, 5–16

Nondevelopmental Item
SSWG for, 3–3
Adapting system safety program for, 3–2
Testing of, 4–10

Operating and support hazard analysis, 3–11, C–6
Operational hazard report, 5–10
Operational Test and Evaluation Agency, 4–12, 4–14
Organizational and operational plan, 2–2, 2–3, 4–1, 4–14

Preliminary hazard analysis/list, 1–5, 1–9, 5–2, 5–5, appendix D
Product improvement proposal, 1–5, 2–2, 2–6, 3–7, 5–12, 5–13, 5–16

Quality deficiency reports, 5–11

Reliability, availability, and maintainability, 3–11
Request for proposal, 1–5, 4–14, appendix C
Required operational capability, 2–2, 4–14, 5–4
Risk
Assessment codes, 1–8, 1–9, 1–10, appendix E
Assessment of. (See system safety risk assessment.)
Management, 1–4, 1–5, 1–6, 1–10, 3–8
Residual, 1–10, 2–2, 2–6

Safety-of-flight message, 2–3, 5–15
Safety-of-use message, 2–3, 5–14
Safety assessment report, 3–13, 3–15, 4–3, 4–14, appendixes C and G
Safety release, 4–3, 4–14
Surgeon General, 3–16
System safety management plan
Preparation guidance, appendix E
Sample of, appendix E
Use of, 1–1, 1–4, 1–10, 3–4
System safety program plan
Preparation guidance, appendix C
Review of, 1–5, 3–3, appendix C
Use of, 3–5, 3–7
System safety risk assessment, 1–5, 1–9, 1–10, 2–6, 2–8, 3–8, appendix F
System safety working group
Activities of, 1–8, 3–12, 3–16, 4–4
Charter, 1–4, 1–5, 4–14, appendix B
Meeting agenda, 3–3
Membership of. Appendix B
Purpose for, 3–3

Test and evaluation master plan, 1–5, 2–5, 3–6, 3–7, 4–1, 4–4, 4–10, 4–14
Test integration working group, 2–5, 3–6, 4–6
Tester, 1–4, 4–3
Testing
Contractor, appendix C
Technical, 2–8, 3–6, 4–2, 4–3, 4–4, 4–8, 4–14, appendixes C, and G
User, 2–5, 3–6, 4–2, 4–3, 4–9, 4–14, appendixes C and G
Trade off analysis, 1–7, 2–2, 2–4, 4–14
Trade off determination, 1–7, 3–7, 4–14
Training
As corrective measure, 1–10
Contractor prepared, appendix C
Developer, 2–8, 5–16
Evaluation of, 1–5, 2–2, 4–2, 4–9, 5–2, 5–16
Ranges, appendix C
Safety personnel, 5–7
Type classification, 1–5

U.S. Army Safety Center, 2–3, 2–4, 2–6, 3–3, 3–8, 3–10, 4–13, appendix C
User, 1–4, 2–6, 2–7, 5–1, 5–2, 5–3, 5–10, 5–11, 5–12
User testing. See Testing, user

USAPA

ELECTRONIC PUBLISHING SYSTEM
TEXT FORMATTER ... Version 2.63

PIN:	062335–000
DATE:	08-03-99
TIME:	13:14:39
PAGES SET:	43

DATA FILE:	p385-16.fil
DOCUMENT:	DA PAM 385–16
DOC STATUS:	REVISION