

Department of the Army
Pamphlet 385-16

Safety

System Safety Management Guide

Headquarters
Department of the Army
Washington, DC
13 August 2013

UNCLASSIFIED

SUMMARY of CHANGE

DA PAM 385-16
System Safety Management Guide

This major revision, dated 13 August 2013-

- o Updates guidance on risk assessment and acceptance per Department of Defense guidance (para 1-4 and chap 2).
- o Provides a description of environment, safety, and occupational health system tasks in relation to the systems engineering v-charts per Department of Defense guidance (para 2-13).
- o Describes the relationship between systems engineering, the systems engineering plan, and system safety (para 3-2).
- o Provides an updated description of the Health Hazard Assessment Program (para 3-8).
- o Provides updated standards for software system safety (para 3-11).
- o Provides updated guidance on the Independent Safety Assessment Program (para 4-9 and app I).
- o Updates the sample format for a Safety and Health Data Sheet (app J).
- o Makes administrative changes (throughout).

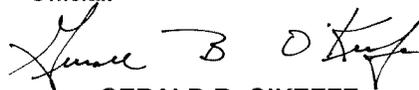
Safety

System Safety Management Guide

By Order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:



GERALD B. O'KEEFE
Administrative Assistant to
the Secretary of the Army

History. This publication is a major revision.

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

Applicability. This pamphlet applies to the active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. It also applies to Department of the Army civilian employees and

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

Proponent and exception authority. The proponent of this pamphlet is the Director of the Army Staff. The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this pamphlet by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the

requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Headquarters, Department of the Army, Director of the Army Staff (DACs-SF), Building 1456, 9351 Hall Road, Fort Belvoir, VA 22060–5860.

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

Contents (Listed by paragraph and page number)

Part One System Safety Engineering and Management, page 1

Chapter 1 System Safety Management, page 1

Purpose • 1–1, page 1

References • 1–2, page 1

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

Participants and key players • 1–4, page 1

Army Safety Action Team • 1–5, page 3

Chapter 2 Risk and Hazard Management, page 4

*This pamphlet supersedes DA Pam 385–16, dated 13 November 2008.

Contents—Continued

Section I

Risk Management, page 4

Process • 2-1, *page 5*

Risk management in system safety • 2-2, *page 5*

Identify hazard • 2-3, *page 5*

Assess hazard • 2-4, *page 7*

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

Implement controls • 2-6, *page 10*

Supervise and evaluate • 2-7, *page 10*

Hazard tracking • 2-8, *page 11*

Hazard closeout • 2-9, *page 12*

System safety risk management objectives • 2-10, *page 12*

Section II

System Safety Program Management Activities within the Life Cycle, page 13

Program elements • 2-11, *page 13*

Adapting the system safety program • 2-12, *page 13*

System safety integration with systems engineering • 2-13, *page 13*

Material solution analysis • 2-14, *page 14*

Technology development • 2-15, *page 17*

Engineering and manufacturing development • 2-16, *page 21*

Production and deployment phase • 2-17, *page 25*

Operations and support • 2-18, *page 28*

Chapter 3

Integration of System Safety Associated Disciplines, page 31

General • 3-1, *page 31*

Systems engineering • 3-2, *page 31*

Reliability, availability, and maintainability • 3-3, *page 32*

Quality engineering • 3-4, *page 32*

Integrated logistics support • 3-5, *page 32*

Combat survivability • 3-6, *page 33*

Human factors engineering • 3-7, *page 33*

Health hazards • 3-8, *page 34*

System safety in the manpower and personnel integration process • 3-9, *page 35*

Environment • 3-10, *page 36*

Software system safety • 3-11, *page 36*

Chapter 4

System Safety for Testers and Evaluators, page 37

Section I

Introduction, page 37

General • 4-1, *page 37*

Definition • 4-2, *page 37*

Section II

Test Planning and Conduct of Test, page 38

Test planning • 4-3, *page 38*

General • 4-4, *page 38*

Developmental tests • 4-5, *page 38*

User tests • 4-6, *page 38*

Non-developmental item tests • 4-7, *page 39*

Section III

Evaluations, page 39

Contents—Continued

Evaluators • 4–8, *page 39*

U.S. Army Combat Readiness/Safety Center independent safety assessment • 4–9, *page 39*

Part Two

Facility System Safety, *page 40*

Chapter 5

Facility System Safety Management, *page 40*

Purpose of facility system safety • 5–1, *page 40*

Facility system safety participants • 5–2, *page 40*

Chapter 6

Facility System Safety Program Management, *page 40*

General • 6–1, *page 40*

Background • 6–2, *page 41*

Using or Activity installation responsibilities • 6–3, *page 41*

Engineering organization responsibilities • 6–4, *page 42*

Design agent functions • 6–5, *page 43*

Standard designs • 6–6, *page 43*

Self-help projects • 6–7, *page 44*

Construction facility system safety • 6–8, *page 44*

Facility/project operation and maintenance • 6–9, *page 44*

Chapter 7

Facility System Safety Program Contracting, *page 45*

General • 7–1, *page 45*

Contractor selection • 7–2, *page 45*

Task selection • 7–3, *page 45*

System safety engineering plan • 7–4, *page 45*

Appendixes

A. References, *page 47*

B. Preparation Guidance for a System Safety Working Group Charter, *page 50*

C. System Safety Management Plan, *page 52*

D. Preliminary Hazard List/Preliminary Hazard Analysis, *page 56*

E. System Safety Risk Assessment Preparation Guidance, *page 58*

F. Safety Release Preparation Guidance, *page 58*

G. Manpower and Personnel Integration Joint Work Group System Safety Checklist, *page 59*

H. Non-developmental Item System Safety Market Investigation/Survey Questions, *page 59*

I. Independent Safety Assessment, *page 60*

J. Safety and Health Data Sheet Sample Format, *page 61*

Table List

Table 2–1: Hazard Tracking System—sample format for a hazard tracking record, *page 11*

Table 2–2: Inputs of the materiel solution analysis phase, *page 15*

Table 2–3: Steps of the materiel solution analysis phase, *page 16*

Table 2–4: Outputs of the materiel solution analysis phase, *page 16*

Table 2–5: Inputs of the technology development phase, *page 18*

Table 2–6: Steps of the technology development phase, *page 19*

Table 2–7: Outputs of the technology development phase, *page 20*

Table 2–8: Steps of the engineering and manufacturing development phase, *page 23*

Contents—Continued

- Table 2-9: Outputs of the engineering and manufacturing development phase, *page 24*
Table 2-10: Inputs of the production and deployment phase, *page 26*
Table 2-11: Steps of the production and deployment phase, *page 27*
Table 2-12: Outputs of the production and deployment phase, *page 27*
Table 2-13: Inputs of the operations and support phase, *page 30*
Table 2-14: Steps of the operations and support phase, *page 30*
Table 2-15: Outputs of the Operations and Support Phase, *page 31*
Table D-1: Sample format of preliminary hazard analysis (typical), *page 57*

Figure List

- Figure 2-1: The risk management process, *page 5*
Figure 2-2: Hazard identification process, *page 6*
Figure 2-3: Process for developing alternatives, *page 9*
Figure 2-4: Defense Acquisition Framework, *page 14*
Figure 2-5: Materiel solution analysis v-chart, *page 15*
Figure 2-6: Technology development v-chart, *page 18*
Figure 2-7: Engineering and manufacturing development v-chart, *page 22*
Figure 2-8: Production and deployment v-chart, *page 26*
Figure 2-9: Operations and support v-chart, *page 29*
Figure C-1: Milestones, *page 53*

Glossary

Part One

System Safety Engineering and Management

Chapter 1

System Safety Management

1-1. Purpose

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

- a. Establish and manage system safety programs to minimize risks throughout the system life cycle.
- b. Conduct hazard identification, system safety, hazard tracking procedures, and risk management during all phases of the lifecycle.

1-2. References

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

1-3. Explanation of abbreviations and terms

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

1-4. Participants and key players

The effectiveness of the system safety program can be directly related to the proactive 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. *Capability developer.* The CAPDEV has a vital role in the success of any system safety effort in all stages of a system's life cycle. During materiel solution analysis, the CAPDEV should ensure that system safety is considered an integral component. They will seek the appropriate system safety expertise (for example, U.S. Army Training and Doctrine Command (TRADOC) System Safety Engineer), as soon as it is determined a new system is the appropriate solution to correct deficiencies identified during the mission area analysis. If a modification or a doctrine change is the solution for a fielded system, then the CAPDEV will also seek system safety expertise to determine the potential safety impact of the selected solution. Some CAPDEVs have system safety expertise within their organizations; however, for those who do not, the secondary sources of help are at the CAPDEV's Army command (ACOM)/Army service component command (ASCC)/direct reporting unit (DRU) safety office. The CAPDEV is the integrator of system safety until a PM is chartered, usually after Milestone B. The principle system safety responsibility of the CAPDEV is to seek system safety expertise and to articulate the user's safety requirements throughout the system life cycle. Inadequate or poorly designed equipment exposes users to an increased safety risk and a higher potential for loss of combat resources. The CAPDEV must incorporate system safety performance objectives into the concept formulation package. Historical lessons learned should be considered in concept studies and trade off analyses (TOAs). CAPDEVs—

- (1) Identify needed safety capabilities to reduce the potential for mishaps.
- (2) Integrate safety requirements into capabilities documents.
- (3) Develop user safety test issues and criteria.
- (4) Participate in the system safety working group (SSWG) to ensure that the system's operational and safety capabilities satisfy the mission needs.
- (5) Represent the user throughout the life cycle and coordinate all system safety and risk management issues with their system safety representative.
- (6) As the user representative, review all risk acceptance decisions and provide concurrence per DODI 5000.02.
- (7) Ensure their system safety representative attend program integrated product/process team and SSWG meetings, as appropriate.

b. *Research, development, and engineering organizations.* For a system in the technology base, the research, development, and engineering organizations must—

- (1) Charter and maintain a technology safety working group. The technology safety working group is responsible for reviewing emerging technologies and assessing and recommending steps to be taken to ensure safety.
- (2) Provide qualified system safety personnel (such as, the research, development, and engineering safety personnel) to conduct safety analyses and safety assessments appropriate for technologies that are going to be tested or fielded.
- (3) Provide the safety analyses and safety assessments to a program office when technology is transitioned.
- (4) Ensure hazard analyses are conducted and the resulting safety and health requirements are included in standard operating procedures (SOPs) and enforced, when performing research, development, and engineering, testing or industrial operations.

(5) Ensure research, development, and engineering project efforts include safety criteria, critical items, and hazards identified as part of the project documentation.

c. Program executive officers/program managers/materiel development/life cycle management command or direct reporting program manager. The PEO/PM/MATDEV/LCMC or direct reporting program manager ensures that hazards associated with the design, operation, maintenance, servicing, support, and disposal of the system are identified and resolved early in the life cycle through the application of system safety management and engineering. To accomplish this objective, the PEO/PM/MATDEV sets goals and establishes mechanisms to attain these goals.

(1) PEOs—

(a) Act as the safety officer for assigned systems with the responsibility for the proper planning and execution of a system safety program per DODI 5000.02, AR 70–1, and AR 385–10.

(b) Act as risk acceptance authority for risk levels defined in Military Standard 882 (MIL–STD–882), DODI 5000.02, AR 70–1, or the approved alternate system safety risk matrix (see chap 2 of this pamphlet).

(c) Furnish a representative (general officer/senior executive service-level) to serve on the Army safety action team (ASAT) for their programs.

(d) Ensure PMs are personally involved in their system safety programs. PMs are to fully integrate system safety into their programs.

(2) The PM will—

(a) Implement system safety programs as required by DODI 5000.02 and AR 70–1.

(b) Charter and support with existing resources an SSWG (see app B, of this pamphlet) to provide the technical expertise needed to manage the system safety effort. PMs will obtain system safety engineering (SSE) management support through their associated LCMC or research, development, and engineering command safety office.

(c) Maintain a system safety management plan (SSMP) (see app C of this pamphlet) to define the system safety activities throughout the system life cycle. The SSMP will be prepared at program initiation and updated prior to each decision review.

(d) Establish and maintain a Hazard Tracking System (HTS) throughout the system’s life cycle, ensuring that there is a formal closed-loop process for managing hazards. No hazards shall be closed until the mitigating measure’s implementation has been verified and any residual risk accepted by the appropriate authority. All residual risks must be accepted prior to fielding. Institute procedures to identify and manage hazards that are discovered post-fielding (see para 1–5, below), document associated risk acceptance decisions, and communicate the risks and required actions to the field as appropriate. The process should include proactive review of user feedback and the maintenance of a permanent record of identified hazards and closeout actions.

(e) Serve as the risk acceptance authority for risk levels defined in MIL–STD–882, DODI 5000.02, AR 70–1, and/or the approved alternate system safety risk matrix (see chap 2 of this pamphlet). Ensure that all high and serious risk hazards are addressed at all technical and program reviews. Obtain user representative coordination prior to all risk acceptance decisions.

(f) Integrate the system safety program into the acquisition process. System safety representation should span the program integrated product/process team structure to ensure cross-functional interaction.

(g) Request Safety Releases for all test events involving user personnel.

(h) Assure that engineering changes, alterations, deviations, waivers, and modification proposals are reviewed for impact on safety.

(i) Copies of system safety program documentation should be forwarded to the appropriate LCMC or U.S. Army Research, Development, and Engineering Command, and the U.S. Army Combat Readiness/Safety Center (USACR/SC), as appropriate.

(j) Ensure that human systems integration (HSI) processes are implemented to design human machine interfaces in compliance with human factors engineering (HFE) standards and criteria (that is, MIL–STD–1472G), to reduce the incidence of human errors, to make systems error tolerant, to reduce the incidence of ergonomic injuries, and to enhance human performance.

(3) LCMCs—

(a) Establish a responsible command focal point to manage system safety efforts and provide representation to the Department of the Army (DA) System Safety Council.

(b) Provide qualified system safety personnel to support the development and sustainment of Army materiel.

(c) Provide system safety risk assessments (SSRAs) recommendation, and the safety focal point shall provide an independent recommendation for formal risk assessments (see app E, of this pamphlet).

(d) As the materiel release authority, ensure the materiel is safe for fielding per AR 700–142 (that is, as documented in a safety and health data sheet (SHDS) (see app J of this pamphlet) or programmatic environment, safety, and occupational health evaluation (PESHE)).

(e) Serve as release authority for safety messages, per AR 750–6.

d. Tester. The tester supports the system safety process by structuring tests based upon test planning documentation (for example, test and evaluation master plan (TEMP), system evaluation plan, test design plan, and so forth). Testing

will provide data to assess the effectiveness of system designs and processes implemented to eliminate or control identified hazards, and it may identify new hazards. Hazards identified by the tester will be provided to the decision-maker (for example, PEO/PM/MATDEV/CAPDEV, and so forth) for risk management. A Safety Confirmation is developed by Army Test and Evaluation Command (ATEC) or the Army Medical Department (AMEDD) Board and provided to the PM and to the independent evaluator, the latter copy to be used to support development of the independent evaluation. The sources of data can be contractor testing, technical testing, or user testing. The Safety Confirmation is a stand-alone document required at each milestone review and may identify unresolved hazards and risks.

e. Evaluator. An evaluator is an individual in a command or agency, independent of the MATDEV and the user, that conducts overall evaluations of a system's operational effectiveness, suitability, and survivability (see also para 4–8, of this pamphlet). The evaluator consolidates test data from all available sources to address the technical and user test issues and requirements developed for a system. As a part of continuous evaluation (CE), the evaluator should assess and report the cumulative impact of unresolved hazards on the system's effectiveness.

f. User. The users are the equipment operators and maintainers.

(1) Initial activity occurs during early technical development and continues through the life cycle of the system. Two major roles are—

(a) Identification of hazards in order to improve the safety of existing systems (for example, by submitting an equipment improvement report or product quality deficiency report, Standard form (SF) 368 (Product Quality Deficiency Report (PQDR)), and by participation in the conduct of post-fielding training effectiveness analysis).

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

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

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

(b) Early identification of new mission requirements.

(3) Development activity, sometimes with the cooperation of the U.S. Army Materiel Command (AMC) Field Assistance in Science and Technology Program, identifies new operational requirements. AMC Field Assistance in Science and Technology Program or rapid equipping force community is responsible for reviewing and identifying safe systems, identifying any residual risks to users, and obtaining risk acceptance in accordance with this pamphlet. If the program does not go into a full developmental project, the user must perform the role of the CAPDEV, MATDEV, and tester/independent evaluator. The user will use the procedures contained in this pamphlet for identifying operational and materiel risks involved with the equipment's configuration and operation. AR 700–142 provides applicable safety documentation requirements for urgent materiel release, tests, demonstrations, and training. Consideration must be given that equipment often classified as “prototype” may be used for many years.

(4) The user is represented by the TRADOC capability manager (TCM) and will coordinate with the end users, especially the first unit equipped.

1–5. Army Safety Action Team

a. Objectives. The objectives of the ASAT are the following:

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

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

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

(1) Principal members are as follows:

(a) Assistant Secretary of Army for Acquisition, Logistics and Technology.

(b) Deputy Chief of Staff (DCS), G–3/5/7.

(c) DCS, G–4 (Chairman).

(d) DCS, G–8.

(e) Director of Army Safety.

(f) AMC.

(g) Appropriate PEO.

(h) Applicable proponent branch chief.

(i) Applicable MATDEV.

(2) Advisory members are as follows:

(a) DCS, G–1.

(b) Chief, Public Affairs.

- (c) Chief, Legislative Liaison.
- (d) Chief, Army National Guard.
- (e) Chief, Army Reserve.
- (f) Assistant Secretary of the Army for Installations, Energy and Environment/Deputy Assistant Secretary of the Army for Environment, Safety, and Occupational Health.

(3) Other agencies and subject matter experts (for example, U.S. Army Forces Command and U.S. Army Special Operations Command may be included, as directed by the Director, Army Staff or the chairperson).

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

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

(1) When a hazard is identified that has a potentially significant impact upon Army training or operations, the PM, in conjunction with the cognizant MATDEV agency, will immediately alert the ASAT Chairman. This notification will be in the form of a hazard EXSUM. This hazard EXSUM will normally include a description of the problem, a preliminary determination of risk, the potential operational impact, the current logistical status, and the get-well concept. However it should not be delayed if this data is not yet available. It is understood that the accuracy and completeness of this initial assessment will be dependent upon the technical and operational data available at that point; the intent is to provide an early hazard alert to provide the basis for a timely and collective assessment of the risks and potential controls as more information is gained on the nature and extent of the problem. The hazard EXSUM will be updated as additional technical and operational knowledge become available.

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

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

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

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

e. Fielded system/materiel Army safety action team. For fielded systems or materiel, MATDEVs will establish procedures for alerting the ASAT Chairman of impending safety issues with significant risk or that have the potential for significant impact upon operations and training. If such changes require transmission of safety information to the field, the MATDEV agency will develop and coordinate a safety of flight/safety of use message. Specific procedures for developing and coordinating these messages are contained in AR 750-6 for aviation and ground systems.

Chapter 2 Risk and Hazard Management

Section I Risk Management

Risk management is the process of identifying, eliminating or mitigating, and accepting residual risk associated with a mission; design of a system, facility, equipment, or process; or their operation. The risk assessment levels and

acceptance decision authority levels in MIL-STD-882, DODI 5000.02, and AR 70-1 will be used in all programs unless a modified matrix has been approved per AR 70-1.

2-1. Process

The Army uses risk management to mitigate risks associated with all hazards that have the potential to injure or kill personnel, damage or destroy equipment, or otherwise impact mission effectiveness. The five-step process established in FM 5-19 and DA Pam 385-30 is shown in figure 2-1.

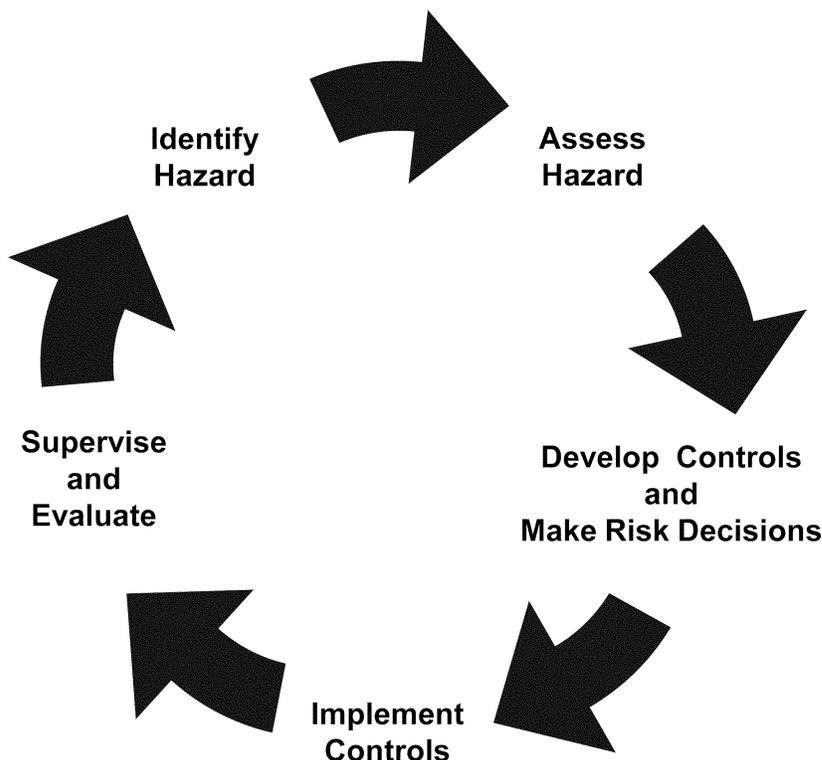


Figure 2-1. The risk management process

2-2. Risk management in system safety

Within the context of this pamphlet, risk management is a means for capturing hazards and providing a communication forum, via the HTS. Additionally, it provides hazard close-out methods and criteria within the five-step process by which hazards can be officially closed. Development of the mechanics and criteria to capitalize on this concept for the overall benefit to the Army is a dynamic process and requires “real time” communication among all concerned to ensure its application.

2-3. Identify hazard

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

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

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

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

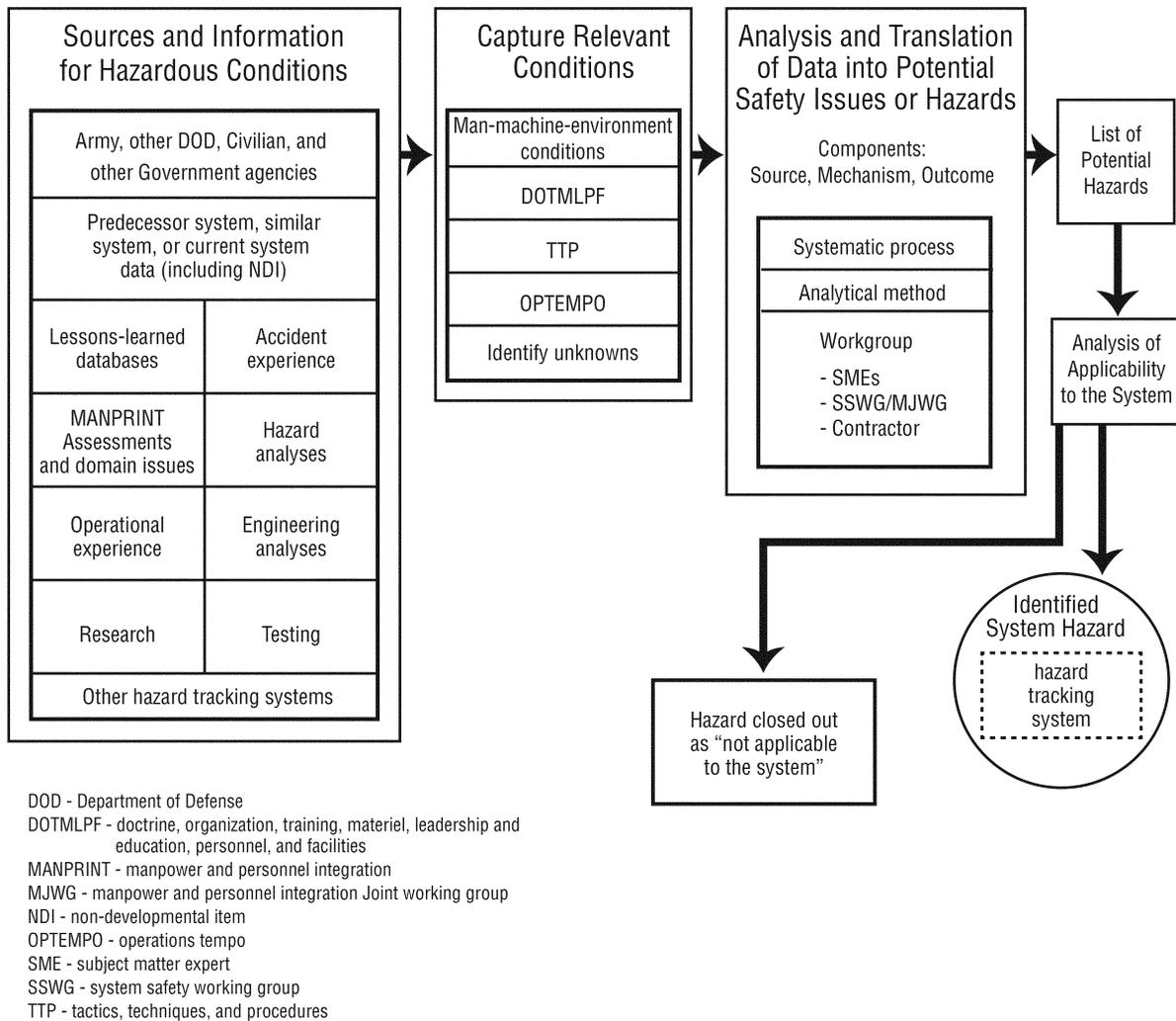


Figure 2–2. Hazard identification process

d. The sources of these potential or real hazards might be lessons learned, hazards analyses, accident experience, technology base development data, operational experience, testing, government studies, or information from non-military usage of similar technology. These hazards include any issues which have the potential to result in losses or damage to materiel or the environment or injury (accidental and/or health-related) to any personnel. Potential causes of losses must be translated (if possible) into a potential system hazard. For example, a “human error” cause of an accident may have been induced by a system design hazard. All potential system hazards are then added to the HTS. Once a real or potential hazard is identified, it is handled and treated as a real hazard. It will be formally considered, tracked in the HTS, and reviewed. Several activities and analyses performed by the government or the contractor can contribute to the HTS, such as design and program reviews, test and evaluation (T&E) reports, safety assessment reports (SARs) (initial and updates), health hazard assessment reports (HHARs), Safety Releases and Safety Confirmations, preliminary hazard lists (PHLs), and preliminary hazard analyses (PHAs). Related disciplines, such as those listed in chapter 3, of this pamphlet, will identify hazards or other information that must be evaluated to identify hazards.

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

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

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

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

(3) Materiel developers may choose or be required to use NDIs (for example, government furnished-equipment, commercial off-the-shelf items, and so forth) in the development of their systems. Regardless, proponent MATDEVs are required to consider hazards associated with NDIs, including the interfaces of the NDI with other components. All identified hazards associated with the NDIs will be documented and tracked in hazard analyses and the HTS.

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

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

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

2-4. Assess hazard

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

a. *Hazard assessment.* In establishing priorities for correcting a system’s hazards, hazards must be evaluated to determine their probability levels and severity categories. Hazard risk, probability, and severity will be categorized according to MIL-STD-882. When necessary, a program may propose an alternate risk assessment matrix that is based on MIL-STD-882. Alternate matrices will be developed, coordinated, and approved per AR 70-1.

(1) Care should be taken to ensure the system is adequately defined. For example, if a tank engine is defined as the system, a hazard that causes it to stop could be catastrophic, since there was a total system loss. Now, if the system were the tank and the engine stopped, then the hazard may not be catastrophic. Care also must be taken to look at associated hazards. For example, if the tank engine also powered the brakes, then the hazard of an engine stoppage might be higher. Software hazard causes and controls should be considered in all hazard identification and risk management efforts. Software is an increasingly common component of Army systems that affects safety-related functionality and is a primary interface in system-of-systems (SOS) configurations.

(2) The risk associated with a hazard is a function of its severity and probability. When severity categories and probability levels are combined, they provide a matrix for assigning a code to the risk associated with a hazard. These codes are known as risk assessment codes (RACs). Single-digit RACs could be created by using numerical rather than alphabetical rankings of probability, then multiplying probability by severity. This method should be avoided, because the use of single-digit codes presumes that the lower the product, the higher the risk associated with the hazard. This presumption is not always true, and common products (such as 1 x 4 and 2 x 2) mask prioritization.

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

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

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

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

c. Close out criteria during risk assessment. During this step of the risk management process, the only way a hazard can be closed out is by “meeting or exceeding acceptable standards.” This method requires careful consideration by system safety practitioners and program managers, as abuses of the process may occur. MAs are encouraged to consider all hazard fixes that derive a level of safety that is in concert with program cost and schedule, as well as maximize warfighting capability. System safety programs that consider all programmatic assets can provide the leading edge for quality.

(1) *Design meets or exceeds applicable standards.* The goal is to recognize appropriate application of consensus standards. For example, any pressure vessel presents a hazard; however, if it has been designed to meet or exceed American Society of Mechanical Engineers, American National Standards Institute, and MIL–STD–1522A, and it is used in an environment appropriate to these standards, then it may not require formal acceptance.

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

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

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

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

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

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

2–5. Develop controls and make risk decisions

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

a. With the risk of the hazard assessed, the next task is to develop alternatives for controls. Here alternatives should be generated using the system safety design order of precedence per MIL–STD–882, determining which control or combination of controls will be applied given the program’s resource constraints. Therefore, cost and other programmatic impacts must be identified with each alternative. While effectiveness of specific controls may vary, the system safety order of precedence for mitigating identified hazards generally is—

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

(2) *Incorporate safety devices.* If unable to eliminate the hazard through design selection, reduce the risk to an acceptable level using protective safety features or devices.

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

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

b. The decisionmaking task involves selecting the alternatives identified in the develop controls portion of this step, as shown in figure 2–3. Formal acceptance of any residual risk that exists after the controls have been implemented must be documented.

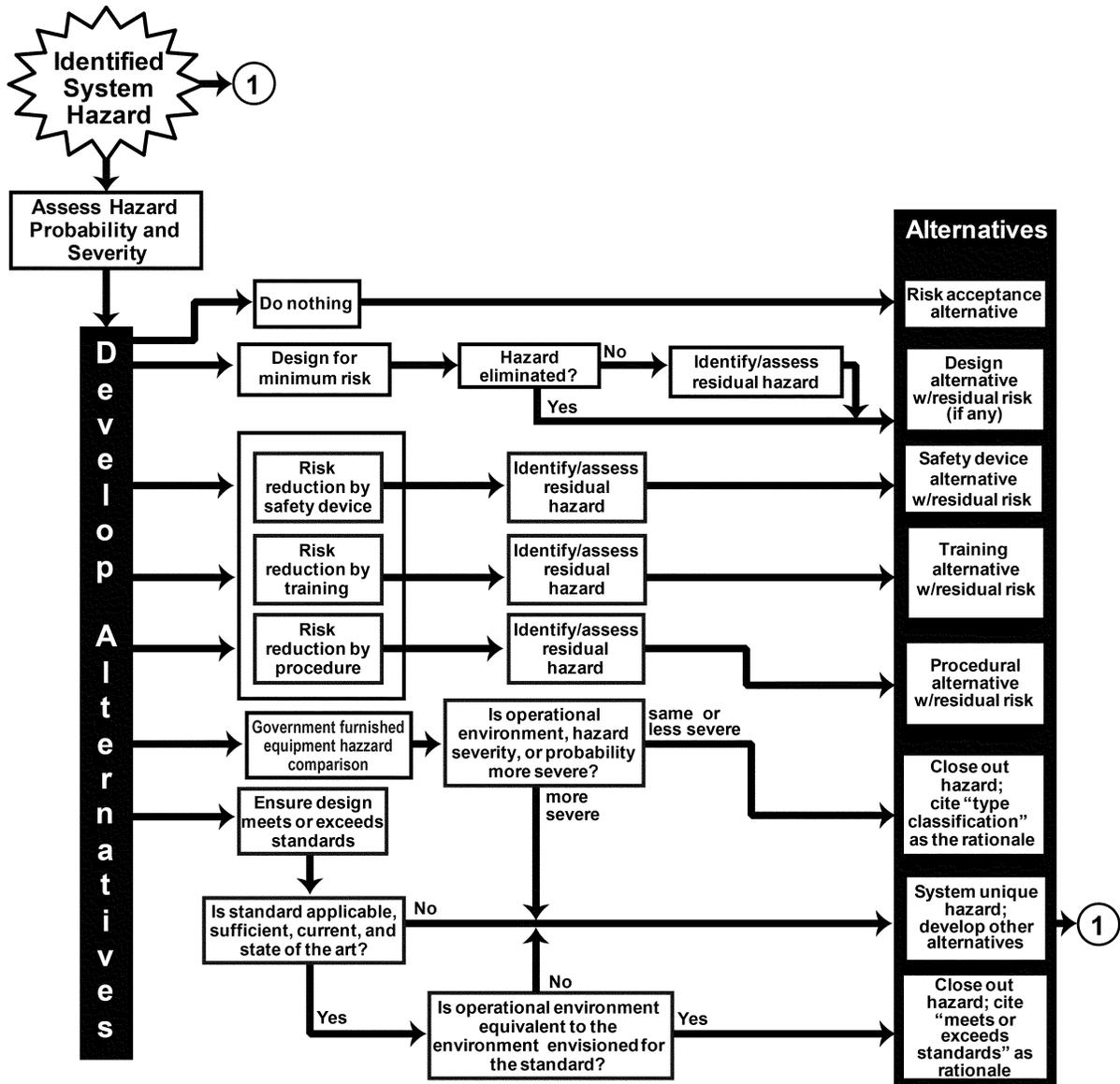


Figure 2-3. Process for developing alternatives

c. The residual hazards in figure 2-3 refer to the risk remaining after corrective action(s) have been applied. For example, a hazard is identified and assigned a RAC of IIA. The PM allocates additional funds for the contractor to apply an engineering "fix" to the system, which would reduce the RAC to IID. The cost to further reduce the risk is prohibitive in the judgment of the PM; however, given the matrix in MIL-STD-882 and the program SSMP, the PM must decide whether to accept the risk for this residual hazard. If the decision authority decides that the risk is acceptable, then the engineering "fix" should be applied and tested. In another example, an IIA hazard is identified, but the PM's recommended engineering "fix" will only reduce the RAC to IIC. The PM cannot accept that level of risk; therefore, the PEO must decide on risk acceptability. If the decision authority decides that IIC is an unacceptable level, then the PM will have to take necessary action(s) to further reduce the risk.

d. Determining which alternative control(s) to apply is important. The decision to accept the risk of a residual hazard must be at a level appropriate to the priority of the residual hazard. From a safety standpoint, the goal should be to achieve the lowest level of risk in concert with mission effectiveness. The residual hazard control alternatives in paragraph 2-5a, above, are listed in their order of effectiveness to reduce risk. Designing for minimum risk, incorporating safety devices, and providing warning devices usually require engineering design changes. Because such changes

become increasingly more expensive later in the life cycle, early hazard identification is essential. Caution should be taken when relying on procedures or training as controls.

e. The residual hazard closeout procedures, during the “develop controls and make risk decisions” step of the risk management process, are—

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

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

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

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

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

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

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

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

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

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

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

(a) Reviewing/defining the source, mechanism, and outcome of the hazard.

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

(c) Documenting rationale for not eliminating the hazard.

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

(e) Developing and coordinating an SSRA for the hazard (see app E, of this pamphlet).

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

f. Acceptance decisions will be performed at a level of management authority commensurate with the risk. Army’s standard system safety risk decision matrix is established by AR 70–1 and is in accordance with DODI 5000.02.

(1) Should program requirements dictate a different decision authority; the change(s) must be documented and submitted for approval to the highest affected level of authority. The recommended matrix will be submitted for approval per AR 70–1 and/or more current guidance. The PM will include the alternate matrix in the SSMP (see app C, of this pamphlet).

(2) Each potential control should be identified, and the risk, if it is applied, should be projected. The consequences of risk acceptance and of each alternative control should be expressed using projected costs in terms of deaths, injuries, system damage, and program delay.

2–6. Implement controls

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

a. Designate or obtain funding for the fix.

b. Develop and implement an action plan for implementation of the risk decision.

(1) Production and retrofit.

(2) Follow-up plan for monitoring corrective action and implementation status.

(3) Implement devices, training, or procedures.

(4) Publish the procedures in the appropriate manuals.

c. Develop and execute a follow-up plan to verify anticipated/assigned hazard severity/probability and adequacy of the fix in the operational environment.

d. Verify that implementation of selected control(s) does not result in creating another hazard.

e. Testing is the primary method of verifying the effectiveness of the hazard controls implemented as described in chapter 4, of this pamphlet.

2–7. Supervise and evaluate

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

b. Only when the above criteria have been met, including the addressing of the residual risk and the effectiveness of

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

2-8. Hazard tracking

a. The HTS tracks the status of all identified hazards throughout the life cycle of the system. A PHL and PHA (see app D, of this pamphlet) should be performed on each technology or conceptual system and then used as the basis for establishing the HTS, if the technology matures into a concept. The data elements for an automated hazard tracking record format are shown in table 2-1. The status will reflect approval by the appropriate decision authority and whether the control/mitigation measure has been applied. Once identified, the hazard should never be removed from the HTS, during the life cycle of the hardware and successor systems.

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

Table 2-1
Hazard Tracking System—sample format for a hazard tracking record

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

**Table 2-1
Hazard Tracking System—sample format for a hazard tracking record—Continued**

SSRA required (Yes/No)	Indicates the need for an SSRA.
SSRA completed (Yes/No)	Indicates whether or not the SSRA is complete.
SSRA signature date	Date the SSRA was finalized.
Signature fields	The necessary signature fields for the SSRA.

2-9. Hazard closeout

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

- (1) Not applicable to the system.
- (2) Eliminated by design modification.
- (3) Design meets or exceeds applicable Federal, Department of Defense (DOD), DA, recognized national consensus standards, or regulations for the operating environment.
- (4) Review and certification by the appropriate authority (for example, Army Fuze Safety Review Board, Insensitive Munitions (IM) Board, Ignition System Safety Review Board, or DOD Explosives Safety Board).
- (5) Risk acceptance.

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

2-10. System safety risk management objectives

a. The PEO/PM will maximize operational readiness and mission effectiveness through accident prevention by ensuring—

- (1) Hazards and associated risks are identified and managed for each system throughout its life cycle and all mission variations.
- (2) Hazards are eliminated through design or controlled to acceptable levels, and risk associated with residual hazards is formally identified, accepted by the appropriate management decision level, and documented.
- (3) Hazards associated with new technology or operations are identified for consideration in later applications.
- (4) Safety performance capabilities are established addressing hazards with similar legacy systems.
- (5) Sustain safe systems throughout the life cycle.

b. The CAPDEV will—

- (1) Establish safety performance capabilities addressing hazards with similar legacy systems.
- (2) Integrate system safety into technology development, prior to Milestone B.
- (3) Ensure risk mitigation and acceptance decisions for developmental systems are coordinated with users and CAPDEV system safety expertise.
- (4) Ensure users' perspectives on the acceptability of residual risk is incorporated into any modification.

c. Testers will—

- (1) Identify potential and real hazards.
- (2) Verify the effectiveness of the correction imposed.
- (3) Determine test event residual risk level.

d. Independent evaluators will—

- (1) Provide an independent assessment for materiel acquisition decision process reviews.
- (2) Receive from the PM copies of the appropriate documents for evaluation prior to the materiel acquisition decision process review date.

e. Life cycle managers will—

- (1) Maintain continuity and capability for SSE and management.
- (2) Maintain system safety expertise for support to the PM throughout the life cycle.
- (3) Assist the PM in ensuring all hazards are managed and laws/regulatory requirements are met throughout the life cycle.
- (4) Ensure materiel release environment, safety, and occupational health (ESOH) requirements are completed per AR 700-142.

Section II

System Safety Program Management Activities within the Life Cycle

2-11. Program elements

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

2-12. Adapting the system safety program

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

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

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

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

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

(2) *Incremental development.* In this process, a desired capability is identified, an end-state requirement is known, and that requirement is met over time by development of several increments, each dependent on available mature technology.

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

e. A successful system safety effort requires adaptation, in order to fit the particular materiel acquisition program. This is particularly true for NDIs and other programs with accelerated acquisition cycles. This is also true when a "materiel system" interfaces with a "facility." Special care must be taken so the life cycles of the two are connected. The best document for this is the support facility annex of the logistic support analysis (LSA). The PM's system safety advisor will recommend activities that are necessary for his system. The selected activities are then included in the SSMP.

f. The HTS will be maintained and updated during all phases of the life cycle, as will the risk management requirements.

2-13. System safety integration with systems engineering

a. DODI 5000.02 describes the Defense Acquisition Framework for materiel acquisition. DODI 5000.02 also directs the PM to integrate ESOH risk management into the overall systems engineering (SE) process for all developmental and sustaining engineering activities. In order to understand how the system safety process works within the overall acquisition structure, it is customary to view the process as a waterfall structure as shown in figure 2-4. The figure includes major milestones, reviews, and related technical baselines. It is DOD policy to integrate ESOH and HSI into SE throughout the acquisition framework. System safety is a major subset of both these programs and also includes some efforts and products unique to system safety.

b. This chapter includes a description of ESOH tasks in relation to the SE v-charts per the Defense Acquisition Guidebook. The v-charts depict when ESOH activities should be performed to influence the SE process. SE v-charts are shown for each phase, followed by a list of program inputs and outputs; ESOH activities that support each phase are listed following the SE v-charts, in relation to the individual inputs, outputs, and SE activities for each phase.

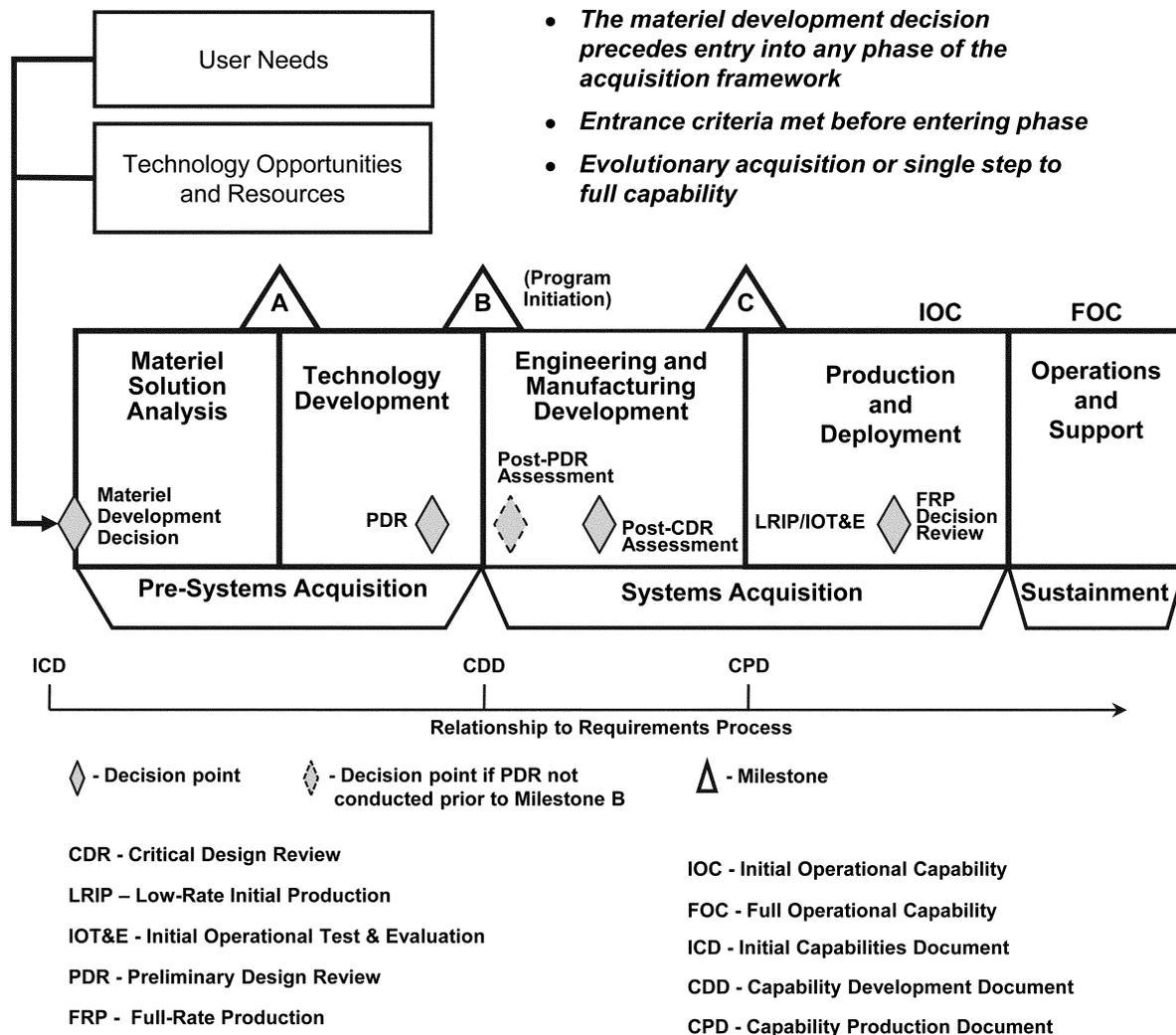


Figure 2-4. Defense Acquisition Framework

2-14. Materiel solution analysis

The purpose of this phase is to assess potential materiel solutions and to satisfy the phase-specific entrance criteria for the next program milestone designated by the milestone decision authority (MDA). Figure 2-5 below depicts the integration of system safety efforts into the SE process that begins during the materiel solution analysis phase. The significant system safety activities are to—

- Initiate development of top-level hazards analyses.
- Identify applicable environment, safety, and occupational health considerations and constraints, as part of the system-level trade studies.
- Review and provide inputs to initial capabilities document (ICD).

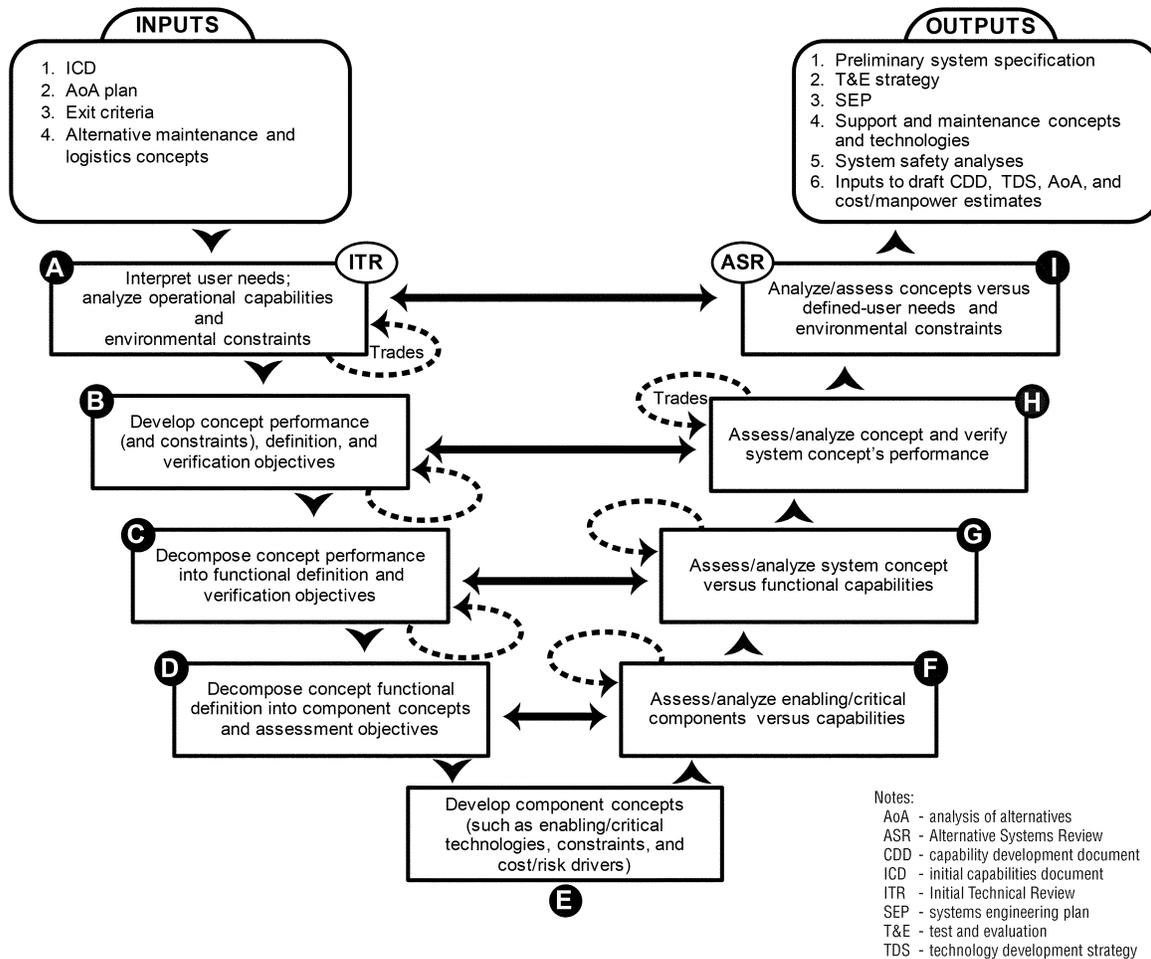


Figure 2-5. Materiel solution analysis v-chart

Table 2-2
Inputs of the materiel solution analysis phase

Inputs	System safety should—
ICD	Provide ESOH characteristics as part of the capability definition.
Analysis of alternatives (AoA) plan	Participate in AoA development.
Exit criteria	Provide the following exit criteria: -PHL. -Strategy for integrating ESOH risk management into the systems engineering plan (SEP).
Alternative maintenance and logistics concepts	Provide ESOH inputs.

Table 2–3
Steps of the materiel solution analysis phase

Step ²	System safety should—
A	Review the system threat assessment. Identify applicable ESOH criteria and asset requirement.
B	Assess each system concept against identified ESOH criteria and requirements.
C	Translate concept-level ESOH criteria (such as, air emissions, noise, hazardous material, effluents, and discharges) into functional requirements. Identify applicable verification objectives.
D	Initiate the PHL.
E	Prepare the PHL. Initiate identification of component ESOH constraints. Recommend ESOH input into projected system attrition rates. Review historical ESOH information (such as, successes, mishaps, and lessons learned) from similar or related legacy systems.
F	Identify ESOH requirements against critical component capabilities. Evaluate component test results against identified system constraints.
G	Evaluate ESOH functional requirements for the system concept, based on component test and analysis results.
H	Evaluate the system concept's ability to meet performance capability requirements within identified ESOH constraints.
I	Finalize the PHL for each system concept. Recommend the preferred ESOH approach for system concept.
Initial technical review	Identify applicable ESOH criteria for the system(s).
Alternative systems review	Prepare results of the PHL for each alternative, and recommend ESOH level of effort required for the technology development phase.
Trades	Participate in trade studies to identify potential top-level hazards, and ensure ESOH criteria are included in the trade studies throughout this phase.

Notes:

¹ Assess ESOH efforts using the system safety ESOH management evaluation criteria for DOD acquisition.

² The letters in this column correspond with the letters in figure 2–5 and are associated with the v-chart step boxes.

Table 2–4
Outputs of the materiel solution analysis phase

Outputs	System safety should—
Preliminary system specification	Provide PHL & ESOH criteria. Identify ESOH requirements, constraints, and performance attributes for the system. Incorporate ESOH requirements, as applicable.
T&E strategy	Provide approach to ESOH planning and the National Environmental Policy Act (NEPA) (Title 10, United States Code, Section 4321 et seq. (10 USC 4321 et seq.)/Executive Order (EO) 12114 compliance schedule. Provide ESOH hazard risk mitigation test and verification methodologies, and approach toward obtaining Safety Releases and ESOH risk acceptance.
SEP	Participate in developing the strategy for integrating ESOH risk management into SE using MIL–STD–882. Identify responsibilities for integrating ESOH into SE.
Support and maintenance concepts and technologies	Identify potential ESOH operations and maintenance issues, and identify emerging ESOH technologies and hazards.
System safety analysis	Ensure PHL has been completed for each system concept.
Inputs to draft CDD, technology development strategy, AoA, cost/manpower estimates	Provide ESOH inputs.
SSMP	Initiate plan.
SSWG	Establish a chartered SSWG.
Hazard tracking log	Establish a HTS.

Table 2-4
Outputs of the materiel solution analysis phase—Continued

Lessons learned	Collect lessons learned from predecessor systems to be used for mishap prevention.
-----------------	--

2-15. Technology development

The purpose of this phase is to reduce technology risk, determine, and mature the appropriate set of technologies to be integrated into a full system, and to demonstrate critical technology elements on prototypes. Technology development is a continuous technology discovery and development process reflecting close collaboration between the science and technology community, the user, and the system developer. It is an iterative process designed to assess the viability of technologies, while simultaneously refining user requirements. Figure 2-6, below, depicts the integration of system safety efforts into the SE process during technology development. In this phase, the integration of system safety efforts into the SE process involves—

- a.* Continuing development of the requirements.
- b.* Identifying top-level hazards as part of participation in the trade studies.
- c.* Anticipating applicable system-level requirements for environment, safety, and occupational health as the technologies are integrated into the system.

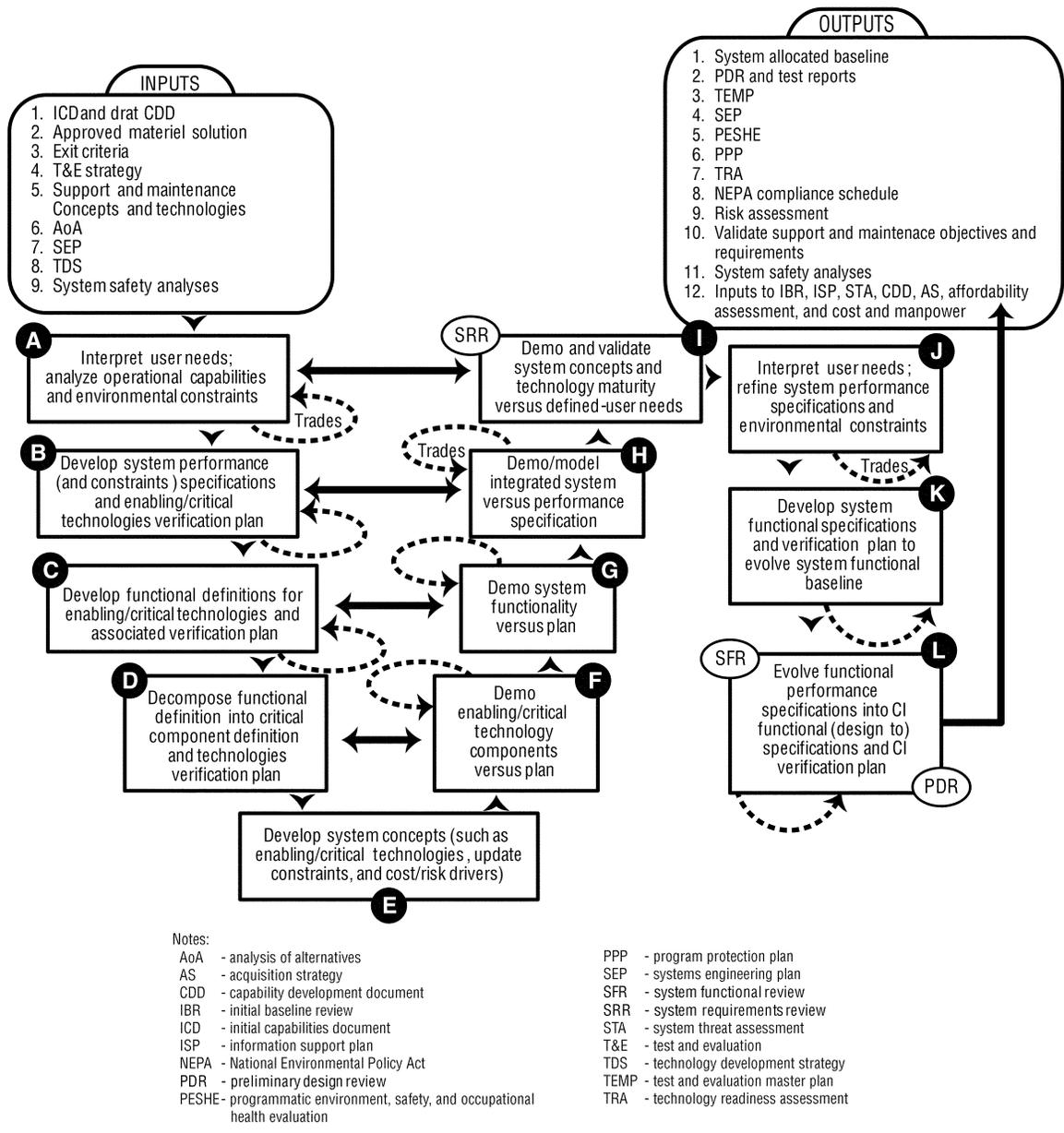


Figure 2-6. Technology development v-chart

Table 2-5
Inputs of the technology development phase

Inputs	System Safety should:
ICD and draft CDD	Develop and/or coordinate ESOH criteria and requirements. Identify ESOH constraints and performance attributes for the system.
Approved materiel solution	Evaluate the approved materiel solution identified ESOH criteria.
Develop exit criteria	Provide the following exit criteria: Update the PHL. Update strategy for integrating ESOH risk management into SE.
T&E strategy	Incorporate ESOH hazard risk mitigation test and verification methodologies, and work towards obtaining Safety Release(s) and ESOH risk acceptance. Include the ESOH planning strategy and requirements to support T&E (to include NEPA/EO 12114 compliance).

**Table 2-5
Inputs of the technology development phase—Continued**

Support and maintenance concepts and technologies	Provide ESOH inputs, as requested.
AoA	Characterize ESOH footprints and risks for AoA development.
SEP	Update the strategy for integrating ESOH risk management into SE.
Technology development strategy	Include strategy to identify hazards and needed ESOH technology development.
System safety analyses	Initiate safety requirements analysis (SRA) and update PHL for preferred concept.

**Table 2-6
Steps of the technology development phase**

Step ²	System safety should—
A	Update identification of ESOH constraints. Develop ESOH criteria (such as, air emissions, noise, hazardous materials, effluents, and discharges). Identify ESOH-critical technology needs.
B	Update ESOH criteria. Include ESOH-critical specifications in the verification plan. Identify ESOH requirements in any system or subsystem performance specification, solicitation, contract, and evaluation criteria.
C	Update system ESOH criteria. Develop requirements for verification of risk mitigation controls.
D	Update system ESOH criteria. Develop requirements for verification of component risk mitigation controls.
E	Update PHL. Update ESOH constraints. Identify potential operational and maintenance ESOH training and staffing requirements. Refine ESOH input for system attrition rates. Identify ESOH hazard mitigation, IMs, mishap reduction, and safety technology requirements.
F	Evaluate enabling/critical technologies from an ESOH perspective. Review demo results for new technology component ESOH hazards.
G	Evaluate enabling/critical technologies from an ESOH perspective. Review demo results for new ESOH hazards.
H	Evaluate enabling/critical technologies from an ESOH perspective. Review demo results for new ESOH hazards.
I	Evaluate enabling/critical technologies from an ESOH perspective.
J	Develop life cycle ESOH footprint and system boundaries. Develop more detailed ESOH criteria (for example, air emissions, noise, hazardous materials, effluents, and discharges). Identify and develop ESOH-critical requirements, and verify they are included in the requirements tracking system. Provide ESOH activities for inclusion in the integrated master schedule.
K	Initiate development of PHA and threat hazard analysis. Update ESOH criteria. Verify ESOH-critical functional specifications are included in the requirements tracking system and system verification plan. Verify NEPA and EO 12114 requirements are met at proposed testing and training locations. Identify ESOH requirements in any system or subsystem solicitation or contract.
L	Finalize PHA. Update ESOH criteria for component, subsystem, and system to include test requirements. Expand and update SRA to include functional specifications as detailed design specifications evolve. Verify that ESOH-critical design specifications are included in the requirements tracking system, detailed design specifications, and configuration item verification plan.
System requirements review	Prepare and present ESOH performance criteria at system requirements review.
System functional review	Present ESOH-critical requirements and risk status at system functional review.
Preliminary design review (PDR)	Present PHA and identify ESOH hazards and risk status at PDR; ensure ESOH requirements are in product specifications and the integrated master schedule.

**Table 2–6
Steps of the technology development phase—Continued**

Trades	Participate in trade studies to evaluate options against identified ESOH criteria throughout this phase.
--------	--

Notes:

¹ Assess ESOH efforts using the system safety ESOH management evaluation criteria for DOD acquisition.

² The letters in this column correspond with the letters from figure 2–6 and are associated with the v-chart step boxes.

**Table 2–7
Outputs of the technology development phase**

Outputs	System safety should—
System allocated baseline	Include ESOH criteria and requirements, SRA data, and applicable specifications. Require concurrence and approvals from the applicable safety boards.
PDR and test reports	Provide ESOH inputs (such as, ESOH risks status, new hazards identified, and effectiveness of mitigation measures).
TEMP	Document Safety Release(s) and specific ESOH test requirements, to include verification of risk mitigation measures and risk acceptance. Include ESOH planning strategy and requirements to support T&E, to include NEPA/EO 12114 compliance.
SEP	Update strategy for integrating ESOH risk management into SE. Identify applicable safety boards and process for concurrence/approval.
PESHE	Identify ESOH responsibilities. Develop strategy for integrating ESOH considerations into SE. Identify preliminary ESOH risks/status. Describe method for tracking hazards. Develop NEPA/EO 12114 compliance schedule. Identify applicable safety boards and processes for concurrence and approval. Ensure ESOH effort is resourced.
Program protection plan	Provide ESOH inputs, as requested.
Technology readiness assessment	Update ESOH risk mitigation technology readiness levels (for example, IM technology).
NEPA compliance schedule	Include all actions that may trigger NEPA/EO 12114 and assess applicability and compliance.
Risk assessment	Document and report risk status and risk acceptance decisions. Document concurrence and approval of applicable safety boards.
Validated system support and maintenance objectives and requirements	Provide preliminary ESOH input.
System safety analyses	Ensure completion of SRA, and update PHL for the approved materiel solution. Initiate or update safety requirements and analysis. Participate in design reviews. Update HTS. Identify all residual risks, and prepare the required SSRAs.
Inputs to integrated baseline review, information support plan, system threat assessment, CDD, AS, affordability assessment, cost and manpower estimates	Provide ESOH hazard mitigation, IM, mishap reduction, and safety technology requirements. Incorporate NEPA/EO 12114 compliance schedule and summary of the PESHE in the SEP. Identify ESOH requirements, constraints, and attributes for the system.
SSMP	Initiate or update plan.
Developmental tests (DTs)	Provide ATEC required ESOH information.
Surface danger zone (SDZ)	Conduct modeling and simulation. Develop initial SDZ.
Explosive hazard classification	Prepare interim hazard classification. Final hazard classification. Conduct subsystem tests.
HFE analyses	Provide applicable safety input.

**Table 2-7
Outputs of the technology development phase—Continued**

Radiation authorizations and licenses	Coordinate with the commodity command radiation safety officer (and Nuclear Regulatory Commission (NRC)).
Health hazard assessment (HHA)	Coordinate with U.S. Army Institute of Public Health (USAIPH).
Air worthiness statement	Obtain an air worthiness release per AR 70-62.
Army Fuze Safety Review Board approval	Ensure Army Fuze Safety Review Board review, when required, per MIL-STD- 1316E.
Army Ignition System Safety Review Board approval	Ensure Ignition System Safety Review Board review, when required, per MIL-STD-1901A.
Safety Release/Confirmation	Obtain a Safety Release or Safety Confirmation from ATEC, per AR 70-1.
Explosive ordnance disposal (EOD) supportability statement	Obtain an EOD supportability statement, when required, per AR 75-15.
Energetic Material Qualification Board certification	Obtain certification when required per North Atlantic Treaty Organization Standardization Agreement 4170 (STANAG 4170).
TMs	Ensure the system safety review of TMs prior to the materiel release of a system per AR 700-142.
Software safety statement	Prepare a software safety statement prior to the release of software upgrade/updates, per AR 700-142.
Equipment safety inspections and analyses	Conduct safety inspections to identify compliance to specification and potential hazards.
Lessons learned	Collect lessons learned to be used in follow-on procurements and other system developments.

2-16. Engineering and manufacturing development

a. The purpose of the engineering and manufacturing development phase is to develop a system or an increment of capability; complete full system integration (technology risk reduction occurs during technology development); develop an affordable and executable manufacturing process; ensure operational supportability with particular attention to minimizing the logistics footprint; implement HSI; design for producibility; ensure affordability; protect critical program information by implementing appropriate techniques, such as anti-tamper; and demonstrate system integration, interoperability, safety, and utility. The majority of system safety activities occur in this phase, relying heavily on the planning and analysis conducted in materiel solution analysis and technology development.

b. The integration of system safety efforts into the SE process continues in the engineering and manufacturing development phase as depicted in figure 2-7, below. It is important that SSE personnel be active participants in both trade studies and technical reviews conducted during this phase, such as the PDR where the final PHA will be presented, and at the critical design review (CDR) when the following documents would be discussed:

- (1) The subsystem hazard analysis and system hazard analysis should be nearing completion.
- (2) The operating and support hazard analysis (O&SHA) should have been initiated.

c. After the CDR, these analyses continue to be updated, along with the execution of safety verification activities. The analyses will influence engineering plans, requirements, and specifications; trade studies; T&E; technical reviews; and production and operational planning.

d. The PESHE is updated to support the Milestone C and full-rate production review processes.

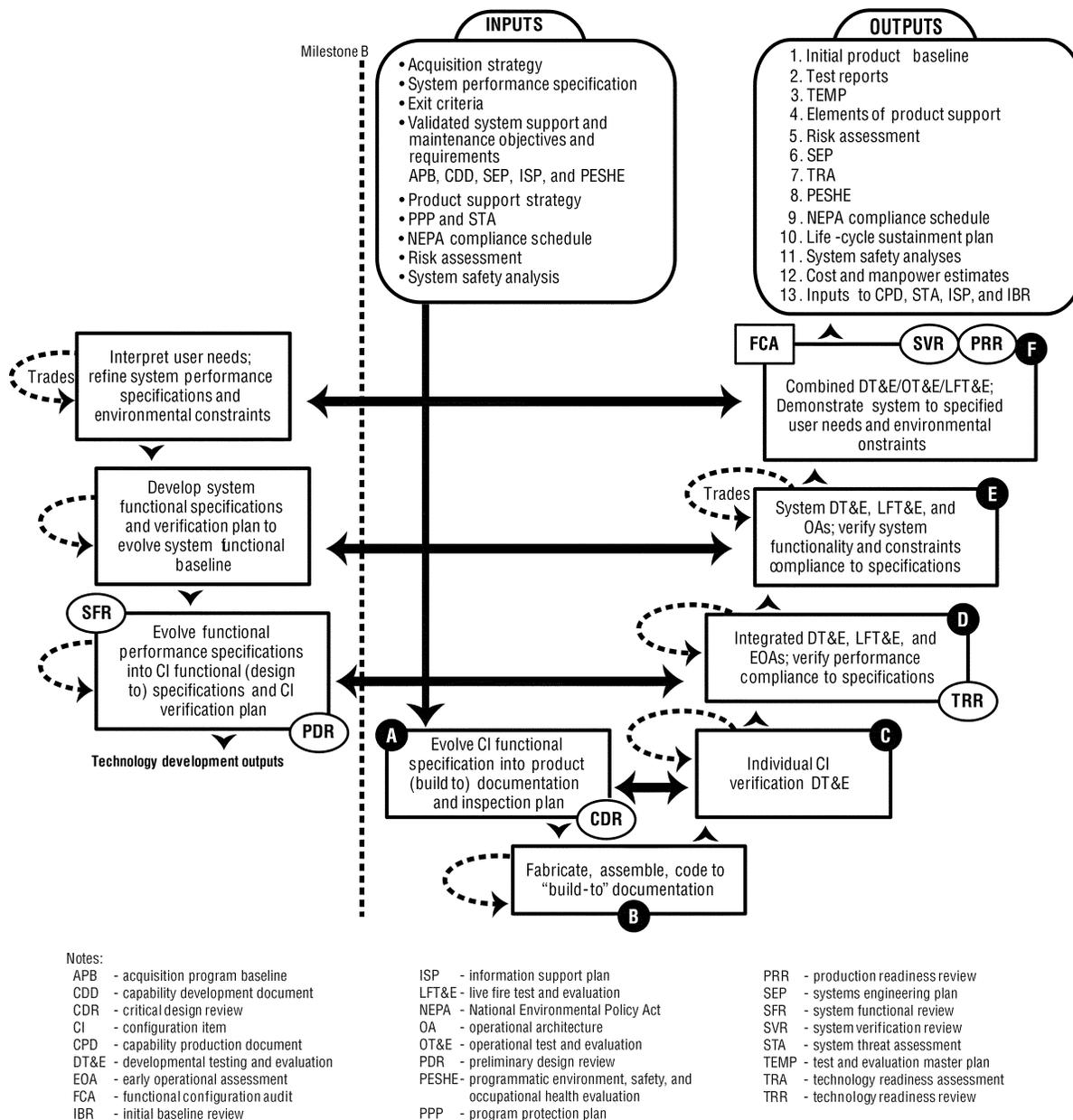


Figure 2-7. Engineering and manufacturing development v-chart

**Table 2–8
Steps of the engineering and manufacturing development phase**

Step ²	System safety should—
A	<p>Prepare subsystem hazard analysis, system hazard analysis, O&SHA, and update the SRA. Update ESOH criteria for component, subsystem, and system, to include test and inspection requirements. Identify ESOH input for demilitarization and disposal planning. Identify ESOH critical process for product build-to-documentation (such as, safety-critical items list). Include system ESOH-critical processes and components in inspection plan (for example, component screening and testing). Participate in component design selections. Initial presentations to system safety boards, as appropriate. Verify system ESOH-critical design specifications are included in the requirements tracking system and detailed in design specifications.</p>
B	<p>Evaluate, process, and design changes, as necessary. Review and recommend ESOH updates to the TEMP. Ensure configuration item verification developmental T&E procedures include ESOH requirements and verification testing. Initiate Safety Releases based on the SAR and ESOH risk acceptance documentation, as appropriate, for user tests.</p>
C	<p>Ensure that ESOH tests were conducted, and results were reviewed for effectiveness of mitigation measures. Update hazard status. Verify that integrated developmental T&E, live fire T&E, and early operational assessment procedures include appropriate tests derived from system safety analyses and environmental reviews. Recommend ESOH hazard closure, based on test results. Obtain Safety Releases based on the SAR, HHA, and ESOH risk acceptance documentation, as appropriate, for user tests. Ensure NEPA and EO 12114 compliance is completed prior to testing.</p>
D	<p>Ensure that tests were conducted, and results were reviewed for effectiveness of hazard mitigation measures. Update hazard status, hazard analyses, and threat hazard analysis, based on configuration changes. Assess configuration changes for test and document results. Continue to provide ESOH input for demilitarization/disposal planning. Verify system developmental T&E, live fire T&E, and early operational assessment procedures include appropriate tests derived from system safety analyses and environmental reviews. Recommend ESOH hazard closure based on test results. Obtain Safety Releases based on the SAR and ESOH risk acceptance for upcoming test activities, as appropriate.</p>
E	<p>Ensure that ESOH tests were conducted, and results were reviewed for effectiveness of mitigation measures. Update ESOH hazard status and analyses based on configuration changes. Assess configuration changes for testing and document results. Verify combined developmental T&E/operational assessment/live fire T&E procedures include appropriate tests derived from system safety analyses and environmental reviews. Recommend ESOH hazard closure based on test results, as appropriate. Obtain Safety Release based on the SAR and ESOH risk acceptance for upcoming test activities, as appropriate. Ensure NEPA and EO 12114 compliance is completed prior to testing.</p>
F	<p>Ensure that tests were conducted, and results were reviewed for ESOH considerations, newly identified ESOH hazards, and effectiveness of risk mitigation measures; recommend hazard closure, as appropriate. Update ESOH hazard status and hazard analyses, based on configuration changes. Ensure NEPA and EO 12114 compliance is completed prior to testing. Continue to identify and provide ESOH input for demilitarization and disposal planning.</p>
Test readiness review	<p>Assess configuration for testing, document, and present results; ensure all Safety Releases and ESOH risk acceptances are completed; report ESOH risks and their status; and ensure NEPA and EO 12114 compliance.</p>
Production readiness review	<p>Present ESOH-critical requirements, ESOH risks, and their acceptance status.</p>
System verification review	<p>Present ESOH risk to the user.</p>
Functional configuration audit	<p>Review the functional configuration audit for consistency with ESOH requirements.</p>
CDR	<p>-Present ESOH hazards and risks and their acceptance status; ensure ESOH requirements are in product specifications and the integrated master schedule.</p>
Trades	<p>Ensure ESOH professional participation in the trade studies to evaluate options against established criteria throughout this phase.</p>

Notes:

¹ Assess ESOH efforts using the system safety ESOH management evaluation criteria for DOD acquisition.

² The letters in this column correspond with the letters in figure 2–7 and are associated with the v-chart step boxes.

Table 2–9
Outputs of the engineering and manufacturing development phase

Outputs	System safety should—
Initial product baseline (integrated baseline review)	Ensure that ESOH-critical items and processes are included in the baseline. Identify inspection requirements.
Test reports	Verify that mitigation measures reduce ESOH hazard risk effectively. Analyze anomalies, incidents, and mishaps.
TEMP	Update specific test and Safety Release requirements based on the SAR, and include requirements for verification of risk mitigation measures. Validate the NEPA/EO 12114 compliance schedule.
Elements and product support	Provide the results of the preliminary O&SHA
Risk assessment	-Document and report risk status and risk acceptance decisions -Document concurrence and approval of applicable safety boards
SEP	Update the strategy for integrating ESOH risk management into SE
Technology readiness assessment	Update the ESOH risk mitigation technology readiness levels
PESHE	Update the PESHE to identify ESOH responsibilities; the strategy for integrating ESOH considerations into SE; identify ESOH risk/status; describe method for tracking hazards; identify hazardous materials/wastes and pollutants used on the system, and plans for their minimization and/or safe disposal; and NEPA/EO 12114 compliance schedule.
NEPA compliance schedule	Update to ensure NEPA/EO 12114 requirements are met at proposed testing, training, and basing locations.
Life cycle sustainment plan	Provide results of O&SHA and other relevant ESOH data.
System safety analyses	Ensure completion of PHA and SRA. Finalize the subsystem hazard analysis, system hazard analysis, and threat hazard analysis. Finalize the preliminary O&SHA. Identify ESOH requirements, constraints, footprint, and performance attributes.
Cost and manpower estimate	Recommend operational and maintenance ESOH training and staffing requirements. Update system attrition rate inputs, due to mishaps and ESOH hazard mitigation, IM, safety technology requirements, and mishap reduction requirements.
Inputs to capability production document, system threat assessment, in-service review, and integrated baseline review	Provide ESOH hazard mitigation IM, mishap reduction, and safety technology requirements. Identify ESOH requirements, constraints, and attributes for the system.
System safety analysis	Initiate or update safety requirements and analysis. Participate in design reviews. Update HTS. Identify all residual risks, and prepare the required SSRAs.
SSMP	Initiate or update plan.
DTs	Provide ATEC-required ESOH information.
SDZ	Conduct modeling and simulation. Develop initial SDZ.
Explosive hazard classification	Prepare interim hazard classifications. Final hazard classification. Conduct subsystem tests.
HFE analyses	Provide applicable safety input.
Ionizing radiation authorizations and licenses	Coordinate with the commodity command radiation safety officer (and NRC).

Table 2-9
Outputs of the engineering and manufacturing development phase—Continued

Radiofrequency radiation study - Hazards of electromagnetic radiation to ordnance - Hazards of electromagnetic radiation to fuel - Hazards of electromagnetic radiation to personnel	Coordinate with ATEC and USAIPH for needed data to support analysis.
Laser/Optical radiation study	Coordinate with ATEC and USAIPH for needed data to support analysis.
HHA	Coordinate with USAIPH.
Air worthiness release	Obtain an air worthiness per AR 70-62.
Army Fuze Safety Review Board approval	Ensure Army Fuze Safety Review Board review, when required, per MIL-STD-1316E.
Army Ignition System Safety Review Board approval	Ensure Ignition System Safety Review Board review, when required, per MIL-STD-1901A.
Safety Release/Confirmation	Obtain a Safety Release or Safety Confirmation from ATEC, per AR 70-1.
EOD supportability statement	Obtain an EOD supportability statement, when required, per AR 75-15.
Energetic Material Qualification Board certification	Obtain certification, when required, per NATO STANAG 4170.
TMs	Ensure the system safety review of TMs prior to the materiel release of a system, per AR 700-142.
Software safety statement	Prepare a Software safety statement prior to the release of software upgrades/updates, per AR 700-142.
Equipment safety inspections and analyses	Conduct safety inspections to verify compliance to specifications and identify potential hazards.
Lessons learned	Collect lessons learned to be used in follow-on procurements and other system developments.

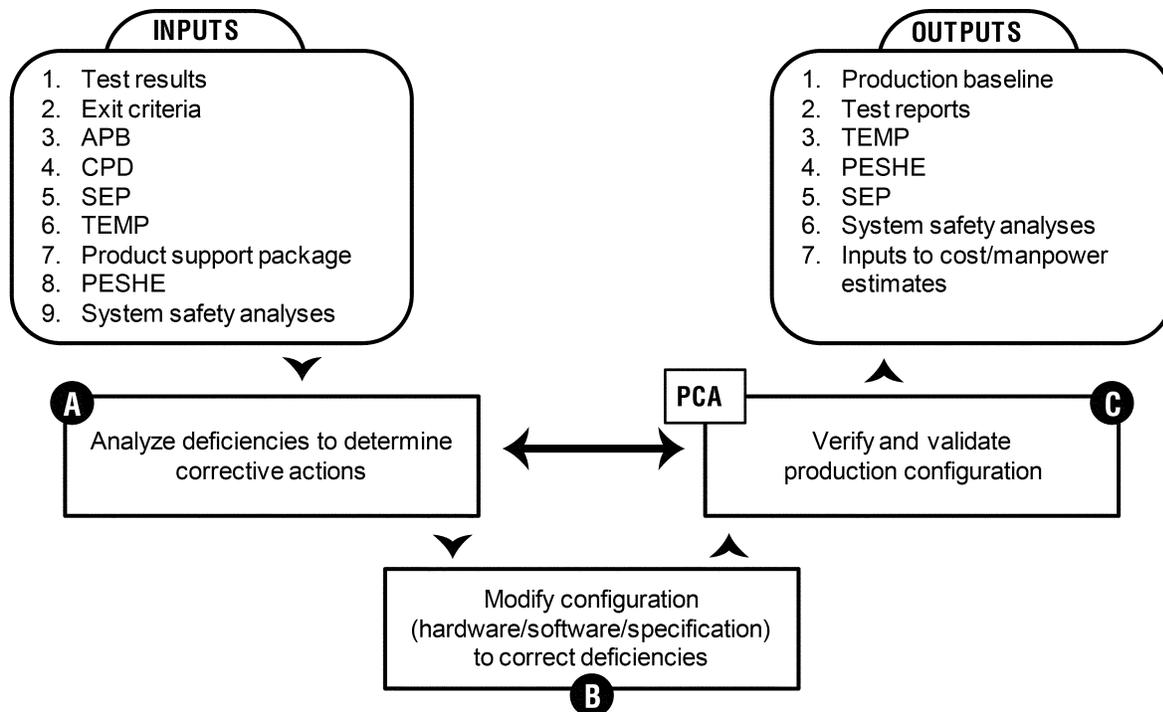
2-17. Production and deployment phase

a. The purpose of the production and deployment phase is to achieve an operational capability that satisfies mission needs. Operational T&E will determine the effectiveness and suitability of the system. In this phase, system safety is focused on—

- (1) Analyzing deficiencies.
- (2) Participating on the configuration control board.
- (3) Verifying and validating safety-critical item production configuration.
- (4) Reviewing the physical configuration audit to identify potential safety impacts.

b. Hazards continue to be identified, assessed, mitigated, and tracked to closure in the HTS.

c. Figure 2-8, below, depicts the integration of system safety efforts into the SE processes during the production and deployment phase.



- Notes:
- APB - acquisition program baseline
 - CPD - capability production document
 - PCA - physical configuration audit
 - PESHE - programmatic environment, safety, and occupational health evaluation
 - SEP - systems engineering plan
 - TEMP - test and evaluation master plan

Figure 2–8. Production and deploymentv-chart

Table 2–10
Inputs of the production and deployment phase

Inputs	System safety should—
Test results	Review initial operational T&E results for effectiveness of risk mitigation controls. Analyze anomalies, incidents, and mishaps.
Exit criteria	Document formal risk disposition of identified hazards, such as SAR. Obtain concurrence/approval of appropriate safety boards as required (such as, Army Fuze Safety Review Board, and so forth). Update PESHE. Provide updated inputs for demilitarization and disposal plan.
Acquisition program baseline	Provide inputs as requested for ESOH. PM should be made aware of ESOH issues that could significantly affect acquisition program baseline for cost, schedule, or performance. Provide the PM ESOH assistance, if required, in making tradeoff decisions.
Capability production document	Update hazard mitigation requirements as necessary. Update IM requirements as necessary. Identify mishap reduction requirements as necessary.
SEP	Update strategy for integrating ESOH risk management into SE. Identify applicable safety boards and process for concurrence/approval.

Table 2-10
Inputs of the production and deployment phase—Continued

TEMP	Update specific test requirements (such as, MIL-STD-2105D, MIL-STD-1316E, MIL-STD-331C, MIL-STD-1901A, Institute of Electrical and Electronic Engineers (IEEE)/Electronic Industry Association (EIA) 12207, 29 Code of Federal Regulations (CFR) 1910.95). Update requirements for verification of risk mitigation controls (based upon system safety analysis). Update Safety Release requirements/documents (for example, SAR, most recently published HHA, and so forth).
Product support package	Include O&SHA results.

Table 2-11
Steps of the production and deployment phase

Step ²	System safety should—
A	Review deficiency reports for system safety implications. Participate in development of corrective actions. Participate in configuration control board to include reviewing of engineering change proposals.
B	Identify system safety-critical items and inspection requirements. Review and recommend updates to TEMP/test plan, based upon system safety analyses. Provide Safety Release documentation as appropriate.
C	Verify and validate system safety-critical item configuration. Participate in test activities as appropriate.
Operational test readiness review	Update SAR to support the PM's requirement to provide a Safety Release.
Physical configuration audit	Review PCA to identify potential system safety implications.

Notes:

¹ Assess ESOH efforts using the system safety ESOH management evaluation criteria for DOD acquisitions.

² The letters in this column correspond with the letters in figure 2-8 and are associated with the v-chart step boxes.

Table 2-12
Outputs of the production and deployment phase

Outputs	System safety should—
Production baseline	Identify system safety-critical items and processes. Specify inspection requirements. Document concurrence/approvals of applicable safety boards.
Test reports	Document effectiveness of risk management controls. Document findings from anomalies, incident, and mishaps.
TEMP	Update specific test requirements (such as, MIL-STD-2105D, MIL-STD-1316E, MIL-STD-331C, MIL-STD-1901A, IEEE/EIA 12207, 29 CFR 1910.95). Update requirements for verification of risk mitigation controls (based upon system safety analysis). Update/obtain Safety Release for test requirements/documents (for example, SAR, most recently published HHA, NEPA, and so forth).
PESHE	Update hazard status. Update hazard analysis. -Identify applicable safety boards and process concurrence/approval.
NEPA/EO 12114 compliance document	Update the NEPA/EO 12114 document (for example, categorical exclusion, environmental assessment, finding of no significant impact, environmental impact statement, record of decision, overseas environmental assessment, and overseas environmental impact statement) which the proponent should complete prior to the proposed action start date.
SEP	Update strategy for integrating ESOH risk management into SE. Identify applicable safety boards and process concurrence/approval.

Table 2–12
Outputs of the production and deployment phase—Continued

System safety analysis	Update safety requirements and analysis. Participate in design reviews. Update HTS. Identify all residual risks, and prepare the required SSRAs.
Input to cost/Manpower estimate	Recommend training and staffing requirements. Update system attrition rate input due to mishaps.
SSMP	Update plan.
Operational tests	Provide ATEC-required ESOH information, so that they can prepare Safety Release for test.
Materiel release	Document the system safety assessment in a SHDS (per AR 700–142) to support of materiel release.
Type classification	Document the system safety assessment in a SHDS (per AR 700–142) to support type classification.
Safety Confirmation	Provide ATEC-required ESOH information, so that they can prepare a Safety Confirmation that supports materiel release, type classification, and milestone decisions.
Materiel fielding plan	Provide applicable safety input.
Lessons learned	Collect lessons learned to be used in follow-on procurements and other system developments.

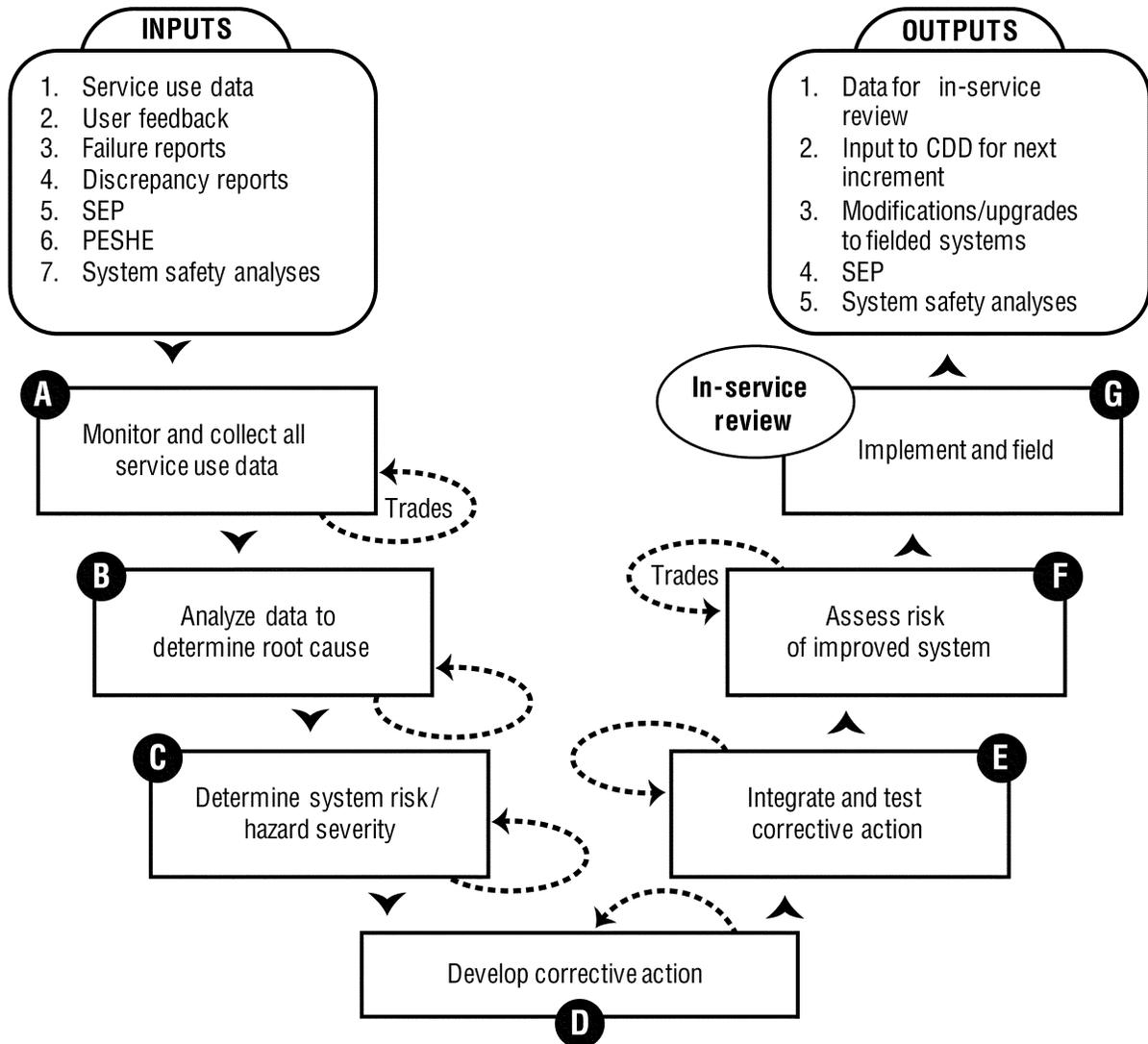
2–18. Operations and support

a. The purpose of the operations and support phase is to execute a support program that meets materiel readiness and operational support performance requirements and sustains the system in the most cost-effective manner over its total life cycle. During this phase, system safety is focused on—

- (1) Analyzing deficiencies, system health, and mishaps.
- (2) Participating on the configuration control board.

b. Hazards continue to be identified, assessed, mitigated, and tracked to closure in the HTS.

c. Figure 2–9, below, depicts the integration of system safety efforts into the SE processes during the operations and support phase.



Notes:
 CDD - capability development document
 PESHE- programmatic environment, safety, and occupational health evaluation
 SEP - systems engineering plan

Figure 2-9. Operations and support v-chart

Table 2–13
Inputs of the operations and support phase

Inputs	System safety should—
Service use data	Review for system safety implications.
User feedback	Review for system safety implications.
Failure reports	Review follow-on operational T&E results for system safety implications. Review failure/mishap reports for causal factors or mitigation failures, and recommend alternative mitigation measures. Assist in mishap investigations, as requested.
Discrepancy reports	Review discrepancy reports for system safety implications.
SEP	Update strategy for integrating ESOH risk management into SE. Identify applicable safety boards and process for concurrence/approval.
SSMP	Update plan.

Table 2–14
Steps of the operations and support phase

Step²	System safety should—
A	Provide system safety review criteria to engineering and logistics staff. Review data for system safety implications (for example, trend analysis). Identify opportunities for technology insertion to reduce risk (new technologies, obsolescence).
B	Apply appropriate system safety analysis techniques to determine root cause (for example, failure modes, effects, and criticality analysis (FMECA), fault tree analysis). Evaluate data for system safety implications. Update hazard analyses/database as appropriate.
C	Prioritize hazards for risk mitigation. Update hazard analyses/database as appropriate.
D	Apply system safety order of precedence to corrective actions. Update hazard analyses/database as appropriate. Identify requirements for verification of risk mitigation controls (based upon updated system safety analyses).
E	Evaluate test results for risk mitigation effectiveness. Update hazard analyses/database as appropriate.
F	Update hazard analyses/database as appropriate. Recommend hazard closure to appropriate risk acceptance authorities (updated residual risk).
G	Continue to track system health, mishaps, hazards, closure actions, mitigation measure effectiveness, and residual risk.
In-service review	Provide inputs to the in-service review on mishaps. Provide inputs to the in-service review on any newly identified hazards with assessment of risks, selected mitigation measures, verification of mitigation controls, and acceptance of residual risks.
Trades	Participate in the trade studies to evaluate options against established system safety criteria.

Notes:

¹ Assess ESOH efforts using the system safety ESOH management evaluation criteria for DOD acquisition.

² The letters in this column correspond with the letters in figure 2–9 and are associated with the v-chart step boxes.

Table 2–15
Outputs of the Operations and Support Phase

Outputs	System safety should—
Input to CDD for next increment	Update hazard mitigation requirements as necessary. Update IM requirements as necessary. Update mishap reduction requirements as necessary.
Modifications/upgrades to fielded systems	Recommend an appropriate funding level for system safety. Present updated residual risk to user (such as, safety assessment). Update HTS as required. Provide updated inputs for demilitarization/disposal plan. Provide the required SHDS (app J) to support modification work orders or follow-on release actions.
SEP	Update strategy for integrating ESOH risk management into SE. Identify applicable safety boards and process for concurrence/approval. Update SSMP.
Safety messages	Provide support in the preparation and coordination of safety messages per AR 750–6.
Field assistance	Provide ESOH field support.
Lessons learned	Collect lessons learned to be used in system modifications, follow-on procurements, and other system developments.
Configuration management safety	Review all configuration changes, deviations, waivers for safety impact.

Chapter 3

Integration of System Safety Associated Disciplines

3–1. General

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

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

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

3–2. Systems engineering

a. System safety is a subset of SE. Rigorous SE discipline is necessary across the acquisition life cycle to ensure that the Army meets the challenge of developing and maintaining needed warfighting capability. SE provides the integrating technical processes to define and balance system performance, cost, schedule, and risk within a family-of-systems and SOS context. SE shall be embedded in program planning and be designed to support the entire acquisition life cycle.

b. An SEP is prepared and updated for each milestone review, beginning with Milestone A. At Milestone A, the SEP supports the technology development strategy; at Milestone B or later, the SEP supports the AS. The SEP describes the program’s overall technical approach, including key technical risks, processes, resources, metrics, and applicable performance incentives. It details the timing, conduct, and success criteria of technical reviews.

c. The SEP describes how SSE efforts are integrated across disciplines and into SE to determine system design characteristics that can minimize the risks of acute or chronic illness, disability, death, or injury to operators and maintainers; and enhance job performance and productivity of the personnel who operate, maintain, or support the system.

d. ESOH risk management must be integrated into the overall SE process for all developmental and sustaining engineering activities. As part of risk reduction, ESOH hazards should be eliminated where possible, and manage ESOH risks where hazards cannot be eliminated. Methodology detailed in MIL–STD–882 will be used to guide this process. The status of ESOH risks and acceptance decisions at technical reviews will be reported. Acquisition program reviews and fielding decisions shall address the status of all high and serious risks and applicable ESOH technology requirements. Prior to exposing people, equipment, or the environment to known system-related ESOH hazards, the associated risks must be accepted by the appropriate acceptance authority (see chap 2 of this pamphlet). The user

representative shall be part of this process throughout the life cycle and shall provide formal concurrence, prior to all serious and high-risk acceptance decisions.

e. Programs, regardless of acquisition category (ACAT) level, will develop a PESHE which incorporates the MIL-STD-882 process and includes the following: identification of ESOH responsibilities; the strategy for integrating ESOH considerations into the SE process; identification of ESOH risks and their status; a description of the method for tracking hazards throughout the life cycle of the system; identification of hazardous materials, wastes, and pollutants (discharges/emissions/noise) associated with the system and plans for their minimization and/or safe disposal; and a compliance schedule covering all system-related activities for NEPA and EO 12114. The SEP incorporates a summary of the PESHE, including the NEPA/EO 12114 compliance schedule.

f. Programs will support system-related Class A and B mishap investigations per AR 385-10 by providing analyses of hazards that contributed to the mishap and recommendations for materiel risk mitigation measures, especially those that minimize human errors. If specific hazard related mishaps are occurring at greater than the previously assessed severity and probability, the risk assessment must be reassessed and managed at the appropriate level of authority.

3-3. Reliability, availability, and maintainability

a. A reliability, availability, and maintainability program is required for most systems, per DODD 5000.01.

b. Reliability is the probability that an item will perform its intended function for the duration of a mission or a specific time interval. It is usually stated as a mean time (or distance, rounds, and so forth) between failures. The requirement for a reliability program plan (see Government Electronics and Information Technology Association standard 0009 (GEIA-STD-0009) is normally incorporated into the request for proposal (RFP). Provisions will be made for the SSWG to examine reliability test reports (for example, DI-TMSS-81586A) and failed item reports (for example, DI-QCIC-80131). Environmental factors, failure rates, failure modes, mean time between failures, and problems associated with major items of system equipment are usually contained in these reports.

c. Availability is the percentage of time an item is in a mission-committable status expressed as inherent, achieved, or operational availability. An FMECA report (DI-QCIC-81495) will normally be required as a part of the reliability program. The contractor's integration of the results of the FMECA into their system safety program will be established as criteria for the system safety engineering plan (SSEP) evaluation during source selection in those cases where the FMECA is required.

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

3-4. Quality engineering

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

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

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

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

c. The PM will ensure that the SSWG monitors the critical items and service life surveillance programs. Also, the PM must ensure contractor integration of those programs into the contractor's system safety program by requiring a quality program plan (DI-QCIC-81722) in the RFP and establishing it as evaluation criteria for the SSEP and for the quality program plan during source selection.

3-5. Integrated logistics support

As one of its primary tools, integrated logistics support employs a management science application termed LSA.

a. An LSA is required for all acquisition programs by AR 700-127 and should be established per MIL-HDBK-502. The logistic support analysis record (LSAR) (see GEIA-STD-0007) is a manual and/or automated database that is used to document, consolidate, and integrate the detailed engineering and logistics data generated by the LSA process.

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

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

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

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

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

3–6. Combat survivability

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

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

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

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

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

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

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

3–7. Human factors engineering

a. The HFE program is a domain of MANPRINT and a life cycle activity responsible for properly integrating the human element into systems. The DCS, G–1 exercises staff responsibility for the HFE program, and AMC has the system integration responsibility. AR 602–2 provides policy and guidance for the MANPRINT program and HFE assessments.

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

c. Human factors hazard identification and management is an integral part of HFE. Life cycle tests, analyses, and other tasks must include efforts to ensure critical human performance problems (actual or potential) are being systematically identified and managed to reduce risk. Key sources of information include accident and incident data,

system hazard analyses, and other information from predecessor and current systems. These analyses will help establish the severity and probability or safety-related human performance problems for risk assessments, management, and tradeoffs.

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

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

3-8. Health hazards

a. The Surgeon General is the proponent of AR 40-10, maintains staff responsibility for the regulation that implements the Army HHA program, prescribes specific HHA responsibilities for the acquisition and AMEDD communities in support of the Army acquisition process, and describes the HHA Program as an integrated effort throughout the life cycle of a system. Specifically, AR 40-10 considers mission needs, concept analysis, research, development, testing, evaluation, procurement, training, use, storage, system maintenance, and disposal. The Surgeon General also—

- (1) Determines if Army materiel presents a health hazard to personnel and provides all medical policies, health standards, exposure limits, and recommendations to control such health hazards.
- (2) Designates USAIPH as the lead agency for implementing the AMEDD responsibilities for the Army's HHA program.
- (3) Designates the Commanding General, U.S. Army Medical Research and Materiel Command, as Deputy for Medical Systems to assist the Assistant Secretary of the Army for Acquisition, Logistics and Technology and the Army Acquisition Executive (AAE) with health hazards of medical and nonmedical systems acquisitions.
- (4) Provides AMEDD review of concept, requirement, and capability documents through the U.S. Army Medical Department Center and School.
- (5) Staffs, plans, programs, and budgets for implementation of the AMEDD responsibilities of the Army's HHA Program.

b. The primary objective of the HHA program is to identify and assess health hazards associated with the life cycle management of the following systems and provide recommendations to MATDEVs and CAPDEVs to eliminate or control the hazards: weapons platform, munitions, equipment, clothing, training devices, and other materiel systems. The Army's effort to eliminate health hazards from materiel systems links the HHA program with Army warfighting capabilities and performance. The specific HHA program objectives include—

- (1) Preserve and protect the health of individual Soldiers.
- (2) Reduce degradation of Soldier performance and enhance system effectiveness.
- (3) Design out health hazards to eliminate the need for health hazard-based retrofits.
- (4) Reduce readiness deficiencies attributable to health hazards, thereby reducing training or operational restrictions.
- (5) Reduce personnel compensation claims by eliminating or reducing injury or illness caused by health hazards associated with the use and maintenance of Army systems.
- (6) Reduce environmental and occupational health hazards attributable to Army systems.

c. The health hazard categories addressed by the HHA program include:

- (1) Acoustic energy (steady-state noise, impulse noise, and blast over pressure).
- (2) Biological substances (pathogenic microorganisms and sanitation).
- (3) Chemical substances (weapon or engine combustion products and other toxic materials).
- (4) Oxygen deficiency (crew/confined spaces and high altitude).
- (5) Radiation energy (ionizing and nonionizing radiation, including lasers).
- (6) Shock (acceleration/deceleration).
- (7) Temperature extremes and humidity (heat and cold injury).
- (8) Trauma (blunt, sharp, or musculoskeletal).
- (9) Vibration (whole-body and hand-arm, multiple shocks).

(10) Ultrasound (exclusive of auditory effects).

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

e. The PEO/PM/MATDEV will request an HHA and ensure the SSWG is placed on distribution for related HHAs efforts.

f. The PEO/PM/MATDEV will ensure the RFP requires contractor information to support the HHA, based on the potential health hazard issues identified in the initial HHA or SMMP.

g. Appropriate health hazard objectives will be established early in acquisition programs (that is, in capabilities documents) and used to guide the health hazard activities and the decision process. Contracts should include language that encourages contractors to design out health hazards associated with their systems.

h. An HHA program that identifies and evaluates health hazards will be integrated and coordinated with the program's system safety, MANPRINT, environmental, and T&E activities. The HHARs provide MATDEVs and CAPDEVs with an estimate of the occupational health risk associated with normal use of materiel items. HHARs are not intended to provide an all-inclusive medical assessment or AMEDD approval to use an item. MATDEVs and CAPDEVs must use the risk information in the HHARs to monitor and manage health risks along with safety risks and MANPRINT issues. Mishaps resulting in injuries, although sometimes health-related, do not fall within the scope of the HHA program. The system safety professionals supporting the MATDEV and CAPDEV assess risks associated with mishaps, accidents, or equipment failures. The AMEDD can support the system safety effort, when the adverse outcome is health-related.

3–9. System safety in the manpower and personnel integration process

Improving HSI to make systems more error-tolerant is one of the most critical tasks for enhancing force protection and mission effectiveness. The MANPRINT process provides the vehicle for system safety to influence the human-system integration aspects of materiel design, development, acquisition, and usage, in accordance with AR 70–1. AR 602–2 provides the policy and procedures guiding the MANPRINT program.

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

b. One of MANPRINT's key objectives is to ensure stronger representation for each of the domains at the decision reviews. The manpower and personnel integration joint working group (MJWG) safety representative and reviewers of the SMMP must ensure certain system safety items are included in the document (see app G, of this pamphlet). The USACR/SC develops independent safety assessments (ISAs) for Army Systems Acquisition Review Council (ASARC)-level materiel acquisition decision processes and provides a copy to the Director for DCS, G–1 (MANPRINT Directorate) and the Army Research Laboratory (ARL), Human Research and Engineering Directorate (HRED) for input to the system safety domain of the MANPRINT Assessment, per paragraph 4–9 of this pamphlet.

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

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

- (1) Budget requirements.
- (2) Facilities safety.
- (3) Engineering change proposals/modifications.
- (4) Post fielding safety tracking requirements.
- (5) Materiel only safety hazards.

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

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

3–10. Environment

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

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

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

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

(2) Where the use of hazardous materials cannot be reasonable avoided, procedures for identifying, tracking, storing, handling, and disposing of such materials and equipment will be developed and implemented, as outlined in DODI 4715.4 and DODI 6050.05. The U.S. Army Environmental Command is available to assist as needed.

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

3–11. Software system safety

a. Software system safety is an increasingly critical function within system safety, SE, and software development, particularly as safety-significant (that is, safety-critical or safety-related) software and functions become principal hazard causes and mitigations. A software system safety engineering activity is based on a hazard analysis process, safety-significant software development process, and a level of rigor (LOR) process. These tasks ensure that software is considered in its contribution to mishap occurrence for the system under analysis, as well the overall system's architecture. The safety-significant software development and LOR processes comprise the software system safety integrity process. Emphasis is placed on the context of the "system" and how software contributes to, or mitigates, failures, hazards, and/or mishaps. The Joint Software System Safety Engineering Handbook provides detailed guidance in developing and executing a software system safety program. Within the context of safety-significant software, software system safety—

(1) Will be integrated within the systems engineering, system safety, software development processes, and verification processes.

(2) Will assess the system architecture, capabilities, and functions with emphasis on safety-significant functions being performed by software.

(3) Will identify software affected system hazards and safety-significant software functions.

(4) Will assess software requirements, design, and architecture, identifies hazard mitigation requirements, and ensures implementation and verification, per software development and LOR safety requirements.

(5) Will produce end-to-end (system definition through design implementation and verification) traceability and evidence.

(6) Will assess software contributions to hazard residual risk.

b. MIL–STD–882 requires identification of hazards through a systematic hazard analysis process encompassing detailed analysis of system hardware and software, the environment, and the intended use or application. The Joint Software System Safety Engineering Handbook provides guidance on performing software system safety activities. Each PM should tailor the software system safety program to provide the required levels of hazard mitigation and risk reduction for their program.

c. PMs are responsible for the dissemination of software system safety requirements to contractors and other government agencies supporting their programs.

d. In the context of software system safety, software includes firmware and programmable logic devices, as well as both developmental software and NDI (commercial off-the-shelf items, government furnished-equipment, and re-use) software.

e. The software system safety tasks are defined by performing a functional hazard analysis to identify safety-significant functions, assigning a software control category to each of the software-related safety-critical and safety-significant software functions, assigning a software criticality index based upon severity and software control category, and implementing LOR tasks for safety-significant software based on the software criticality index. One of the primary purposes of the functional hazard analysis is the identification of mitigating safety requirements that, once implemented and verified, reduce residual hazard risk. These mitigating safety requirements may be from an existing specification or software requirements specification, or they may be newly derived safety requirements that need to be added to the requirements specifications.

f. Once safety-significant software functions are identified, assessed against the software control category, and assigned a software criticality index, the implementing software should be designed, coded, and tested against the approved software development artifacts (for example, software development plan, coding standards and practices, software test plans and descriptions) containing the software system safety requirements, (those derived by safety analyses and the software development process safety requirements) and LOR. These criteria should be defined, negotiated, agreed to by the software developer, PM, LCMC, and ATEC, and documented early in the development life cycle.

g. The successful execution of pre-defined LOR activities increases the confidence that the software will perform as specified to software performance requirements, while reducing the number of contributors to hazards that may possibly exist in the system. Both the safety-significant software development and LOR processes are essential in reducing the likelihood of software initiating a propagation pathway to a hazardous condition or mishap. All software system safety tasks will be performed at the required LOR, based on the safety criticality of the software functions within each software configuration item or software module of code.

h. The documented evidence supports the safety case that hazard controls provide the required level of mitigation, and the resultant residual risks can be accepted by the appropriate decision authority. Failure to execute one or more LOR activities should be assessed for potential residual risk to the associated system level hazard(s).

Chapter 4

System Safety for Testers and Evaluators

Section I

Introduction

4-1. General

a. *Purpose.* Army T&E has the following three purposes:

- (1) To help the PEO/PM/MATDEV uncover system problems for correction.
- (2) To help the decision authorities determine whether development is progressing satisfactorily and whether the system is likely to meet operational needs.
- (3) To verify the elimination or control of safety and health hazards.

b. *Information.* This chapter provides the tester and evaluator the information needed to develop and conduct a system safety test or evaluation. The key to this effort is the formulation of a TEMP (see AR 73-1 and DA Pam 73-1), which should address the identification of new hazards and the evaluation of the “fixes” made to previously identified hazards. The major effort of safety testing should be directed toward identifying, evaluating, and tracking these hazards (see chap 2, of this pamphlet). Hazard resolution will be accomplished by the PEO/PM/MATDEV. System safety evaluations should focus on deficiencies in the system safety program, as well as hazards.

c. *Application.* T&Es apply to both developmental and NDI acquisition strategies. Testers’ system safety requirements by phase during the materiel acquisition life cycle are covered in chapter 2 of this pamphlet.

4-2. Definition

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

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

- (1) Estimate the operational effectiveness and suitability of the system.
- (2) Identify the need for modifications.

(3) Examine the adequacy of concepts for doctrine, tactics, organization, and training.

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

Section II

Test Planning and Conduct of Test

4-3. Test planning

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

b. Distribution of test plans is made by Headquarters, ATEC, who is responsible for the initial placing of published documents into Versatile Information Systems Integrated On-line, an ATEC initiative to integrate data across test centers to provide a common Web-based user interface, and is available at <https://vdlis.atc.army.mil/>. Published documents are also distributed into the Defense Technical Information Center.

c. System safety tests for critical devices and components will be incorporated into tests required for other disciplines. This is accomplished through the T&E working-level integrated product team. The PM will ensure adequate safety representation in this group.

4-4. General

a. 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 test risk management and Safety Release processes are used to resolve any conflicts in this area.

b. Safety testing can be used to—

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

4-5. Developmental tests

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

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

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

- (1) Evaluating special safety and health hazards listed in paragraph 3-8, of this pamphlet.
- (2) Verifying the adequacy of safety and warning devices and other measures employed to control hazards.
- (3) Analyzing the adequacy of hazard warning labels on equipment and warnings, precautions, and control procedures in equipment publications.
- (4) Verifying the adequacy of safety/health guidance and controls in the SAR, TMs, and HHAR.
- (5) Considering hazard-mitigating recommendations in reviewing and/or developing test center SOPs.
- (6) Including/coordinating any unique data requirements in the safety or human health test designs that are implied in test documentation (for example, SAR, initial HHAR, and so forth).
- (7) Identifying new hazards in reports and test incident reports, when the risk assessment is inaccurate or requires revision.

4-6. 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 Soldier 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 DTs. It is common, however, for unanticipated hazards to occur when a system is placed in the hands of Soldiers and put in operation. Therefore, test planning must include disciplined observation and other data collection procedures to ensure that such hazards are identified and added to the HTS.

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

4-7. Non-developmental item tests

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

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

Section III Evaluations

4-8. Evaluators

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

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

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

d. System safety issues enter the CE process through continual dialogue among the PEO/PM/MATDEV, CAPDEV, technical and operational testers and evaluators, these organizations' system safety personnel, and other members of the acquisition team. Key activities for input of system safety issues to CE are the developed TEMP issues and criteria. Again, the forum for coordination of acquisition team activities is the T&E working-level, integrated, product team. The SSWG ensures that the updated SSMP is used throughout the development process by the T&E working-level integrated product team for updating the TEMP and by ATEC for updating the system evaluation plan.

4-9. U.S. Army Combat Readiness/Safety Center independent safety assessment

The Commander, USACR/SC, will provide an ISA of ACAT I and II Major Defense Acquisition Programs, as needed, at the program milestone decision review to the AAE and the ASARC or designated acquisition program MDA to contribute to the decision for the program to enter the next phase of acquisition. The ISA distribution will include the the Assistant Secretary of the Army for Acquisition, Logistics and Technology, DCS, G-1 (MANPRINT Directorate), Deputy Assistant Secretary of the Army for ESOH, PEO, PM, TCM, ASARC Secretary, and others as required. A copy of the ISA will also be provided to the ARL HRED for input to the system safety domain of the MANPRINT Assessment. The ISA is an evaluation of the PEO/PM total safety program and their management of the ESOH considerations for the safety program and the safety risks for potential technical issues, problems, and hazards. The ISA is conducted through a review of available programmatic, system safety management, and system safety technical documentation for the system program and communications with representatives from the applicable offices of the PEO/PM and supporting LCMC. The system program is assessed to ensure compliance with standard practices and the tenets AR 70-1, AR 385-10, MIL-STD-882, and the application of the System Safety-ESOH Management Evaluation Criteria for DOD Acquisition.

Part Two Facility System Safety

Chapter 5 Facility System Safety Management

5-1. Purpose of facility system safety

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

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

5-2. Facility system safety participants

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

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

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

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

d. *USACE divisions and DRUs.* USACE divisions and DRUs have responsibility for supervision and oversight of the system safety activities carried out by their subordinate organizations.

e. *Headquarters, USACE.* USACE develops and maintains overall facility/project system safety policy and program guidance.

Chapter 6 Facility System Safety Program Management

6-1. General

The purpose of this chapter is to discuss the basic operating procedures used in the FASS effort. The following sets

forth the actions required in the planning, design, and construction phases of MILCON-funded or civil works facilities. These actions will be performed by the responsible FASS participants identified in paragraph 5–2, above.

6–2. Background

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

6–3. Using or Activity installation responsibilities

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

(1) Representatives from the appropriate MILCON stakeholders should be included in any MILCON SSPT.

(a) Member of the activity that will occupy the facility. This individual must have a detailed knowledge of the mission and function of the project and of specific hazards introduced by the work activities to take place within the structure and the impacts of the structure to/from adjacent activities.

(b) A representative from the Directorate of Public Works, or equivalent, or the appropriate USACE agency. This individual will provide the group with information regarding the project schedule, planning data, background information on the MILCON process. The Directorate of Engineering and Housing/Directorate of Public Works representative will normally serve as the SSPT chairperson in the initial SSPT.

(c) A representative from the installation/using activity safety office. This individual will provide background information and knowledge in the system safety process, address safety and occupational health standards applicable to the project design and construction, and will provide information related to accident and injury data, regarding like or similar structures.

(d) A representative from the installation medical activity or clinic. This member is generally an industrial hygienist or environmental health officer who has detailed knowledge of the health hazards associated with the installation's mission and functions.

(e) A fire protection engineer or specialist. This member brings detailed knowledge of fire hazards, fire prevention measures, and fire protection requirements.

(f) An environmental engineer or specialist. This member brings knowledge of environmental requirements and hazards, as related to facility/project design considerations.

(g) The facility system safety point of contact for the engineering activity. This member is responsible for oversight and coordination of the SSPT activities.

(2) Representatives from the appropriate civil works stakeholders should be included in the SSPT for civil works projects.

(a) Member of the activity that will occupy the project. This individual must have a detailed knowledge of the mission and function of the project and of specific hazards introduced by the work activities to take place within the structure and the impacts of the structure to/from adjacent activities.

(b) A representative from the requesting agency and the USACE for a civil-funded facility/project.

(c) Applicable state, local, and federal entities and/or other stakeholders.

(d) A fire protection engineer or specialist. This member brings detailed knowledge of fire hazards, fire prevention measures, and fire protection requirements.

(e) An environmental engineer or specialist. This member brings knowledge of environmental requirements and hazards, as related to facility/project design considerations.

(3) Appropriate stakeholders should make up the SSPT for other projects (for example, environmental, superfund, base realignment and closure, formerly used defense sites, and so forth).

b. Preparation of a PHL. The SSPT will initially prepare or oversee the preparation of a PHL. The PHL is a high level document upon which the system safety effort is based. As such, it must be completed in time to influence planning, design, and funding documents. The PHL is used to initially identify hazards to be controlled, uncertainties to be resolved, and other safety, health, and fire protection concerns of the user that will require special attention in the design process. A well-prepared and documented PHL helps to ensure design and construction of a facility acceptable to the user. The PHL is included as part of the DD Form 1391 (FY__Military Construction Project Data) funding documents. By requiring the PHL to accompany the funding documentation, funding for system safety tasks becomes an integral part of the budget process. If the scope of the system safety effort is to be extensive, funding for this effort

will be obtained as part of the design/construction funds. The initial PHL will generate a list of safety-critical areas. Areas that need special safety emphasis (for example, hazard analysis) will be identified. Also, special requirements can be written into the detailed functional requirements to address these areas. This input may be in the form of specific design features that the facility must include, or it may be requirements for hazard analyses to be performed as part of the design process. Once included in the design contract, safety is integrated into the design of a facility starting with concept design.

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

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

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

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

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

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

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

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

6-4. Engineering organization responsibilities

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

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

c. Prepare project SSMP. This is a plan tailored to the specific project which establishes management policies and responsibilities for execution of the design system safety effort. It is based upon the PHL and associated recommendations from the user, regarding risk and design safety analysis needs. The following are the minimum elements of the SSMP:

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

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

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

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

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

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

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

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

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

d. Incorporate system safety requirements in contract documents. These requirements are structured from the project tailored SSMP. To provide an understanding of potential contractor's system safety capabilities, candidate contractors will be requested to provide their proposed approach to the system safety requirements in their written or oral presentations to government contractor selection boards. Consider including the requirement for a SSEP in the statement of work. See paragraph 7-4 of this pamphlet, for the key elements of a SSEP. See AR 385-10 and DA Pam 385-10 for policy and standards for integrating safety into the contracting process.

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

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

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

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

6-5. Design agent functions

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

b. Review engineering change proposals, before forwarding to the engineering organization for impact on FASS.

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

6-6. Standard designs

a. FASS is an integral part of a standard design. Each standard design shall include a set of standard FASS documents, prepared using the requirements contained in chapter 7 of this pamphlet.

b. The effort required to complete the FASS program for a standard design should not be duplicated for each application of the design. Local analysis of the design application shall be performed to identify specific hazards associated with the impact of the structure to/from its intended siting (for examples, utilities, activities, adjacent structures, and so forth).

c. For each application of the standard design, deviations from the standard design shall be analyzed to identify any new hazards or increased risk introduced in the facility. This effort should be performed by the engineering organization responsible for the standard design and included with the standard FASS package for the design application.

d. Standard designs shall have a HTS, to include hazards associated with deviations from the standard design. Each standard design shall include a lessons learned database. Any HTS or lessons learned database shall be available to the users of the standard design.

6-7. Self-help projects

a. Self-help projects consist of work that can be performed using Army training, materials, equipment, and supervision. These projects include minor maintenance (for example, painting a room), improvements (for example, landscaping and fencing), and Soldier-sponsored projects (for example, renovation of barracks).

b. Self-help projects, if not properly managed, can increase the risk to a facility/project and/or personnel. For example, failure to use the appropriate fire retardant building materials or the construction of a wall in the hallway of a barracks building increases the risk of fire and injuries to personnel in the event of a fire.

c. Safety and occupational health personnel should provide input to the system safety point of contact at the engineering activity for the establishment of strict policies and procedures for the authorization and performance of self-help projects. These policies and procedures should address, as a minimum, scope of work/projects authorized to be performed, development of project proposals, selection and requisition of supplies and materials, training in use of equipment and procedures, supervision, and inspection/quality assurance.

6-8. Construction facility system safety

a. *Safety features.* During the construction phase, two activities involving FASS will take place. Change orders will be reviewed to ensure changes do not degrade safety features already incorporated in the design. This is an area that will take considerable effort, as configuration control has historically been poor in facility construction. Also, arrangement with the engineering organization may be made for site visits to check on the progress of the facility.

b. *Occupancy inspection.* This inspection should take place immediately, before the user takes over control of the facility. This inspection will verify the presence of critical safety features incorporated into the design. At this point, the HTS is important; review of the tracking system will identify safety features that should be looked at during the inspection. The hazard tracking log should be used to generate a checklist for safety items that should be a part of the inspection.

6-9. Facility/project operation and maintenance

a. *Procedure development.* After a facility/project design is completed, risks have been controlled and/or accepted, and the construction phase has begun, it is time to begin the process of developing facility/project operating, maintenance, and emergency procedures. The output of the design system safety effort should be used as the point of departure for procedure development. The primary focus should be on residual risks and assuring that critical safety features of the structure are included in maintenance plans. Plans to deal with natural and man-made emergencies must also be developed at this time. In addition, necessary training programs for instructing building occupants in the use of these procedures and plans should commence.

b. *Change analysis.* After building occupancy, any proposed building mission changes must be analyzed to detect changes that could introduce a new hazard or change the attributes or nature of an existing hazard or hazard control. A determination must be made of whether new mission tasks can be safely performed in the facility/project as originally designed and to identify any modifications necessary to insure the safety and occupational health of building occupants.

c. *Facility/project/site maintenance and repairs.* Maintenance and repair of existing facilities or sites must comply with applicable standards and procedures. Maintenance is the work required to preserve and maintain a facility/project or site in such condition that it may be effectively used for its designated functional purpose. Maintenance includes cyclic work done to prevent damage or work performed to sustain components. Repair is work performed to restore a project or facility. Repair may be overhaul, reprocessing, or replacement of deteriorated component parts or materials. All new work performed as repairs must meet new construction standards.

Chapter 7 Facility System Safety Program Contracting

7-1. General

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

7-2. Contractor selection

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

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

7-3. Task selection

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

7-4. System safety engineering plan

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(3) *System safety program milestones.* The program plan will—

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

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

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

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

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

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

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

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

(a) The analyses needed to meet specified requirements.

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

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

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

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

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

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

(b) Identify deliverable data.

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

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

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

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

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

Appendix A References

Section I Required Publications

AR 40-10

Health Hazard Assessment Program in Support of the Army Acquisition Process (Cited in paras 3-8a, C-8f(1)(m).)

AR 70-1

Army Acquisition Policy (Cited in paras 1-4c(1)(a), 1-4c(1)(b), 1-4c(2)(a), 1-4c(2)(e), 2-4a, 2-5f(1), 2-14, 3-9, 4-7, I-1b, J-2.)

AR 385-10

The Army Safety Program (Cited in paras 1-1, 1-4c(1)(a), 3-2f, 4-9, 6-4d, I-1b.)

AR 602-2

Manpower and Personnel Integration in the System Acquisition Process (Cited in paras 3-7a, 3-9, 3-9c.)

AR 700-142

Type Classification, Materiel Release, Fielding, and Transfer (Cited in paras 1-4c(3)(d), 1-4f(3), 2-10e(4), 2-14.)

DODI 5000.02

Operation of the Defense Acquisition System (Cited in paras 1-4a(6), 1-4c(1)(a), 1-4c(1)(b), 1-4c(2)(a), 1-4c(2)(e), chap 2, 2-5f, 2-13a, I c(3)(a)(1), J-2.) (Available at <http://www.dtic.mil/whs/directives/>.)

MIL-STD-882

Standard Practice for System Safety (Cited in paras 1-4c(1)(b), 1-4c(2)(e), 2-4a, 2-5a, 2-14, 3-2d, 3-2e, 3-11b, 6-3c(3), 6-4c(1), 6-4c(3), 7-3, B-8d, C-8b(1), C-8g(1), E-1d, G-1d, H-1, H-2, I-1b, J-2.) (Available at <http://quicksearch.dla.mil/>.)

Section II Related Publications

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

AR 25-30

The Army Publishing Program

AR 40-61

Medical Logistics Policies

AR 70-62

Airworthiness Qualification of Aircraft Systems

AR 73-1

Test and Evaluation Policy

AR 75-1

Malfunctions Involving Ammunition and Explosives

AR 75-15

Policy for Explosive Ordnance Disposal

AR 700-127

Integrated Logistic Support

AR 750-6

Army Equipment Safety and Maintenance Notification System

DA Pam 73-1

Test and Evaluation in Support of Systems Acquisition

DA Pam 385-10

Army Safety Program

DA Pam 385-30

Mishap Risk Management

DA Pam 385-40

Army Accident Investigations and Reporting

DFARS 207.102 et seq.

Acquisition Plans

DI-MNTY-81600

Maintainability Program Plan

DI-QCIC-80131

Failure and Analysis Tracking Report

DI-QCIC-81495

Failure Mode, Effects, and Criticality Analysis Report

DI-QCIC-81722

Quality Program Plan

DI-TMSS-81586A

Reliability Test Reports

DOD 5000.4-M

Cost Analysis Guidance and Procedures

DODD 5000.01

The Defense Acquisition System

DODI 4715.4

Pollution Prevention

DODI 6050.05

Department of Defense Hazard Communication Program

Executive Order 12114

Environmental Effects Aboard of Major Federal Actions

FAR 7.101 et seq.

Acquisition Plans

FM 5-19

Composite Risk Management

GEIA-STD-0007

Logistics Products Data

GEIA-STD-0009

Reliability Program Standard for Systems Design, Development, and Manufacturing

IEEE/EIA 12207

Standards for Information Technology Software Life Cycle Processes

MIL-HDBK-502

Acquisition Logistics

MIL-HDBK-470A

Designing and Developing Maintainable Products and Systems, Vol. 1

MIL-STD-331C

Environmental and Performance Tests for Fuze and Fuze Components

MIL-STD-1316E

Safety Criteria for Fuze Design

MIL-STD-1472G

Human Engineering

MIL-STD-1522A

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

MIL-STD-1901A

Design Criteria Standard: Safety Criteria for Munition Rocket and Missile Motor Ignition System Design

MIL-STD-2105D

Test Method Standard: Hazard Assessment Tests for Non-nuclear Munitions

NATO STANAG 4170

Principles and Methodology for the Qualification of Explosive Materials for Military Use

29 CFR 1910.95

Occupational noise exposure

32 CFR 651

Environmental Analysis of Army Actions

49 CFR 172.101

Purpose and use of hazardous materials table

10 USC 4321 et seq.

National Environmental Policy

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate (APD) Web site (<http://www.apd.army.mil/>); DD forms are available on the Office of the Secretary of Defense (OSD) Web site (<http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm>); and Standard forms (SF) are available on the U.S. General Services Administration (GSA) Web site (<http://www.gsa.gov>).

DA Form 2028

Recommended Changes to Publications and Blank Forms

DD Form 1391

FY__Military Construction Project Data

SF 368

Product Quality Deficiency Report (PQDR)

Appendix B

Preparation Guidance for a System Safety Working Group Charter

B-1. Purpose

Briefly describe the SSWG's purpose.

B-2. Scope

Describe the scope of the SSWG's activities.

B-3. Authorizations

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

B-4. References

References will contain publications to be used in the charter.

B-5. Tasks

a. List the major tasks the SSWG should perform. These tasks will be broad in scope. Paragraphs 2–14 through 2–18 of this pamphlet include descriptions of ESOH tasks for each phase of the acquisition framework and can be used as a check against omission of important tasks.

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

B-6. Operation

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

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

c. *Administration.*

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

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

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

B-7. Term

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

B-8. Example of a system safety working group charter

Below is an example of an SSWG charter—

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

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

(1) Validation of system safety tasks.

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

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

(4) Coordinating with other program elements.

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

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

d. *References.* MIL-STD-882.

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

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

(2) Review and evaluation of the best technical approach.

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

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

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

- (6) Review of the (system name) RFP.
- (7) Development of source selection evaluation board selection criteria for system safety.
- (8) Evaluation of contractor proposals for system safety, to include crashworthiness.
- (9) Development of an HTS to identify, eliminate if possible, rank, estimate a likelihood of occurrence, and track hazards throughout the life cycle of the system. Recommendations for corrective action will be provided to the (system name) PM, as appropriate.
- (10) Development of an SSMP.
- (11) Review and evaluation of the contractor's SSEP.
- (12) Assistance to the (system name) PM during safety system safety analyses reviews at the contractor's facility. Comments or recommendations for corrective action should be provided to the (system name) PM, as appropriate.
- (13) Development of a PHL.
- (14) Collection and evaluation of lessons learned pertaining to (system name) system safety.

f. Operation.

- (1) Membership.
 - (a) The principal voting members to be appointed from the MATDEV's organizations are—
 - 1. (System name) PM's office.
 - 2. Supporting safety office (LCMC matrix support).
 - 3. Engineering representative.
 - 4. CAPDEV safety representative (for example, TRADOC System Safety Engineer).
 - 5. MANPRINT representative.
 - 6. Installation safety manager, if applicable.
 - 7. Prime contractor's system safety manager, if appropriate.
 - (b) Advisory members will be appointed from the following organizations:
 - 1. ACOMs/ASCCs/DRUs safety offices (LCMC, CAPDEV, and/or user).
 - 2. User test organization.
 - 3. Representatives from ACOMs/ASCCs/DRUs developing subsystems.
 - 4. Technical test organization.
 - 5. Developmental independent evaluator.
 - 6. Operational independent evaluator.
 - 7. ARL HRED.
 - 8. DA observer (USACR/SC).
 - 9. Other organizations as required.
 - (c) Advisory members will be invited to attend meetings on an as-required basis when their expertise, opinions, or comments are required or solicited.
 - (d) The DA observer will be a representative from the USACR/SC. The observer's responsibility will be to participate in the SSWG meetings and provide any technical safety input to the SSWG through its chairman.
 - (e) Chairmanship is vested jointly in the (system name) PM's office member and the supporting safety office member.
 - (f) 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.
- (2) 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.
- (3) Administration.
 - (a) The SSWG chairmen will establish the agenda for scheduled meetings no later than two weeks prior to the meeting.
 - (b) Proposed agenda items may be submitted by any member of the SSWG.
 - (c) 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.
 - (d) The SSWG does not have the authority to accept risks associated with identified hazards. All hazards identified by any source will be entered in the HTS, and recommendations for their elimination or mitigation will be provided through the PM to the appropriate decision authority.
 - (e) SSWG recommendations to the PM will include any minority opinions.
 - (f) All items from previous meetings will be reviewed to determine that the action is closed or adequate progress is being made.
 - (g) Accident or incident experience will be reviewed at each meeting to identify trends and to monitor and evaluate the corrective actions taken.

(h) Implementation of the provisions of this charter will be governed by the SSMP, developed by the SSWG, and approved by the PM.

(i) This charter and the SSMP will be reviewed at least annually and updated or modified, as required.

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

Appendix C

System Safety Management Plan

C-1. General program requirements

a. Purpose.

b. References.

c. Scope.

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

C-2. System safety organization

a. Program/project/product management office.

b. LCMC Matrix Support Safety Office.

c. Integration of associated disciplines.

C-3. Tasks

The specific tasks to accomplish the objectives in paragraph C-8d, below, should be listed with the responsible action agency. The activities described in paragraphs 2-14 through 2-18 of this pamphlet can be tailored for use in the SSMP. It can also be used as a check against omission of important tasks.

C-4. Milestones

A milestone schedule that parallels the overall program schedule will be established. Specific start and completion dates should be developed for the activities/tasks referenced in paragraph C-3, above (see fig C-1).

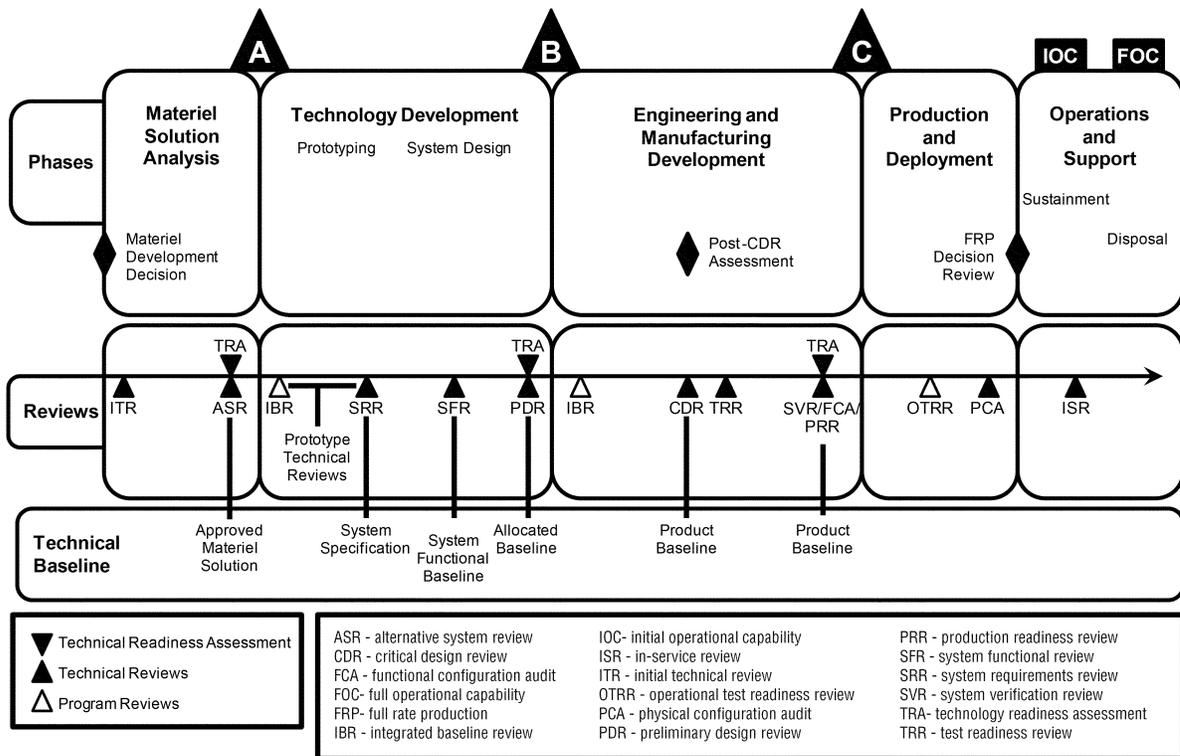


Figure C-1. Milestones

C-5. Risk management

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

C-6. Administration

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

C-7. Resources

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

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

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

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

C-8. Sample system safety management plan

General program requirements—

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

b. References.

(1) MIL-STD-882.

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

c. Scope. This plan establishes ground rules for government and contractor interaction with respect to system safety. It applies to the (system name) SSWG, functional areas within the command supporting the (system name) program, (system name) program/project/product management office, and (system name) contractors. The plan establishes the methodology by which the (system name) PM may oversee and evaluate the execution of contractor SSEPs.

d. Objectives.

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

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

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

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

(5) Risk acceptance decisions are documented.

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

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

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

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

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

(1) The (system name) MJWG and test integration working group.

(2) ARL HRED and USAIPH to integrate the human factors engineering analysis and the HHA into the (system name) system safety program.

(3) ATEC to obtain results of operational evaluations of the (system name) system and to ensure incorporation of key safety issues into the test, evaluation, analysis, and modeling plan.

(4) Environmental considerations.

f. Tasks.

(1) *The PM will—*

(a) Charter and guide an SSWG.

(b) Designate the program system safety manager.

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

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

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

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

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

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

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

(j) Prepare SSRA for each hazard. The SSRA will be sent to the CAPDEV 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 USACR/SC.

(k) Assure that adequate source selection evaluation board safety criteria are established to evaluate the contractor's proposals and simplified acquisition procedures.

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

(m) Request a HHAR from the USAIPH (per AR 40-10) at each major milestone, and provide the most recent version to ATEC 60 days prior to the start of all testing. HHA subject matter assistance to support safety events may be provided by contacting the USAIPH HHA Program.

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

(2) *Supporting safety office will—*

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

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

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

(d) Review procurement documentation for compliance with DOD and U.S. Army system safety policy.

(e) Establish and maintain a system safety lessons learned file for the (system name) system. Submit lessons learned on an annual basis (September) to USACR/SC and Defense Technical Information Center throughout the system's life cycle. Make recommendations, as appropriate, for changes to military specifications and standards.

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

(3) *PEO/PM/MATDEV/LCMC organizations.*

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

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

g. *Risk management.*

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

(2) *Risk resolution.*

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

1. Within 14 calendar days after each SSWG meeting.

2. Immediately, when a high risk hazard is identified.

(b) The PM will comment in writing on the recommendations submitted by the SSWG. These comments will constitute the basis upon which hazard resolution actions are to be taken and will serve as initial documentation for risk acceptance decisions. The risk decision matrix defines the command level to which each hazard must be reported and the decision authority for accepting the risk associated with each hazard.

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

(3) *Hazard tracking.*

(a) An HTS will be established jointly by the supporting safety office and the (system name) PM using the format in table 2-3, of this pamphlet.

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

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

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

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

(2) Ensure distribution of contractor deliverable system safety documents to SSWG principal members within 14 calendar days of receipt by the program/project/product management office.

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

(1) *Budget.* To be established by PM.

(2) *Manpower.* To be established by PM.

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

C-9. Key considerations

Key considerations of the SSMP include—

- a. Documenting the SSE approach.
- b. Designating in writing a system safety lead for each program.
- c. Ensuring the contractor-led system safety effort is integrated into the government system safety program. This teaming arrangement does not preclude the responsibility to ensure and verify contractor performance.
- d. Ensuring organizational structures and resources are adequate to perform required system safety program actions. This should include establishing a SSWG comprised of government and contractor representatives, who are responsible for implementing specific safety program requirements.
- e. Ensuring the identification of recommended critical safety items.
- f. Including the system safety program requirements and criteria in acquisition documentation, requests for proposals, specifications, and statements of work.
- g. Reviewing the status of safety-related modifications periodically. Conducting periodic equipment improvement reports, PQDRs, and accident reviews get the PMs personally involved. This demonstrates a shared concern with the user for the safe performance of the system, provides a forum for discussing the appropriateness of material and procedural fixes, and provides an excellent opportunity to solicit support for safety-related modifications. Periodic review of safety-related modifications for fielded systems are an indicator of the success of the original safety program conducted during development. Large numbers of such changes may indicate a weak program or poor management participation and safety emphasis. Regardless, if safety problems are allowed to be created and remain undetected until late in development, the fixes can wreak havoc with budgets and schedules.

Appendix D Preliminary Hazard List/Preliminary Hazard Analysis

D-1. Definition

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

- a. Its results may help develop the guidelines and criteria to be followed in a system/facility design.
- b. Since it indicates the principal hazards as they are known when the system is first conceived, it can be used to initiate actions for their elimination, minimization, and control almost from the start.
- c. It can be used to designate management and technical responsibilities for safety tasks and be used as a checklist to ensure their accomplishment.
- d. It can indicate the information that must be reviewed in codes, specifications, standards, and other documents governing precautions and safeguards to be taken for each hazard.

D-2. Basic elements

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

- a. A review of pertinent historical safety experience and lessons learned data bases. This involves discovering problems known through past experience on similar systems/facilities to determine whether they could also be present in the system or facility under development.
- b. A categorized listing of basic energy sources.
- c. An investigation of the various energy sources to determine provisions that have been developed for their control.
- d. Identification of the safety requirements and other regulations pertaining to personnel safety, environmental hazards, and toxic substances with which the system/facility will have to comply.
- e. Recommended corrective actions.

D-3. Sources of data

Obtain historical safety information from predecessor systems.

D-4. Preliminary hazard analysis chart (sample)

There are several formats that may be used when performing a PHA (see table D-1, below, for a sample format of a functional PHA).

Table D-1
Sample format of preliminary hazard analysis (typical)

Program: Agent Formulation Simulation

System: Binary Lethal Agent Reactor

Part	Hazard	Cause	Hazard Effect	Corrective Category or Prevention Action
Glove box	Ignition of flammable fluid	Flammable solutions within the glove box when electrically functioning of the sampling and injection solenoids	Fire, burn injuries to the operator	Remove all flammable solutions from glove box prior to electrically functioning of the solenoids.
Glove box	Agent exposure	Ventilation failure causing loss of negative pressure within hood	Operator exposure and injury due to agent escaping from hood	Install alarms and train lab workers to stop operations, don masks, containerize agent, and evacuate.
Aluminum foil burst disk	Agent exposure	Leak due to improper installation of or damage to disk	Operator exposure and injury due to premature formation of agent	Stop filling operations when thermal recorder readout shows temperature increases.
Automatic relief valve	Chemical release	Spring loaded relief valve does not actuate at the preset pressure	Operator exposure due to pressure build-up and rupture of reactor	Increase valve reliability by replacing automatic relief valve with a burst disk. If increased pressure is observed, operator will actuate manual relief valve.
Tank T-12	Chemical release	Degradation of tank	Environmental contamination	Monitor level of tank. Install secondary containment. Require spill plan.

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

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

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

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

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

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

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

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

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

(e) Facilities and support equipment with appropriate training for proper use should be carefully examined. These

could include provisions for storage, assembly, and testing hazardous systems and making sure personnel who will handle these systems or assemblies are properly trained.

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

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

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

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

Appendix E

System Safety Risk Assessment Preparation Guidance

E-1. Part I

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

E-2. Part II

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

E-3. Part III

Recommendation by the CAPDEV.

E-4. Part IV

Recommendation by the LCMC.

E-5. Part V

Approval by the appropriate risk decision authority.

E-6. System safety risk assessment process

See figure 2-3 for the SSRA process flow.

Appendix F

Safety Release Preparation Guidance

F-1. Purpose of this Safety Release

State the purpose of the Safety Release.

F-2. References

List appropriate references associated with the system.

F-3. System description

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

F-4. Requirements and background

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

F-5. Conclusions and recommendations

- a.* Indicate whether the system is completely safe for testing or whether it is safe for testing with exceptions. List hazards and any technical or operational limitations or precautions needed to prevent injury and property damage during testing.
- b.* Highlight any known safety problems that will require further investigation during testing.

F-6. Signature

Provide the signature of the appropriate release authority.

Appendix G

Manpower and Personnel Integration Joint Work Group System Safety Checklist

G-1. Coordination for the manpower and personnel integration joint work group system safety checklist process

- a.* The MJWG will meet to write the SMMP.
- b.* The safety representative and the MJWG must ensure that the SMMP will be passed to the associated and interested safety officers for comments.
- c.* Ensure the appropriate CAPDEV's and MATDEV's system safety representative is a voting member and present at all MJWG meetings.
- d.* Ensure all MANPRINT safety issues brought to the MJWG are passed to the SSWG for evaluation and determination of a risk assessment per MIL-STD-882.
- e.* Coordinate with the MJWG health hazard/system health hazard representative to ensure health hazard issues are consistent.

G-2. System safety checklist items

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

- a.* The system safety goals in Section 3, MANPRINT Strategy.
- b.* A SSMP as part of Section 4, Data Sources/Availability, Planned Level of MANPRINT Analysis Effort.
- c.* The data sources used by the developers of the lessons learned are included in Tab A (Data Sources).
- d.* The established level of tradeoff authority for all MANPRINT issues. This tradeoff authority must be consistent with the risk acceptance decision authority established under the SSMP.
- e.* List the SSWG and MJWG interface responsibilities in the SSEP and SMMP, especially as related to obtaining and analyzing data to identify the hazard(s).
- f.* MJWG chairman will ensure the MANPRINT assessment is coordinated with the SSWG chairman.

Appendix H

Non-developmental Item System Safety Market Investigation/Survey Questions

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

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

- a.* Has the system been designed and built to meet applicable safety standards?

- b. Have any hazard analyses been performed? Request copies.
- c. What is the accident history for the system? Request specifics.
- d. Is any protective equipment or actions needed during operation, maintenance, storage, or transport of the system? Request specifics.
- e. Does the system contain or use any hazardous materials (to include radioactive substances), have potentially hazardous emissions (such as from a laser), or generate hazardous waste?
- f. Are special licenses or certificates required to own, store, or use the system?
- g. Is the system similar to a previous military system? If so, what are the lessons learned from the previous system?
- h. If the new system attempts to resolve problems with the previous system, what are the new hazards created with the new system?

H-2. Guidelines

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

Appendix I Independent Safety Assessment

I-1. Independent safety assessment

a. The Commander, USACR/SC, will provide an ISA of Army Category I & II Major Defense Acquisition Programs, as needed, at the program milestone decision review to the AAE and the ASARC or designated acquisition program milestone decision authority to contribute to the decision for the system program to enter the next phase of acquisition. The ISA distribution will include the Assistant Secretary of the Army for Acquisition, Logistics and Technology; DCS, G-1 (MANPRINT Directorate); the Deputy Assistant Secretary of the Army for Environment, Safety, and Occupational Health; PEO; PM; TCM, ASARC Secretary, and others as identified. A copy of the ISA will also be provided to the supporting ARL HRED for input to the system safety domain of the MANPRINT assessment report.

b. The USACR/SC's ISA is an evaluation of the PEO/PM total safety program and their management of the ESOH considerations for the safety program and the safety risks for potential technical issues, problems, and hazards. The ISA is conducted through a review of available programmatic, system safety management, and system safety technical documentation for the system program and communications with representatives from the applicable offices of the PEO/PM and AMC LCMC. The system program is assessed to ensure compliance with standard practices and the tenets of AR 70-1, AR 385-10, MIL-STD-882, and the application of the System Safety ESOH Management Evaluation Criteria for DOD Acquisition.

I-2. Independent safety assessment format

a. The ISA consists of a transmittal memorandum signed by the Commanding General, USACR/SC and the safety assessment. While the nature of the memorandum and the safety assessment may depend on the maturity of the system under review, they will conform to the following general format:

b. The transmittal memorandum will consist of the ISA objective and discussion.

(1) *Objective.* The ISA objective is to provide an evaluation of the PEO/PM total safety program and their management of the ESOH considerations for the safety program and the safety risks for potential technical issues, problems, and hazards in support of the milestone decision review by the appropriate acquisition decision authority (AAE, Defense Acquisition Executive, or designated PEO).

(2) *Discussion.* This paragraph will provide the overall rating of the system safety program and the acquisition program safety readiness to enter the next acquisition phase. The PEO/PM should place special emphasis on the recommendations provided in the safety assessment to further improve system safety management and technical aspects of the program to contribute to the prevention of future accidents or injury to personnel.

c. The safety assessment will consist of five sections—purpose, methodology, results, recommendations, and appendices.

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

(2) *Methodology.* This section will describe procedures used for conducting the safety assessment. These procedures will include a review of all system documents, contacts with program representatives, participation in working groups, design and program reviews, and, if possible, on site evaluation of the system. Limitations in conducting the ISA methodology will also be provided.

(3) *Results.* This section will be subdivided into two subsections.

(a) The first subsection, “System Safety Management Issues,” will identify program attributes and/or deficiencies and assess the overall effectiveness of the PEO/PM system safety management by evaluating the following elements:

1. Planning (PESHE updated per DODI 5000.02; integrated master schedules include ESOH activities; ESOH considerations included in demilitarization and disposal plan).

2. Hazard identification, analysis, and risk acceptance (review of lessons learned; HTS effectiveness; SSWG Charter and participation; hazard analyses completed; appropriate risk acceptance authority and decision designated).

3. Requirements for the system and associated infrastructure (database as an information management and traceability tool to manage requirements implemented; integrated product/process team active with safety ESOH considerations; SSMP implemented; safety review meetings conducted; ESOH integration with associated disciplines).

4. Personnel and funding (adequate funding for safety personnel and organizations support; implementation of safety requirements; Contractor system safety program planned and funded).

(b) The second subsection, “System Safety Technical Issues,” will provide a discussion of significant safety hazards, real or potential, and associated risks to contribute to the prevention of accidents. Special attention should be placed on those potential issues, problems, and hazards that have not been addressed in T&E, but have been noted on other similar systems. Where possible, system hazards should be classified according to potential severity and probability, as outlined in the approved SSMP or as in this pamphlet (if no SSMP exist). Proposed corrective actions, to include implementation and verification schedules, will be indicated, as well as any formal acceptance of risks. The design of the system integration and man-machine interface should not place any burden on the Soldier through the use of procedures to overcome design issues, problems, or hazards. The preferred method of addressing hazards is to design out hazards rather than transferring unnecessary risk to the Soldier.

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

(5) *Appendices*. This section will contain the appendices “References” and “System Safety ESOH Management Scoring Process.” The references include applicable regulations, pamphlets, policies, acquisition program documents, military standards, Codes of Federal Regulations, ESOH assessments, and other related documents. The system safety ESOH management scoring process evaluates the acquisition program’s progress for each of the four ESOH categories (weighted metrics) and scores a color-coded rating of GREEN, YELLOW, or RED. This rating provides a method for combining the four category metrics into a single overall system safety ESOH management rating for the program for entry into the next acquisition phase.

Appendix J

Safety and Health Data Sheet Sample Format

The following is a sample format for an SHDS per AR 700–142 and this pamphlet:

J–1. Sample format

a. *Item/system identification*. Name/nomenclature.

b. *Safety letters and reports*.

(1) Technical test(s), including findings of both the testing activity and the independent evaluator (date of confirmation letter).

(2) User test(s), including findings of user independent evaluator (date of confirmation letter).

(3) Production test(s) (date of confirmation letter).

(4) SARs.

(5) Special safety studies and assessments, including SSRAs.

c. *Radioactive materials*. Item does/does not contain radioactive materials, and if it does, it is properly licensed by NRC (number) and/or DA authorization (number), as appropriate. If NRC license or headquarters authorization has not been obtained, provide status of current effort with an approximate approval date prior to these items.

d. *Explosives/hazardous materials*. Item does/does not contain explosives/hazardous materials, and if it does, the following activities should be addressed:

(1) Interim/final hazard classifications. Provide hazard classifications for the item and all of its explosive components, which require a separate shipping configuration and dates when final hazard classifications were/will be approved. Interim and final hazard classifications data shall include the following:

(a) Hazard class and division (1.1, 1.2, 1.3, 1.4, and so forth).

(b) Storage compatibility group (A, B, C, D, E, F, and so forth).

(c) Department of Transportation (DOT) class (class 1.1, 1.2, 1.3, and so forth).

(d) DOT container marking which consists of proper shipping name (49 CFR 172.101), the national stock number, or part number.

- (e) Net explosive weight.
- (f) Net propellant weight in pounds and kilograms.
- (g) Explosive weight for quantity, distance, and purpose (based on trinitrotoluene (TNT) equivalency tests, if propellant contribution is involved).
- (h) DOT EX NUMBER (if applicable).
- (i) UN serial number.
- (j) DOT label (Explosive 1.1E. Explosive 1.2G. and so forth).
- (2) Range safety data.
 - (a) Maximum range and ordinate (as determined by test or analogy).
 - (b) Drift and probable errors (as determined by test or analogy).
 - (c) Ricochet characteristics (as determined by test or analogy).
 - (d) Sound pressure levels (as determined by test or analogy).
 - (e) Fragmentation radius (as determined by test or analogy).
 - (f) Rearward debris and/or blast and overpressure (as determined by test or analogy).
 - (g) Laser range safety criteria (as determined by test or analogy).
 - (h) Meteorological limitations (as determined by test or analogy).
 - (i) Approved range safety fan which incorporates the above data, as necessary.
- (3) EOD procedures for safe rendering of explosive items developed (yes/no).
- (4) Demilitarization and disposal procedures for disposal of hazardous, unserviceable, excess, or obsolete munitions.
- (5) Safety certification from the Army Fuze Safety Review Board, as applicable (date and restrictions).
- e. *Munitions.* Item does/does not contain munitions. If it does, compatibility for each component which may be stored as a separate item must be established. The following list applies:
 - (1) Component list.
 - (2) SDZ has been developed including fragmentation data (where appropriate) and will be provided to AMC for incorporation into guidance to the field. If the SDZ has not been finalized, provide the status and approximate approval date for the final SDZ.
- f. *Health hazards.* Item does/does not produce health hazards (for example, noise, toxic fumes, radioactive, and laser emissions) to user, maintenance, or other personnel. If it does, an HHA or special study has been performed by the USAIPH and the following corrective actions were/will be implemented (including the HHA report as an addendum, or reference The Surgeon General memorandum exempting system from HHAR).

J-2. Risk assessment

Perform a risk assessment of identified high, serious, and medium risk level safety and health hazards, based upon the decision authority matrix contained in the SSMP per AR 70-1, MIL-STD-882, and DODI 5000.02. This assessment will address hazards that are being fixed, or are yet to be fixed, or residual hazards that will not be eliminated by design. This assessment will define decisions regarding resolution of each identified hazard; design features and controls being or to be implemented for elimination or reduction of associated risks to acceptable levels; and describe any residual hazards concerning safety risks to user personnel and government equipment/facilities that have not been eliminated through design. Provide program milestones for planned corrective actions on hazards yet to be resolved during next acquisition phase. If a formal SSRA (decision authority matrix of SSMP) is required, it will be included as an addendum to this SHDS. If no residual hazards exist, so state.

J-3. Summary/conclusions

Summarize the results of the above identified safety letters and reports. Identify any outstanding safety problems and indicate what corrective actions are planned and when they will be implemented and verified. Identify specific procedural controls and precautions (if any) that should be followed. Conclude with a statement as to whether or not the system is safe to test/operate/proceed to the next acquisition phase. If used for a materiel release, the SHDS will identify the remaining safety problems in the system (safety problems identified in the Safety Confirmation will be included in the summary or referenced) and briefly what is being done to control them. It will conclude with a statement that the system is suitable for conditional release from a safety standpoint.

Glossary

Section I Abbreviations

AAE

Army Acquisition Executive

ACAT

acquisition category

ACOM

Army command

AESMNS

Army Equipment Safety and Maintenance Notification System

AMC

U.S. Army Materiel Command

AMEDD

Army Medical Department

AoA

analysis of alternatives

AR

Army regulation

ARL

Army Research Laboratory

AS

acquisition strategy

ASARC

Army Systems Acquisition Review Council

ASAT

Army safety action team

ASCC

Army service component command

ATEC

Army Test and Evaluation Command

CAPDEV

capability developer

CDD

capability development document

CDR

critical design review

CE

continuous evaluation

CFR

Code of Federal Regulations

CRM

composite risk management

DA

Department of the Army

DA Pam

Department of the Army pamphlet

DCS

Deputy Chief of Staff

DFARS

Defense Federal Acquisition Regulation Supplement

DOD

Department of Defense

DODD

Department of Defense directive

DODI

Department of Defense instruction

DOT

Department of Transportation

DRU

direct reporting unit

DT

developmental test

EIA

Electronic Industry Association

EO

Executive Order

EOD

explosive ordnance disposal

ESOH

environment, safety, and occupational health

EXSUM

executive summary

FAR

Federal Acquisition Regulation

FASS

facility system safety

FMECA

failure modes, effects, and criticality analysis

FY

fiscal year

GEIA-STD

Government Electronics and Information Technology Association standard

HFE

human factors engineering

HHA

health hazard assessment

HHAR

health hazard assessment report

HRED

Human Research and Engineering Directorate

HSI

human systems integration

HTS

hazard tracking system

ICD

initial capabilities document

IEEE

Institute of Electrical and Electronics Engineers

IM

insensitive munitions

ISA

independent safety assessment

LCMC

life cycle management command

LOR

level of rigor

LSA

logistic support analysis

LSAR

logistic support analysis record

MA

managing activity

MANPRINT

manpower and personnel integration

MATDEV

materiel developer

MDA

milestone decision authority

MILCON

military construction

MIL–HDBK

military handbook

MIL–STD

military standard

MJWG

manpower and personnel integration joint working group

NATO STANAG

North Atlantic Treaty Organization Standardization Agreement

NDI

non-developmental item

NEPA

National Environmental Policy Act

NRC

Nuclear Regulatory Commission

O&SHA

operating and support hazard analysis

PDR

preliminary design review

PEO

program executive officer

PESHE

programmatic environment, safety, and occupational health evaluation

PHA

preliminary hazard analysis

PHL

preliminary hazard list

PM

program/project/product manager

PQDR

product quality deficiency report

RAC

risk assessment code

RFP

request for proposal

ROM

read-only memory

SAR

safety assessment report

SDZ

surface danger zone

SE
systems engineering

SEP
systems engineering plan

SHDS
safety and health data sheet

SMMP
system manpower and personnel integration management plan

SOP
standard operating procedure

SOS
system-of-systems

SRA
safety requirements analysis

SSE
system safety engineering

SSEP
system safety engineering plan

SSMP
system safety management plan

SSPT
system safety project team

SSRA
system safety risk assessment

SSWG
system safety working group

TCM
Training and Doctrine Command capability manager

TDA
Tables of Distribution and Allowances

T&E
test and evaluation

TEMP
test and evaluation master plan

TM
technical manual

TOA
trade off analysis

TRADOC
U.S. Army Training and Doctrine Command

USACE

U.S. Army Corps of Engineers

USACR/SC

U.S. Army Combat Readiness/Safety Center

USAIPH

U.S. Army Institute for Public Health

USC

United States Code

Section II**Terms****Acceptable risk.**

That part of identified risk which is allowed by the MA to persist without further engineering or management action.

Acquisition phase

Phases provide a logical means of progressively translating broadly stated mission needs into well defined system-specific requirements and ultimately into operationally effective, suitable, and survivable systems. All the tasks and activities needed to bring the program to the next milestone occur during acquisition phases.

Acquisition plan

A formal written document reflecting the specific actions necessary to execute the approach established in the approved AS and guiding contractual implementation. Refer to Federal Acquisition Regulation (FAR) 7.101 et seq., Defense Federal Acquisition Regulation Supplement (DFARS) 207.102 et seq., and acquisition strategy listed below in this glossary.

Acquisition program

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

Acquisition strategy

The AS documents the appropriate planning process and provides a comprehensive approach for achieving goals established in materiel requirements. It serves as a principal long-range document, charting the course of a major acquisition program over its life-cycle.

Army acquisition executive

Senior acquisition executive responsible for administering acquisition programs in accordance with established policies and guidelines. The AAE is also the senior procurement executive.

Army Systems Acquisition Review Council

Top level DA review body for ACAT I and ACAT II programs. Convened at formal milestone reviews or other program reviews to provide information and develop recommendations for decision by the AAE.

Automated information system

A combination of computer hardware and software, data, or telecommunications that performs functions such as collecting, processing, transmitting, and displaying information. Excluded are computer resources, both hardware and software, that are: physically part of, dedicated to, or essential in real time to the mission performance of weapon systems.

Capability development document

A document that captures the information necessary to develop a proposed program(s), normally using an evolutionary AS. The CDD outlines an affordable increment of militarily useful, logistically supportable and technically mature capability.

Capability production document

A document that addresses the production elements specific to a single increment of an acquisition program.

Chief Information Officer validation

See AR 70–1.

Capability developer

Command or agency that formulates and documents operational doctrine, concepts, organizations, and/or materiel requirements for assigned mission areas and functions. Serves as the user representative during acquisitions for their approved materiel requirements as well as doctrine and organization developments. CAPDEV is the command or agency that formulates warfighting requirements for doctrine, organization, training, materiel, leadership and education, personnel, and facilities. May be used generically to represent the user and user maintainer community role in the materiel acquisition process (counterpart to generic use of MATDEV).

Capability development

The process of analyzing, determining, and prioritizing Army requirements for, doctrine, training, leader development, organizations, Soldier development, and equipment and executing or (in the case of doctrine, training and materiel, initiating) solutions, within the context of the force development process.

Combat load of ammunition

The quantity of conventional ammunition authorized by the command to be on hand in units. The basic load is carried by unit members or organic vehicles; it enables the unit to accomplish its mission until resupply can be affected.

Commercial off-the-shelf item

An existing item determined by a material acquisition decision process review (DOD, military component, or subordinate organization, as appropriate) to be available for acquisition to satisfy an approved materiel requirement with no expenditure of funds for development, modification, or improvement (such as, commercial products, or materiel developed by other countries). This item may be procured by the contractor or furnished to the contractor as government- furnished equipment or government-furnished property.

Condition

An existing or potential state such as exposure to harm, toxicity, energy source, procedure, and so forth.

Continuous evaluation

A process that provides the continuous flow of information regarding system status to include planning, testing, data compilation, analysis, evaluation, conclusions, and reporting to all members of the acquisition team from the drafting of the initial Mission Need Statement through deployment reviews and assessment. All members of the acquisition team will perform the CE.

Contractor

A private sector enterprise or the organizational element of DOD or any other government agency engaged to provide services or products within agreed limits specified by the MA.

Cost (total ownership cost)

Defense systems total ownership cost is defined as life-cycle cost. Life-cycle cost (per DOD 5000.4–M) includes not only acquisition programs direct costs but also the indirect costs attributable to the acquisition program (that is, costs that would not occur if the program did not exist). For example, indirect costs would include the infrastructure that plans, manages, and executes a program over its full life and common support items and systems.

Cut-up tailoring

Disjointed, fragmented system safety requirements that result when deleting, without system safety manager coordination, significant numbers of safety requirements for a "revised" shorter and cheaper safety contract.

Damage

The partial or total loss of hardware caused by component failure; exposure of hardware to heat, fire, or other environments; human errors; or other inadvertent events or conditions.

Deductive analysis

An analysis that reasons from the general to the specific to determine HOW a system may fail or meet a given set of conditions (for example, fault tree Analysis).

Department of the Army System Safety Council

The Department of the Army Safety Council is an advisory group established per AR 385–10 to provide technical

guidance and support to the Director of Army Safety, Army Staff, ACOMs, ASCCs and DRUs and assist them in fulfillment of the system safety management, policy and standards development, and oversight responsibilities.

Effectiveness

The overall degree of mission accomplishment by a system under realistic conditions (tactics, threat, personnel, battlefield and natural environments, and so on).

Equipment

See definition for System.

Environment, safety, and occupational health

The term ESOH refers to all of the individual, but interrelated, disciplines that encompass the processes and approaches for addressing laws, regulations, EOs, policies, and hazards associated with environmental compliance, environmental impacts, system safety, occupational safety and health, hazardous materials management, and pollution prevention.. The system safety methodology is used across the ESOH disciplines to identify hazards and mitigate risks through the SE process.

Explosive ordnance disposal

The detection, identification, field evaluation, rendering-safe, recovery, and final disposal of unexploded explosive ordnance. It may also include the rendering safe or disposal of explosive ordnance that have become hazardous by damage or deterioration when the disposal of such explosive ordnance is beyond the capabilities of personnel normally assigned the responsibility for routine disposal. In this case, this includes applicable weapon systems, all munitions, all similar or related items or components explosive, energetic, or hazardous in nature. This includes explosive ordnance training aids and items, items that could be misidentified as explosive ordnance or bombs, remotely piloted vehicles, and Army aircraft and vehicles.

External interface

Information exchange between system program office personnel and those outside the program office.

Fail safe

A design feature that ensures that the system remains safe or will cause the system to revert to a state that will not cause a mishap.

Family of systems

A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities, dependent on the situation. An example of a family of systems is a unit of action that included armor, infantry, artillery, and combat support systems.

Fielding command

The subordinate command, matrix support, or contracted organization, agency, or activity responsible for the fielding of a materiel system.

Firmware

Software stored in read-only memory (ROM) or programmable ROM. Easier to change than hardware but harder than software stored on disk, firmware is often responsible for the behavior of a system when it is first switched on. A typical example would be a "monitor" program in a microcomputer that loads the full operating system from disk or from a network and then passes control to it.

First unit equipped date

The first scheduled date for handoff of a new materiel system in a gaining command.

First unit equipped

The scheduled date system or end item and its agreed upon support elements are issued to the designated initial operational capability unit and training specified in the new equipment training plan has been accomplished.

Fit

The ability of an item to physically interface or interconnect with or become an integral part of another item.

Form

The shape, size, dimensions, mass, weight, and other physical parameters that uniquely characterize an item. For software, form denotes the language and media.

Function

The action or actions an item is designed to perform.

Functional authority

The policy proponent or office with responsibility for certifying that the activity has been performed verified and accepted when appropriate.

Functional requirement

Administrative requirements, reports, and plans that do not directly prescribe the operational performance of a system but are used to support a program. These fall into two general categories: those that are generated by statute (the FAR, with supplements) and DOD directives and those that are generated by Army regulations, handbooks, pamphlets, or local policy. The second category, those generated by DA and below, may be exempted. The term does not include the operational requirements established by the CAPDEV.

Fuze (fuzing system)

A physical system designed to sense a target or respond to one or more prescribed conditions such as elapsed time, pressure, or command and initiate a train of fire or detonation in a munition. Safety and arming are primary roles performed by a fuze to preclude ignition of the munition before the desired position or time.

Gaining command

The ACOM/ASCC/DRU or a subordinate organization designated to receive the system being fielded.

Government-furnished equipment

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

Hardware

The physical, touchable, material parts of a computer or other system. The term is used to distinguish these fixed parts of a system from the more changeable software or data components it executes, stores, or carries. Computer hardware typically consists chiefly of electronic devices (central processing unit, memory, display) with some electromechanical parts (keyboard, printer, disk drives, tape drives, loudspeakers) for input, output, and storage.

Hazard

Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment.

Hazardous material

See AR 385–10.

Health hazard assessment

See AR 40–10. The Army's formal process used to identify, control, or eliminate health hazards associated with the development and acquisition of new materiel. Health hazard categories addressed by the HHA program include but are not limited to acoustic energy, biological and chemical substances, oxygen deficiency, ionizing and nonionizing radiation, shock, temperature, trauma, vibration, and ultrasound.

Human systems integration

A comprehensive management and technical strategy to ensure that human performance (the burden the design imposes on manpower, personnel, and training), and safety and health aspects are considered throughout the system design and development processes. The Army accomplishes the HSI goals through the MANPRINT program.

Identified risk

That risk which has been determined through various analysis techniques.

Independent safety assessment

See para 4–9. An evaluation of the PEO/PM safety program management and technical issues, problems, and hazards before a milestone decision review to enter an acquisition.

In-process review

Review of a project or program at critical points to evaluate the status and make recommendations to the decision authority.

Inductive analysis

Analyses that reasons from the specific to the general to determine WHAT failed states or other outcomes are possible given certain conditions (for example, failure modes and effect analysis).

Initial capabilities document

Documents the need for a materiel approach to a specific capability gap derived from an initial analysis of materiel approaches executed by the operational user and, as required, an independent analysis of materiel alternatives. It defines the capability gap in terms of the functional area, the relevant range of military operations, desired effects and time. The ICD summarizes the results of the doctrine, organization, training, materiel, leadership and education, personnel, and facilities analysis and describes why nonmateriel changes alone have been judged inadequate in fully providing the capability.

Initial operational capability

As defined within the capability development and production documents, it is the first attainment of the capability (as declared by the initial operational capability organization) by a modified table of organization and equipment unit and supporting elements to operate and effectively maintain a production item or system provided: The item or system has been type classified standard or approved for limited production; the unit and support personnel have been trained to operate and maintain the item or system in an operational environment; and the unit can be supported in an operational environmental in such areas as special tools, test equipment, repair parts, documentation, and training devices. Note: This designation is usually applied at a point in the Defense Acquisition Model that is after the full-rate production decision review and implies that the unit is combat ready.

Installation

An aggregation of contiguous or near contiguous, common, mission-supporting real property holdings under the jurisdiction of the Department of Defense or a State, the District of Columbia, Territory, Commonwealth, or possession, controlled by and at which an Army unit or activity is permanently assigned.

Integrated concept team

An integrated team made up of people from multiple disciplines formed for the purposes of developing operational concepts, developing materiel requirements documents, developing other requirements documents, when desired, and resolving other requirements determination issues.

Integrated logistics support (AR 700–127)

A unified and iterative approach to the management and technical activities to: Influence operational and materiel requirements, system specifications, and the ultimate design or selection (in the case of NDI/commercial off-the-shelf items); define the support requirements best related to system design and to each other; develop and acquire the required support; provide required operational phase support for best value; and seek readiness and cost improvements in the materiel system and support systems throughout the operational life cycle.

Integrated product/process team

A working level team of representatives from all appropriate functional disciplines working together to build successful and balanced programs, identify and resolve issues, and provide recommendations to facilitate sound and timely decisions.

Internal interface

Information exchange between various members of the system program office.

Interoperability

The ability of systems, units, or forces to provide services to, and accept services from, other systems, units, or forces and to use these services to enable them to operate effectively together.

Integrated product and process development

A management technique that simultaneously integrates all essential activities through the use of multidisciplinary teams to optimize the design, manufacturing and supportability processes. Integrated product and process development facilitates meeting cost and performance objectives from product concept through production, including field support.

One of the key integrated product and process development facilitates tenets is multidisciplinary team work through integrated product teams.

Integrated product/process team

A working level team of representatives from all appropriate functional disciplines working together to build successful and balanced programs, identify and resolve issues, provide recommendations to facilitate sound and timely decisions. Integrated product/process team may include members from both Government and industry, including program contractors and subcontractors.

Life-cycle management

A management process, applied throughout the life of a system that bases all programmatic decisions on the anticipated mission-related and economic benefits derived over the life of the system.

Low rate initial production

The first effort of the production and deployment phase. The purpose of this effort is to establish an initial production base for the system, permit an orderly ramp-up sufficient to lead to a smooth transition to full rate production, and to provide production representative articles for initial operational T&E and full-up live fire testing. This effort concludes with a full rate production decision review to authorize full rate production and deployment. The minimum number of systems (other than ships and satellites) to provide production representative articles for operational T&E, to establish an initial production base, and to permit an orderly increase in the production rate sufficient to lead to full rate production upon successful completion of operational testing. For Major Defense Acquisition Programs, low rate initial production quantities in excess of 10 percent of the acquisition objective must be reported in the Selected Acquisition Report. For ships and satellites, low rate initial production is the minimum quantity and rate that preserve mobilization.

Major Defense Acquisition Program

An acquisition program that is not a highly sensitive classified program (as determined by the Secretary of Defense) and that is designated by the Under Secretary of Defense for Acquisition, Technology, and Logistics as a Major Defense Acquisition Program and estimated by the Under Secretary of Defense for Acquisition, Technology, and Logistics to require an eventual total expenditure for research, development, test, and evaluation of more than \$365 million in fiscal year (FY) 2000 constant dollars or, for procurement, of more than \$2.190 billion dollars in FY 2000 constant dollars.

Major system

A combination of elements that shall function together to produce the capabilities required to fulfill a mission need, to include hardware, equipment, software, or any combination thereof, but excluding construction or other improvements to real property. A system shall be considered a major system if it is estimated by the DOD component head to require an eventual total expenditure for research, development, test, and evaluation of more than \$140 million in FY 2000 constant dollars, or for procurement of more than \$660 million in FY 2000 constant dollars.

Managing activity

The original element of DOD assigned acquisition management responsibility for the system, or prime or associate contractors or subcontractors who wish to impose system safety tasks on their suppliers.

Manpower and personnel integration

The comprehensive technical effort to identify and integrate all relevant information and consideration regarding the full range of manpower, personnel capabilities, training development and delivery, human factors engineering, system safety, health hazards, and Soldier survivability into the system development and acquisition process to improve Soldier performance, total systems performance, and reduce the cost of ownership to an acceptable level throughout the entire life cycle of a system. MANPRINT is the Army's Human Systems Integration process for systems acquisition.

Materiel developer

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

Materiel development

The conception, development, and execution of solutions to materiel requirements identified and initiated through the capability developments process, translating equipment requirements into executable programs within acceptable performance, schedule, and cost parameters.

Matériel fielding

The entire process of preparing, taking inventory, and issuing new matériel systems to gaining units.

Matrix support

All categories of functional support provided to the MATDEV necessary to execute/attain the acquisition objective, excluding the core office (tables of distribution and allowances) capability.

Milestone

A milestone is the major decision point that initiates the next phase of an acquisition program. Major Defense Acquisition Program milestones may include, for example, the decisions to begin engineering and manufacturing development, or to begin either low-rate initial or full-rate production. Major Automated Information System program milestones may include, for example, the decision to begin program definition and risk reduction.

Milestone decision authority

The person in whom is vested the authority to make milestone decisions. This may be the Defense Acquisition Executive, the component acquisition executive (for the Army, this is the AAE), or the PEO.

Mishap

An unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment.

Mishap probability

The aggregate probability of occurrence of the individual events/hazards that create a specific hazard.

Modeling and simulation

The development and use of live, virtual, and constructive models including simulators, stimulators, emulators, and prototypes to investigate, understand, or provide experiential stimulus to either (1) conceptual systems that do not exist or (2) real life systems that cannot accept experimentation or observation because of resource, range, security, or safety limitations. This investigation and understanding in a synthetic environment will support decisions in the domains of research, development, and acquisition and in advanced concepts and requirements or will transfer necessary experiential effects in the training, exercises, and military operations domain.

New equipment.

New or improved equipment introduced into the Army. New equipment applies to developed, modified, and non-developmental, and commercial items.

New equipment training

The identification of personnel, training, and training aids and devices and the transfer of knowledge gained during development from the matériel developer/provider to the trainer, user, and supporter.

Nondevelopmental items.

Items (hardware, software, communications/networks, and so forth) that are used in the system development program, but are not developed as part of the program. NDIs include, but are not limited to, commercial off-the-shelf items, Government-off-the-shelf, government-furnished equipment, re-use items, or previously developed items provided to the program "as is".

Operational architecture

Operational architecture contains text, graphic models to show functions and information required, graphic representations of how the Army organizes and equips to execute command, control, communication, and computer processes, and a data base to provide detailed characteristics about information exchanges, such as format voice/data/imagery), speed of service, perishability, and criticality. The operational architecture will show relationships among organizations and functions in terms of the information they need, use, and exchange.

Overarching integrated process/product team

The overarching integrated process/product team is a team appointed by the MDA, commensurate with the ACAT level, to provide assistance, oversight, and independent review for the MDA, as the program proceeds through its acquisition cycle.

Programmatic environmental, safety, and occupational health evaluation

The PESHE is the program office's acquisition documentation of the ESOH aspects of the program. The PESHE is

required at program initiation for ships, Milestones B, C, and full-rate production decision review. It is recommended that the PESHE be updated for the CDR.

Preplanned product improvements

Planned future evolutionary improvement of development systems for which design considerations are effected during development to enhance future applications of projected technology. It includes improvements planned for ongoing systems that go beyond the current performance envelope to achieve a needed operational capability.

Probability

See mishap probability.

Program, project, or product manager

A Headquarters, Department of the Army board-selected manager for a system or program. A PM may be subordinate to the AAE, PEO, or a materiel command commander. Refers to the management level of intensity the Army assigns to a particular weapon system or information system. As a general rule, a program manager is a general officer or Senior Executive Service; a project manager is an O-6 or GS-15; a product manager is an O-5 or GS-14.

Qualitative

Relative evaluation methodology using nonmathematical processes.

Quantitative

Evaluations based on numerical values and mathematical calculations.

Residual risk

The risk that remains after all planned risk mitigations have been implemented.

Reusability of software modules

The extent to which a program unit that is discrete and identifiable with respect to compiling, combining with other units, and loading and can be used as source code in multiple applications, for example, a message parsing module, mathematical equation module.

Risk

An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence.

Risk assessment

The process of characterizing hazards within risk areas and critical technical processes, analyzing them for their potential mishap severity and probabilities of occurrence, and prioritizing them for risk mitigation actions.

Safety

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

Safety assessment report

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

Safety Confirmation

A formal document that provides the MATDEV and the decision maker with the test agency's safety findings and conclusions and that states whether the specified safety requirements have been met. It includes a risk assessment for hazards not adequately controlled, lists technical or operational limitations, and highlights safety problems requiring further testing.

Safety critical

A term applied to a condition, event, operation, process, or item of whose proper recognition, control, performance, or tolerance is essential to safe system operation or use; such as, safety-critical function, safety-critical path, and safety-critical component.

Safety Release

A formal document issued to test organizations before any hands-on testing, training, use, or maintenance by Soldiers. The Safety Release is a stand-alone document that indicates the system is safe for use and maintenance by Soldiers and describes the specific hazards of the system based on test results, inspections, and system safety analysis. Operational limits, precautions, and proposed means of mitigating risks are included.

Severity

An assessment of the consequences of the worst credible mishap that could be caused by a specific hazard.

Software

The instructions executed by a computer, as opposed to the physical device on which they run (the “hardware”). Programs stored on nonvolatile storage built from integrated circuits (for example, ROM or programmable ROM) are usually called firmware. Software can be split into two main types—system software and application software or application programs. System software is any software that is required to support the production or execution of application programs but that is not specific to any particular application. Examples of system software include the operating system, compilers, editors, and sorting programs. Examples of application programs include an accounts package or a computer-aided design program. Software also includes any security information assurance vulnerability alert patches.

Software support activity

An organization assigned the responsibility for post-production software support.

Special tools

A special tool is a tool designed to perform a specific task for use on a specific end item or a specific component of an end item and is not available in the common tool load that supports that end item/unit. It is authorized by the repair parts and special tool list located within that end item’s TM.

Standardization

The process of developing concepts, doctrines, procedures, and designs to achieve and maintain the most effective levels of compatibility, interoperability, interchangeability, and commonality in the fields of operations, administration, and materiel. Standardization is the process by which nations achieve the closest practicable cooperation among forces, the most efficient use of research, development, and production resources, and items.

Subsystem

An element of a system that in itself may constitute a system.

Suitability

The degree to which a system can be supported when employed by Soldiers in an operational environment. Suitability includes reliability, availability, and maintainability, transportability, operational tempo, MANPRINT, safety, logistics, and so on.

Support items

A generic term that refers to the various classes of supply that encompass test, measurement, and diagnostic equipment, special tools and test equipment, technical manuals, training devices, and spare/repair parts used with or on a materiel system.

Supporting command

An AMC LCMC, Defense Logistics Agency, General Services Administration, or other wholesale managing activity that provides any materiel, services, or support equipment for the system being fielded.

Survivability

The capability of a system and crew to avoid or withstand a man-made hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission. Survivability considers ballistic effects; nuclear, biological, and chemical weapons; information assurance; countermeasures; electromagnetic environmental effects; obscurants; and atmosphere and vulnerability.

System

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

System evaluation plan

See AR 73-1. Documents integrated T&E planning. The detailed information contained in the SEP supports parallel development of the TEMP and is focused on evaluation of operational effectiveness, suitability, and survivability. While the documents are similar, the TEMP establishes “what” T&E will be accomplished and the SEP explains “how” the T&E will be performed.

System-of-systems

A set or arrangement of interdependent systems that are related or connected to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole. An example of a SOS could be interdependent information systems. While individual systems within the SOS may be developed to satisfy the peculiar needs of a given user group, the information they share is so important that the loss of a single system may deprive other systems of the data needed to achieve even minimal capabilities.

System safety

The application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.

System safety engineer

An engineer who is qualified by training and/or experience to perform SSE tasks.

System safety engineering

An engineering discipline requiring specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, or reduce the associated risk.

System safety engineering plan

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

System safety working group

A formally chartered group of persons, representing organizations associated with the system acquisition program, organized to assist the MA system PM in achieving the system safety objectives. Regulations of the military components define requirements, responsibilities, and memberships.

System safety management

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

System safety management plan

A plan that documents how materiel developers identify, tracks, and manages system hazards. (See Appendix C)

System safety manager

A person responsible to program management for setting up and managing the system safety program.

System safety program

The combined tasks and activities of system safety management and SSE implemented by acquisition project managers.

System safety risk assessment

A comprehensive evaluation of the risk and its associated impact.

Systems architecture

The physical layout, depicted graphically, showing the relationship of the information exchange and connectivity requirements. The SA identifies components, capabilities, and establishes interconnections among command, control, communication, and computer components of systems. The systems architecture can be developed for an individual system or at higher levels to depict the integration of numerous systems into a SOS architecture.

Systems engineering

The overarching process that a program team applies to transition from a stated capability to an operationally effective and suitable system. SE encompasses the application of SE processes across the acquisition life cycle (adapted to each and every phase) and is intended to be the integrating mechanism for balanced solutions addressing capability needs,

design considerations and constraints, as well as limitations imposed by technology, budget, and schedule. The SE processes are applied early in concept definition, and then continuously throughout the total life cycle.

Systems engineering plan

A description of the program's overall technical approach including processes, resources, metrics, applicable performance incentives, and the timing, conduct, and success criteria of technical reviews.

Technical architecture

Technical architecture is comparable to a building code, not telling you what to build (operational architecture) nor how to build (system architecture), but rather delineating the standards to build to and to pass inspection. The technical architecture identifies a framework of standards and includes top level system specifications, and architectural diagrams for technical interface specifications.

Technique

For analyses, refers to a specific method for analysis using specific engineering expertise (examples: fault tree, failure mode and effect analysis).

Test, measurement, and diagnostic equipment

Any system or device used to evaluate the operational condition of an end item or subsystem thereof or used to identify or isolate any actual or potential malfunction. The test, measurement, and diagnostic equipment includes diagnostic and prognostic equipment, semiautomatic and automatic test equipment (with issued software), and calibration test and measurement equipment.

Threat

Ability of an enemy, or potential enemy, to limit, neutralize, or destroy effectiveness of current or projected mission, organization, or item of equipment. Statement of that threat is prepared in sufficient detail to support Army planning and development of concepts, doctrine, training, and materiel. Statement of a capability prepared in necessary detail, in context of its relationship to specific program or project to provide support for Army planning and development for operational concepts, doctrine and materiel.

Total risk

The sum of identified and unidentified risks.

Training developer

Command or agency that formulates, develops, and documents or produces training concepts, strategies, requirements (materiel and other), and programs for assigned mission areas and functions. Serves as user (trainer and trainee) representative during acquisitions of their approved training materiel requirements and training program developments.

Training devices

Training aids, devices, simulators, and simulations which simulate or demonstrate the function of equipment or weapon systems. These items are categorized as follows: embedded, nonsystem, simulations, simulators, standalone, and system.

Training devices (embedded)

Training that is provided by capabilities designed to be built into or added on to operational systems to enhance and maintain the skill proficiency necessary to operate and maintain that system. Embedded training capabilities encompass four training categories. Category A (individual/operator): to attain and sustain individual, maintenance, and system orientation skills. Category B (crew): to sustain combat ready crews/teams, this category builds on skills acquired from Category A. Category C (functional): to train or sustain commanders, staffs, and crews/teams within each functional area to be utilized in their operational role. Category D (force level (Combined Arms Command and battle staff)): To train or sustain combat ready commanders and battle staffs utilizing the operational system in its combat operational role.

Training devices (nonsystem)

All training aids, devices, simulators, and simulations not defined as system training aids, devices, simulators, and simulations.

Training devices (simulators)

A training medium that replicates or represents the functions of a weapon, weapon system, or item of equipment generally supporting individual, crew, or crew subset training. Simulators may stand alone or be embedded.

Training devices (simulations)

A training medium designed to replicate or represent battlefield environments in support of command and staff training. Simulations may stand alone or be embedded.

Training devices (standalone)

An autonomous item of training equipment designed to enhance or support individual or collective training.

Training devices (system)

A training aids, devices, simulators, and simulations item that supports a specific materiel system or family of systems program.

Unacceptable risk

That risk which cannot be tolerated by the managing activity. It is a subset of identified risk. Unacceptable risk is either eliminated or controlled.

Unidentified risk

The risk that has not been determined. It is real. It is important. But it is not measurable. Some unidentified risk is subsequently determined when a mishap occurs. Some risk is never known.

User

Command, unit, element, agency, crew or person (Soldier or civilian) operating, maintaining, and or otherwise applying products in accomplishment of a designated mission.

User representative

Presents the user viewpoint during requirements determination, documentation, and acquisition processes.

Validation

The review of documentation by an operational authority other than the user to confirm the need or operational requirement. As a minimum, the operational validation authority reviews the mission need statement, confirms that a non-materiel solution is not feasible, assesses the joint service potential, and forwards a recommendation to the MDA for Milestones A action.

Section III**Special Abbreviations and Terms**

This section contains no entries.

UNCLASSIFIED

PIN 062355-000