

CHAPTER 3 SYSTEM SAFETY

This chapter presents the system safety aspects of air vehicle qualification. Topics include the system safety process, safety and hazard analysis, and flight safety parts. In addition, requirements are presented for the System Safety Program, System Safety Management Plan, and System Safety Program Plan.

3-1 INTRODUCTION

System safety is defined as “The application of engineering and management principles, criteria, and techniques to optimize safety within the constraints of operational effectiveness, time, and cost throughout all phases of a system life cycle.”, MIL-STD-882, *System Safety Program Requirements*, (Ref. 1).

A System Safety Program (SSP) is a formal approach to elimination of hazards through engineering design and analysis, management, and supervisory control of conditions and practices. The SSP encompasses the accomplishment of system safety management, research, and engineering tasks and is an essential element of the airworthiness qualification of the system.

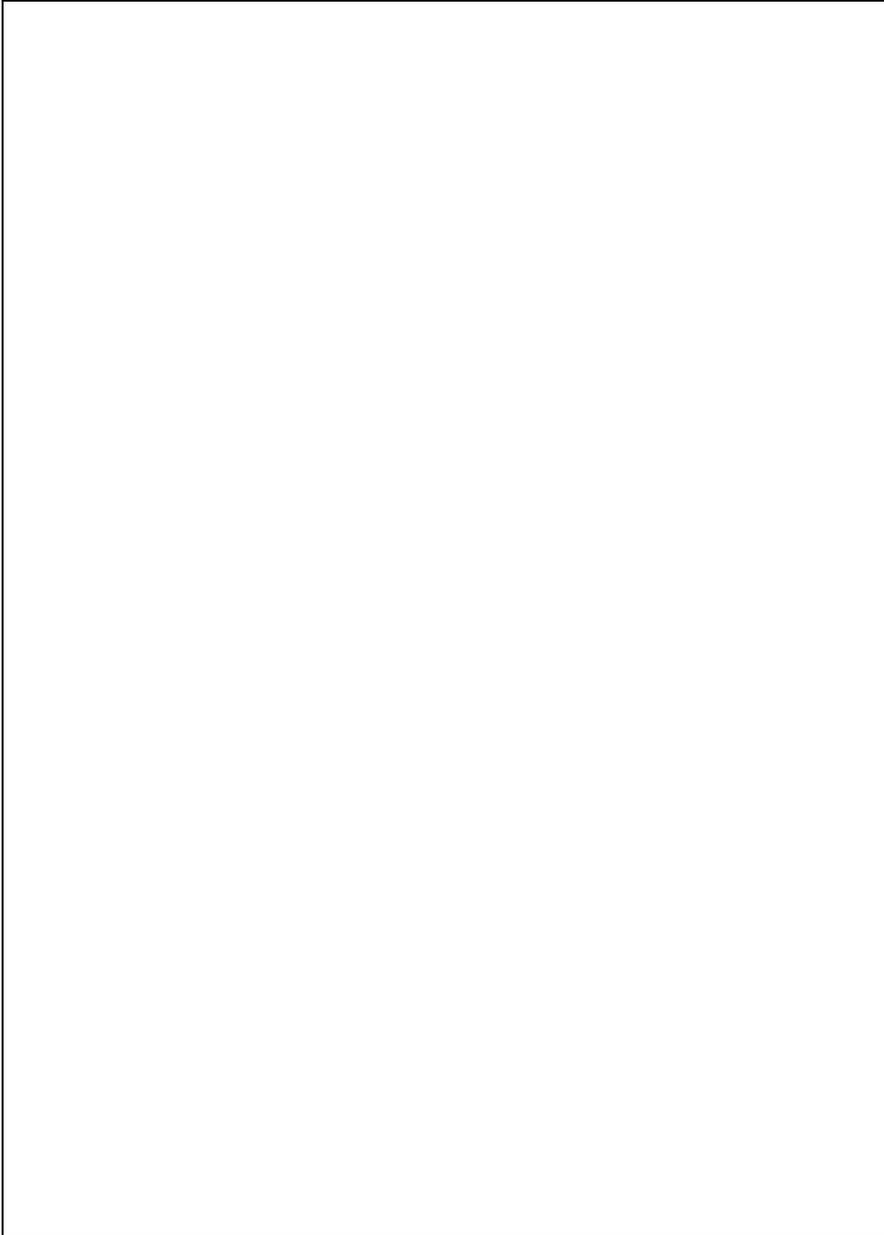
Typical air vehicle system safety tasks during the development process are depicted in Fig. 3-1. Milestones or checkpoints for system safety within the development process should be established at the outset of an air vehicle development program. Typical milestone tasks delineated in MIL-STD-882 (Ref.1) are shown in Fig. 3-1 opposite the equivalent tasks in the air vehicle development process. (These milestones are considered only typical and not necessarily complete in number.) The system safety activity starts early in the conceptual stage of air vehicle design and continues throughout the entire process. The system safety process described in this chapter is applied in an

iterative manner as the program progresses.

3-2 OBJECTIVES

The objectives of an SSP are to ensure that

1. Safety, consistent with mission requirements, is designed into the system in a timely, cost-effective manner.
2. Hazards associated with each system are identified, evaluated, and eliminated, or the associated risk is reduced to a level acceptable to the managing activity (MA) throughout the entire life cycle of a system. Risk should be described in risk assessment terms.
3. Historical safety data, including lessons learned from other systems, are considered and used.
4. Minimum risk is sought in accepting and using new designs, materials, and production and test techniques.
5. Actions taken to eliminate hazards or reduce risk to a level acceptable to the MA are documented.
6. Retrofit actions required to improve safety are minimized through the timely inclusion of safety features during research and development and acquisition of a system.
7. Changes in design, configuration, or mission requirements are accomplished in a manner that maintains a risk level acceptable to the MA.



8. Consideration is given to safety, ease of disposal, and demilitarization of any hazardous materials associated with the system.

9. Significant safety data are documented as “lessons learned” and are submitted to data banks as proposed changes to applicable design handbooks and specifications. (Ref. 2)

3-3 SYSTEM SAFETY PROCESS

The system safety process is shown graphically in Fig. 3-2 and described in the subparagraphs that follow. This process shows a logical approach to attaining the system safety objectives in par. 3-2. The process is repeated as necessary in an iterative fashion at every level of complexity in the design of a system until the requisite assurance of the system hazard level is attained. An integral part of the system safety process is hazard tracking, which is a closed loop system used to identify, monitor, and eliminate hazards. Hazard tracking is developed early in the system safety process and is used throughout the process to document and track hazards and the progress made toward resolution of the associated risk.

3-3.1 KNOWN PRECEDENT (BLOCK A, FIG. 3-2)

From the beginning a System Safety Program should be based on the experience and knowledge gained from previous operations in correcting design deficiencies that have resulted in the accidental loss of or damage to materiel or injuries or death to personnel. Those design features categorized previously as having hazards are also identified, and the hazards corrected if required. It is essential that designers of future air vehicles benefit from all previous experience that affects safe operation.

3-3.2 SYSTEM DELINEATION (BLOCK B)

The boundaries of the system under consideration and its constituent elements are defined clearly as early as possible and revised as required during the system life cycle. Such delineation establishes the limits for succeeding steps in the process and reduces complex systems to manageable parts. Any entity can be labeled a “system” provided it is accurately defined.

3-3.3 IDENTIFICATION OF FLIGHT SAFETY PARTS (BLOCK C)

Flight safety parts are parts whose failure or malfunction could result in an unsafe condition. The handling of flight safety parts is discussed in par. 3-13.

3-3.4 SYSTEM HAZARD ANALYSIS (BLOCK D)

The heart of system safety is the analysis of a system and its elements in a methodical manner. Beginning with preliminary hazard analyses of design concepts and continuing through an integrated hazard analysis of the complete system, this analytical process distinguishes system safety from other separate, but closely interfacing, disciplines. The contractor should select the methodology and techniques for hazard analysis best suited for the particular system element under consideration and for the applicable level of detail design.

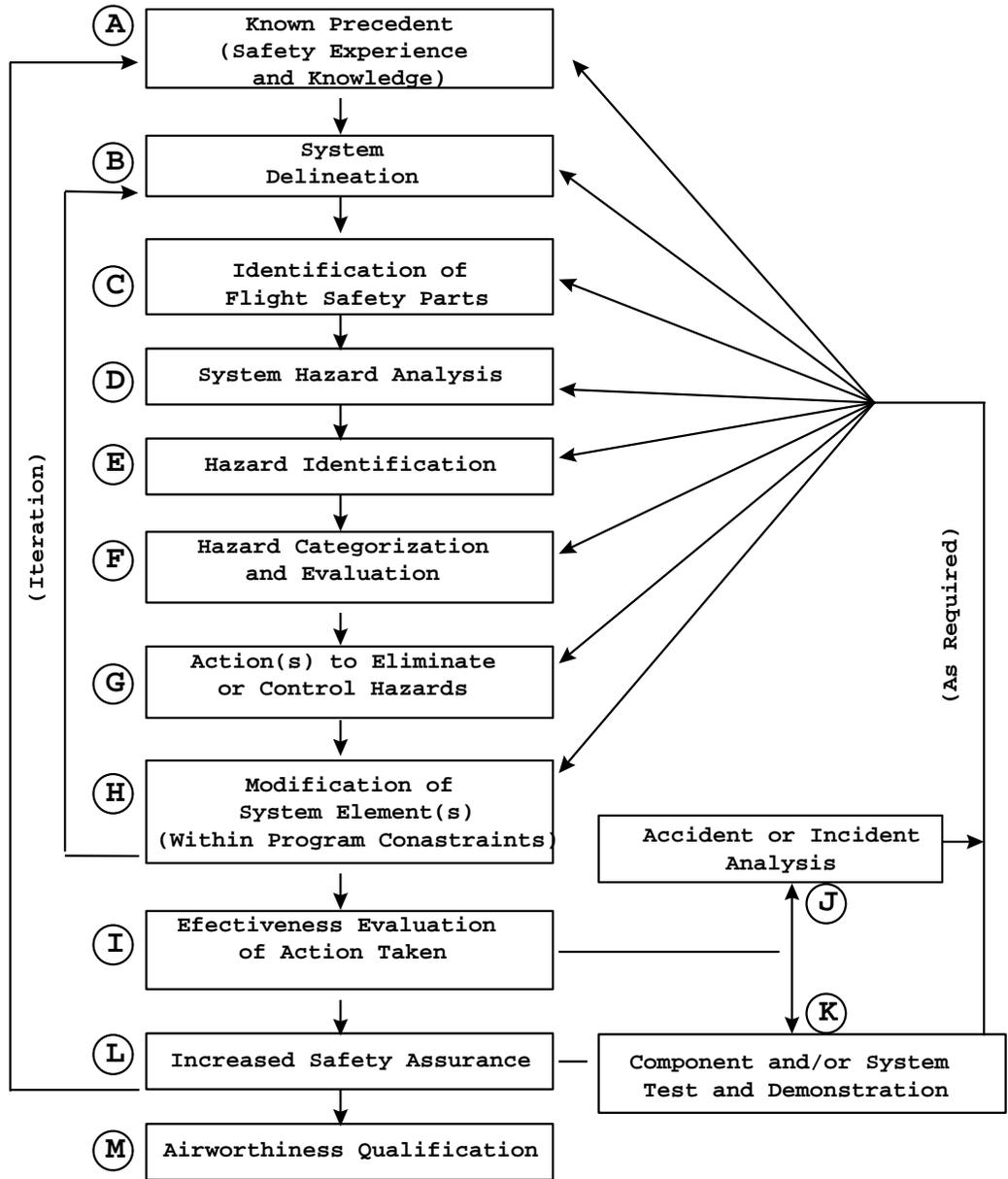


Figure 3-2 System Safety Process

3-3.5 HAZARD IDENTIFICATION (BLOCK E)

By using systematic hazard analyses, the design engineer identifies those features of a system that potentially may cause damage, loss, or injury. Such identification assists the designer in his or her initial efforts by calling attention to undesirable features or deficiencies that can be either eliminated or controlled efficiently early in the design process. As the design proceeds, additional hazards are identified through the system safety process.

3-3.6 HAZARD CATEGORIZATION AND EVALUATION (BLOCK F)

It is impractical to eliminate all hazards identified in a system. The appropriate action to be taken as a result of hazard identification depends on how often the hazard occurs, i.e., frequency, and the impact of the consequences that result from the hazard occurring, i.e., severity. The factors of hazard frequency and severity establish the residual risk of the system. Categorization of hazards according to criteria specified by the procuring activity serves to guide corrective action based upon assessment of the potential residual risk. Evaluation of identified hazards and hazard risk management require relating a hazard to its impact on mission effectiveness, system performance, and program success. This categorization and evaluation are essential parts of the decision-making process to determine appropriate corrective action.

3-3.7 ACTION(S) TO ELIMINATE OR CONTROL HAZARD(S) (BLOCK G)

The system safety process produces no useful result until some action is taken to eliminate or control identified hazards. The effect of alternative courses of action in the design process and tradeoff studies to eliminate or control identified hazards should be considered. Thus management is presented with a tool with which decisions can be made based on other program constraints.

3-3.8 MODIFICATION OF SYSTEM ELEMENTS (BLOCK H)

Any action taken in Block G necessarily results in the modification of some element or elements of the air vehicle system. As a result, the delineation of the system (Block B) should be revised accordingly. The system safety process is then repeated as required until no unacceptable additional hazards are generated by the system modification. This step ensures that a new hazard is not inadvertently introduced into the system while another hazard is being eliminated.

3-3.9 EFFECTIVENESS EVALUATION OF ACTION TAKEN (BLOCK I)

Actions taken to correct hazards as a result of the system safety process are evaluated on how effectively they achieve the system safety objective. A satisfactory evaluation results in increased assurance in the level of safety of the system (Block L).

3-3.10 ACCIDENT OR INCIDENT ANALYSIS (BLOCK J)

The occurrence of an accident or incident of course leads to an unsatisfactory evaluation. The analysis of such an accident or incident experience should reveal any deficiencies in the conduct of the system safety program and direct corrective action to the appropriate step in the process.

3-3.11 COMPONENT AND/OR SYSTEM TEST AND DEMONSTRATION (BLOCK K)

Analytical techniques alone are not sufficient to identify system hazards adequately, and this inadequacy is determined in Block I. Tests and demonstrations normally conducted as part of an air vehicle development program are planned and conducted to reveal such inadequacies. In addition, these tests and demonstrations serve to verify the results of the system safety process and to contribute to the assurance desired. Should system testing reveal additional problems, corrective action is applied at the appropriate step in the process.

3-3.12 INCREASED SAFETY ASSURANCE (BLOCK L)

The assurance that the objectives of system safety are being met is cumulatively increased as the program progresses and contributes increased knowledge to subsequent cycles of the process (Block A).

3-3.13 AIRWORTHINESS QUALIFICATION (BLOCK M)

Ultimately, the system safety process results in data and information that serve as an essential element of airworthiness qualification. The methods and procedures to be followed are pre-

scribed in the Airworthiness Qualification Specification (AQS).

3-4 ANALYTICAL METHODOLOGIES AND TECHNIQUES

Hazard analysis is the heart of the system safety process and requires inductive thought as well as deductive reasoning. An analysis may be either qualitative or quantitative. A qualitative analysis is generally conducted first to provide a departure point for the quantitative analysis. A qualitative analysis examines events to determine the possible existence of hazards, the accidents that could result, possible effects, and safeguards. A quantitative analysis permits comparison of the changes in probabilities if safeguards or alternative designs are used in the system. Results of quantitative analysis may be probabilistic or relativistic, i.e., using comparisons based on judgment.

The ultimate purpose of hazard analysis is to aid management in reaching the determination that the objectives discussed in par. 3-2 have been achieved within the constraints of the particular air vehicle development program. In addition, these analyses form a baseline which can be evaluated objectively by someone other than a system safety analyst to measure the effective influence of subsequent design changes.

There are several types of widely used analyses for system safety. Selection of the analytical methodology or technique to be used in a given program is the responsibility of the contractor and depends upon the level of detail required by program phases, requirements for qualitative and quantitative results, and the particular capabilities developed by the contractor. Methodology selection should maximize use of the design detail

available at the particular phase of the program to ensure the analysis is as comprehensive as possible, and is thorough and accurate. MIL-STD-882 (Ref. 1) should be used as a guide for analyses, methods, and techniques. Also MIL-HDBK-764, *System Safety Design Guide for Army Materiel*, (Ref. 2) may be used as a guide.

MIL-HDBK-764 describes techniques of analysis such as fault hazard analysis (FHA), fault tree analysis (FTA), sneak circuit analysis (SCA), and failure, modes, effects, and criticality analysis (FMECA) that have value for hazard analysis. In addition, Ref. 2 identifies analysis techniques, such as circuit logic analysis, interface analysis, mapping, Monte Carlo simulation, contingency analysis, environmental factors analysis, critical incident technique, and mock-ups, that can be used to support these analyses.

3-5 KNOWLEDGE OF HAZARDS

The system safety analyst should have a thorough knowledge not only of air vehicle engineering but also of hazardous conditions.

For example, major rotorcraft configurations—such as the type of rotor, e.g., articulated or bearingless, the method of directional control, and the control system concept—have inherent safety implications. The tradeoffs used to reach a decision regarding these configurations should include system safety considerations. In addition, hazards are more likely to be present at interfaces between subsystems than within a single subsystem. Some examples of possible interfaces that could lead to hazards are fuel system to engine fuel lines, clearance between components, and connectors that can be improperly installed.

The system safety analyst must also be aware of those conditions that have been proven by past experience to be hazardous for air vehicles. The consideration of hazards must not be limited to those conditions involving only hardware. Software is an important consideration. Also the interactions of air vehicles with personnel who operate and maintain them and those between personnel and the environment in which the air vehicles are used provide potentially hazardous conditions, which should be considered during design. Some examples of possible interrelationships that could lead to hazards are the height of the main rotor above the ground and the location of the pilot with respect to the rotor path.

3-6 CLASSIFICATION OF HAZARDS

Since it is impossible to eliminate or control all hazards, they are usually ranked by degree of severity, i.e., consequences in operation of the air vehicle. Four hazard levels ranging from negligible to catastrophic are defined and established in MIL-STD-882. These are listed in Table 3-1 along with their effect on personnel safety, examples of functional hazards, and definitions. Table 3-2 provides MIL-STD-882 probability levels along with an example of quantitative probabilities. Quantitative probabilities should be developed for each weapon system to meet specific program requirements. For any given hazard a degree of severity and probability of occurrence may be assigned. Table 3-3 shows how those two aspects of a hazard may be combined to arrive at a risk

TABLE 3-1. HAZARD SEVERITY CATEGORIES

DESCRIPTION	CATEGORY	EXAMPLES OF FUNCTIONAL HAZARDS	EFFECT ON PERSONNEL	DEFINITIONS
CATASTROPHIC	I	System nonfunctional; not economically salvageable. Total loss.	Personnel suffer death or serious or multiple injuries precluding return to current duties.	Death, system loss, or severe environmental damage.
CRITICAL	II	Major subsystem(s) non-functional. Hazard requires immediate corrective action.	Personnel suffer serious or multiple injuries requiring extended rehabilitation before return to current duties.	Severe injury, severe occupational illness, major system or environmental damage.
MARGINAL	III	Flyable aircraft; mission equipment or one of redundant subsystems nonfunctional. Hazard can be counteracted or controlled.	Personnel suffer injury requiring short-term recuperation before return to current duties.	Minor injury, minor occupational illness, or minor system or environmental damage.
NEGLIGIBLE	IV	Mission capable with minor performance loss or no immediate effect. Deferrable maintenance.	Personnel suffer minor injury that does not interrupt current duties.	Less than minor injury, occupational illness, or less than minor system or environmental damage.

TABLE 3-2. HAZARD PROBABILITY

DESCRIPTION	LEVEL	GENERIC DEFINITION (MIL-STD-882)	EXAMPLE: MEAN OPERATING HOURS BETWEEN OCCURRENCES	EXAMPLE: EXPECTED NUMBER OF OCCURRENCES PER 100,000 FLIGHT HOURS
FREQUENT	A	Likely to occur frequently	< 10	> 10,000
PROBABLE	B	Will occur several times in life of item	10 - 100	1000 - 10,000
OCCASIONAL	C	Likely to occur sometime during life of item	100 - 1000	100 - 1000
REMOTE	D	Unlikely but possible to occur in life of item	1000 - 10,000	10 - 100
IMPROBABLE	E	So unlikely, it can be assumed occurrence may not be experienced	> 10,000	< 10

severity category. The table also shows that for each risk severity category, a level of Army management authority has been assigned to accept the residual risk associated with the particular hazard in question. For example, a risk whose hazard severity is judged to be “critical” and whose hazard probability is “probable” would have a risk severity category of “HIGH” associated with it. For an Army Materiel Command (AMC)- Aviation (Table 3-3(A))-developed system, the Commander AMC would be the management authority for acceptance of a “HIGH”-risk haz-

ard. For an Aviation-Program-Executive-Office (PEO) (Table 3-3(B))-developed system, the Army Acquisition Executive (AAE) or his designee would be the management authority level for acceptance of a “HIGH”-risk hazard. Similarly, for a hazard whose severity is considered “negligible” and whose hazard probability is frequent, the corresponding hazard risk assessment is “LOW”. The program manager or equivalent is the management authority for the acceptance of a “LOW” risk.

TABLE 3-3. RISK SEVERITY CATEGORY MATRIX

(A) ARMY MATERIEL COMMAND -AVIATION

SYSTEM SAFETY MANAGEMENT DECISION AUTHORITY MATRIX

		HAZARD PROBABILITY				
		FREQUENT	PROBABLE	OCCASIONAL	REMOTE	IMPROBABLE
SEVERITY		A	B	C	D	E
CATASTROPHIC	I					
CRITICAL	II	HIGH				
MARGINAL	III	MEDIUM				
NEGLIGIBLE	IV					LOW

*CG AMC if PMs report directly to HQ AMC

(B) AVIATION PROGRAM EXECUTIVE OFFICE

TAILORED SYSTEM SAFETY MANAGEMENT DECISION AUTHORITY MATRIX

		HAZARD PROBABILITY				
		FREQUENT	PROBABLE	OCCASIONAL	REMOTE	IMPROBABLE
SEVERITY		A	B	C	D	E
CATASTROPHIC	I					
CRITICAL	II	HIGH				
MARGINAL	III	MEDIUM				
NEGLIGIBLE	IV					LOW

- CGAMC = Commanding General, US Army Materiel Command
- MSC = major subordinate command
- CDR = commander
- PM = program manager
- MGR = manager
- PEO = program executive office
- EQ = equivalent

The decision authority matrix can be tailored upon authorization from the “HIGH” risk hazard authority. Both examples in Table 3-3 are tailored for aviation. The tables are identical except for the decision level authorities.

3-7 RESOLUTION OF HAZARDS

Hazards are resolved through elimination or control. Documentation of actions is by means of substantiation of hazard resolution. These two aspects of system safety—hazard control and substantiation—are addressed in the subparagraphs that follow.

3-7.1 CONTROL METHODS

MIL-STD-882 discusses methods of resolving hazards. The first and most desirable method is to eliminate an identified hazard by selection of a design in which the hazard does not appear. If elimination of a hazard is impossible or uneconomical, the next step is to make the design tolerant of the hazard.

Three ways of making a design tolerant of identified hazards are stipulated in MIL-STD-882 in descending order of desirability. The first alternative is to reduce the significance of the hazard through the use of appropriate safety devices. Ideally, such devices should not require human intervention but should operate automatically if the specified hazardous condition arises.

The next choice is to place warning devices in the system to make known to the crew the existence of a hazardous condition. These devices would require human intervention to respond to the warning produced. Audio or visual indicators are commonly used in these instances, but there is a limit to the number of such devices that can be effectively used in one system design. Also such features must be coordinated

closely with the human factors engineering function.

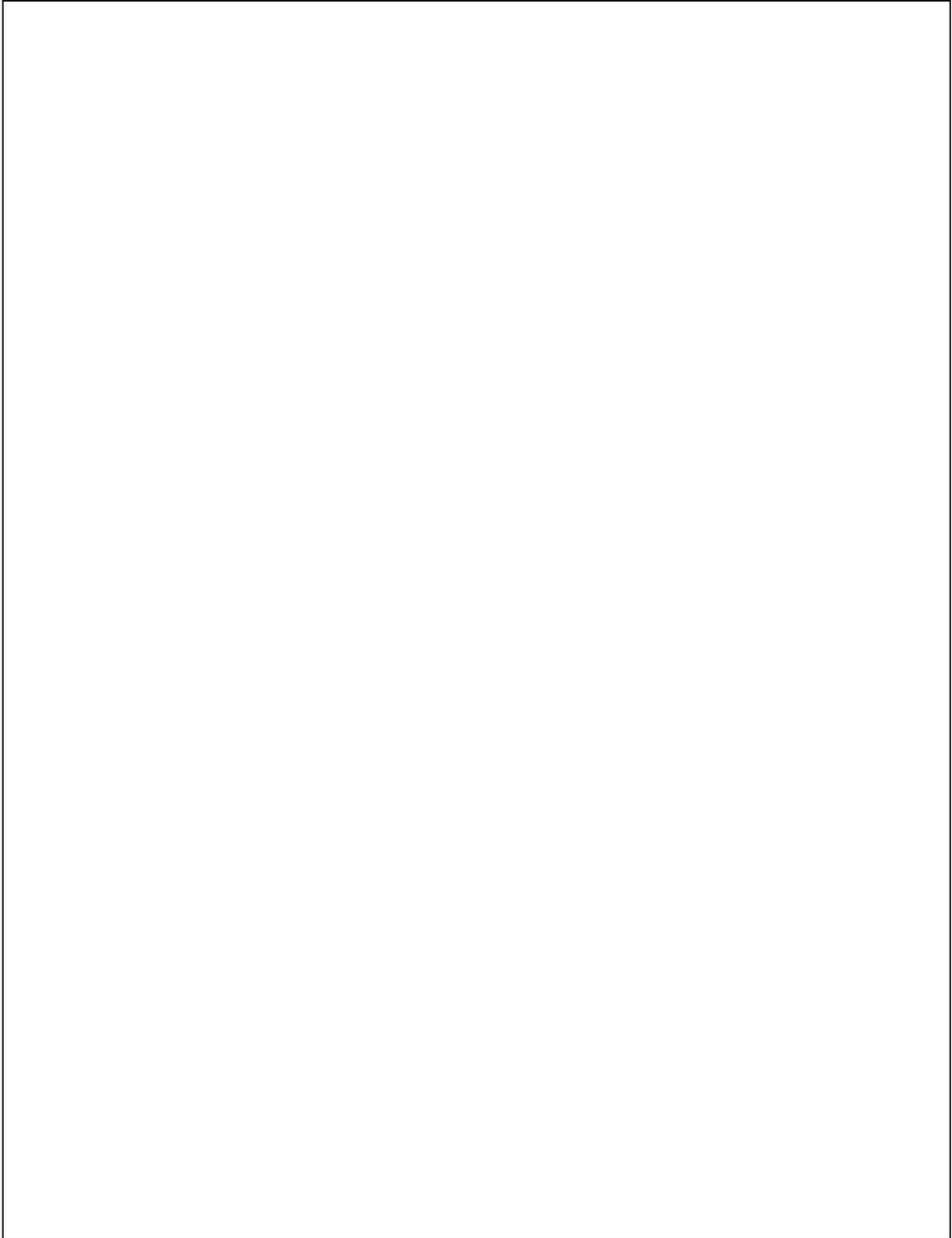
The final and least desirable choice is to prepare, disseminate, and enforce special operating procedures for an identified hazardous condition. However, these procedures are a weak link in achievement of system safety because of the inability to verify communication of the procedure to the person who must operate in accordance with such procedures.

3-7.2 SUBSTANTIATION OF HAZARD RESOLUTION

Once each possible hazard has been analyzed for its significance and resolution of the hazard is determined, there is need for assurance that proper corrective action has been taken. This can be accomplished by inspections, additional analyses, and design reviews. Catastrophic, critical, and other identified hazards should not rely solely on warnings, cautions, or procedures for control of risk.

A particular type of design review that can be effective for system safety is an electronic mock-up review. Functional mock-ups can also become an excellent method of identifying additional potential hazards. Also an electronic mock-up brings the subsystems together at an early stage, i.e., before interface problems become too expensive to change.

Fig. 3-3, taken from MIL-HDBK-764(MI) (Ref. 2), provides a sample format for documenting the identification, risk assessment, and corrective action for hazards. There are also automated hazard-tracking systems that can serve this purpose.



The System Safety Risk Assessment (SSRA), as defined by Army Regulation (AR) 385-16, *System Safety Engineering and Management*, (Ref. 3),

provides a comprehensive evaluation of the safety risk being assumed for a system. It contains identification of the item or system, and for each re

residual hazard, a description of the hazard and its severity and frequency, a source document or reference, alternative actions that could reduce the hazard level, and a recommendation from the project office regarding risk acceptance. Additionally, the SSRA includes recommendations from the appropriate safety manager, the combat developer, and the materiel developer as to acceptability of the residual risk. Finally, the decision of the appropriate acquisition manager is also recorded in the SSRA.

The Health Hazard Assessment (HHA) is performed by applying biomedical and psychological knowledge and principles to identify, evaluate, and control the risk to the health and effectiveness of personnel who test, use, or service the system. The results of the HHA should be included as an addendum to another required analysis report, such as the System Hazard Analysis Report. The HHA task and format should not be confused with the Health Hazard Assessment Report (HHAR), which is prepared by the Government using data provided by the HHA.

Fig. 3-4, taken from Ref. 4, shows a sample Safety and Health Data Sheet which might be used as part of the internal control process of an organization to record health and safety actions. The Safety and Health Data Sheet along with System Safety Risk Assessments are also documentation requirements supporting the materiel release process.

3-8 SYSTEM SAFETY MANAGEMENT PLAN

The System Safety Management Plan (SSMP) is a description of the planned methods to be used by the Government to monitor the contractor's system safety program and to manage the

system safety risks associated with residual hazards.

3-8.1 PURPOSE

The purpose of the SSMP is to define formally the responsibilities and authorities related to the system safety aspects of a program.

3-8.2 CONTENTS

Typically, the SSMP defines the internal management responsibilities of the Government, schedule, and procedures for accomplishment of the system safety management functions that follow:

1. Coordinate and execute procedures to assure appropriate interface with other management functions, e.g., quality assurance, maintenance, research, and development.
2. Establish an audit program to ensure that the objectives and requirements of system safety are attained.
3. Perform liaison with other agencies and commands as needed to attain system safety objectives.
4. Ensure that enough competent persons are assigned to the system safety engineering and management programs to assure proper implementation of system safety.
5. Evaluate, as part of source selection evaluation, the ability of the contractor to include system safety aspects in the final product.
6. Establish the policy and requirements to develop system safety in sufficient detail to identify the safety and health hazards of a system and to remove or control them.
7. Prescribe procedures for management participation in system risk acceptance for residual hazards.

Item/System identification: _____

1. Safety Evaluation Letter/Reports: _____
 - a. Safety Assessment Report: _____
 - b. Safety Analyses/Studies: _____
 - c. Development Test(s): _____
 - d. Operational Test(s): _____
 - e. Production Test(s): _____
2. Item does (does not) contain radioactive materials and (if it does) is properly licensed by (NRC # _____ and/or DA Authorization # _____ as appropriate).
3. Item does (does not) contain explosives/hazardous materials and (if it does) has the following hazard classifications:
 - a. Quantity-Distance Class: _____
 - b. Storage Compatibility Group: _____
 - c. DOT Class: _____
 - d. DOT Marking: _____
 - e. Conveyor Spacing Distance: _____
4. Item does (does not) contain munitions. If it does:
 - a. Compatibility of the following weapon/ammunition components has been established:

 - b. Range safety data (for inclusion in AR 385-62 or AR 385-63) was (will be) finalized (date) _____

Sample format, contractor format or program tailored format may be used.

Figure 3-4 Safety and Health Data Sheet (Ref. 4)

8. Provide system safety data for inclusion in requirements documents.
9. Review and approve System Safety Program Plans.
10. Provide a safety readiness position for program milestone reviews or documents associated with reviews, such as Decision Coordinating Papers or Army program memoranda.
11. Review and approve safety verification documents.
12. Provide safety input to major review boards, such as the Level 1 Configuration Control Board and the Materiel Release Review Board.
13. Assist in safety assessments and other reviews for fielded systems.
14. Establish indicators to measure the effectiveness of the system safety effort.

3-9 SYSTEM SAFETY PROGRAM PLAN (SSPP)

System safety should be considered early in any development process. Although concept evaluation becomes the primary focus early in the program, system safety should be an important factor in evaluation of the design concepts. Requirements and methods needed to ensure safety should be considered early. This can be accomplished during all phases of development with a well-defined SSPP. The contractor should propose an SSPP for approval by the Government. The SSPP is a written plan used to outline the steps required to ensure the activities of system safety engineering, system safety management, and other disciplines and functions are used and coordinated to guarantee system safety. The following subparagraphs describe the purpose and content of the SSPP.

3-9.1 PURPOSE

The purpose of the SSPP is to provide a basis of understanding between the contractor and the procuring activity as to how the System Safety Program will be incorporated into the development effort.

3-9.2 CONTENTS

The SSPP should define the System Safety Program scope and objectives. As a minimum, each SSPP should describe the four elements of an effective system safety program: a planned approach to task accomplishment, qualified people to accomplish tasks, authority to accomplish tasks through all levels of management, and appropriate resources—both manning and funding—to assure tasks are completed. The scope is described, and a list of tasks and activities is provided.

The SSPP describes the system safety organization or function within the organization of the total program, the responsibility and authority of system safety personnel, and the staffing of the system safety organization. In addition, it should describe the procedures by which the contractor will integrate and coordinate the system safety efforts and the process through which contractor management decisions will be made.

The SSPP should define System Safety Program milestones, provide a program schedule of safety tasks, and to preclude duplication, identify integrated system activities, i.e., design analyses, tests, and demonstrations, applicable to the System Safety Program but specified in other engineering studies.

The SSPP describes general engineering requirements and design criteria for safety, describes safety requirements for support equipment, and operational safety requirements for all appropriate phases of the life cycle up to and

including disposal. It describes the risk assessment procedures and the hazard severity categories, hazard probability levels, and system safety precedence that should be followed to satisfy the safety requirements of MIL-STD-882. It states the quantitative and qualitative measures of safety to be used for risk assessment including a description of the acceptable risk level. It describes closed-loop procedures used to take action to resolve identified hazards.

With respect to hazard analyses, the SSPP describes the analysis techniques and formats to be used in qualitative or quantitative analysis to identify hazards, their causes and effects, hazard elimination, or risk reduction requirements and how those requirements are met. It describes the depth within the system to which each technique is used, including hazard identification associated with the system, subsystem, component, personnel, ground support equipment, Government-furnished equipment (GFE), facilities, and their interrelationship in the logistic support, training, maintenance, and operational environments. It also describes integration of the subcontractor's hazard analyses with overall system hazard analyses.

With respect to system safety data, the SSPP describes the approach to be used to research, distribute, and analyze pertinent historical hazard or mishap data. It identifies deliverable data by title and number. It identifies non-deliverable system safety data and describes the procedures used for access by the procuring activity and to retain data of historical value.

The SSPP describes the verification—test, analysis, inspection, etc.—requirements for ensuring that safety is adequately demonstrated. It identifies the certification requirements for safety

devices or other special safety features. It describes the procedures used to ensure test information is transmitted to the procuring activity for review and analysis, and it provides procedures used to ensure safe conduct of all tests.

The SSPP describes the techniques and procedures of an audit program to be used by the contractor to ensure the objectives and requirements of the system safety program are being accomplished.

The SSPP describes the safety training for engineering, technical, operating, and maintenance personnel. It describes the mishap and hazardous malfunction analysis process including alerting the procuring activity to hazardous conditions.

The SSPP identifies in detail the interface between system safety and all other applicable safety disciplines such as nuclear safety, range safety, explosive and ordnance safety, chemical and biological safety, laser safety, nonionizing radiation safety, and any others. In addition, it identifies the interface between system safety and all other support disciplines such as maintenance, quality control, reliability, human factors engineering, medical support (health hazard assessments), and any others.

The SSPP can be submitted as part of a contractor's proposal, or it can be submitted shortly after the start of the contract.

3-10 SAFETY ANALYSES AND ANALYSIS TECHNIQUES

Safety analyses and analysis techniques, as described in MIL-STD-882 and MIL-HDBK-764, are the preliminary hazard analysis, the subsystem hazard analysis, the system hazard analysis, and the operation and support hazard analysis. Although there are a

number of other MIL-STD-882 (Ref. 1) tasks, such as preliminary hazard list, health hazard assessment, test and evaluation safety, safety verification, and safety compliance assessment, these tasks are not described in this handbook.

3-10.1 PRELIMINARY HAZARD ANALYSIS

The preliminary hazard analysis (PHA) is the first of a series of safety analyses conducted during the life cycle of a system or item of equipment. The PHA is used to obtain an initial risk assessment of a concept or system. PHA effort should be started during the earliest phases of the program so that safety considerations are included in tradeoff studies and design alternatives. A carefully executed PHA should provide the following information:

1. Specific potential hazards in a proposed system
2. The probable magnitude and frequency of each adverse effect to a proposed system with and without the recommended safeguards. This information can be used in tradeoff studies of alternatives.
3. Proposed measures to eliminate or control the potential hazards
4. The safety-critical equipment and situations upon which the designers must focus their hazard elimination or control efforts
5. Potential events (accidents) that should be subjected to detailed analysis when additional information becomes available
6. Potential personnel errors that can lead to accidents avoidable by design features such as interlocks, warnings, and procedural instructions
7. Identification of specific safety essentials that satisfy require-

ments in standards, specifications, or similar documents

8. Notes on accidents, near misses, and other potential safety problems uncovered during experience with predecessor systems
9. Potential hazards whose control should be verified through specific safety testing.

3-10.2 SUBSYSTEM HAZARD ANALYSIS

The subsystem hazard analysis (SSHA) identifies hazards associated with the design of subsystems. The analyses should include evaluation of component failure modes, critical human error inputs, and hazards resulting from functional relationships among components and equipment comprising each subsystem. The methods involved in the SSHA are similar to the PHA but are focused on at the subsystem level.

As a minimum, each subsystem should be examined. If a subsystem has been in use for some time, it may be unnecessary for the analysis to go below the subsystem level because the hazards of the subsystem have been identified and corrective action taken. If a subsystem is new and has not had prior use, it may be necessary for the analysis to go to the component level.

The SSHA report should provide the following items:

1. A summary of the results
2. A list of identified hazards that includes the information that follows:
 - a. Component(s) Failure Mode(s). All failure modes that can result in a hazard are discussed. Generally, failure modes explain "how" something fails.

b. System Event(s) Phase. The mission phase of the system when the hazard is encountered is addressed.

c. Hazard Description. A complete description of the hazard is given.

d. Effect on Subsystem and/or System. The effect of the hazard on the subsystem should be considered. Also the possible upstream and downstream effects should be considered.

e. Risk Assessment. A risk assessment for each hazard, as defined in MIL-STD-882 or other documents applicable to the system, should be given.

f. Recommended Action. The action that should be taken to eliminate the hazard is presented. Various courses of action should be discussed, where appropriate. The recommended actions should be in sufficient detail to be of value to the design engineer.

g. Effect of Recommended Action. The change in the risk assessment that the recommended action will effect should be discussed.

h. Remarks. This block should be used for any information, such as references, administrative information, or data on previous similar systems, that has not been included in other parts of the report.

i. Status. The status of action(s) taken to reduce or control the hazard should be given.

Various methods of analysis have been developed to obtain the data necessary for the SSHA. These include the failure modes effects and criticality analysis, the fault hazard analysis, the fault tree analysis (FTA), and the sneak circuit analysis.

3-10.3 SYSTEM HAZARD ANALYSIS

The system hazard analysis (SHA) is necessary to define the safety

interfaces between subsystems and to identify possible safety hazards in the overall system. Typically, it will determine whether system hazards can be eliminated or controlled with design safeguards. The need for procedural safeguards, however, should be recommended only as a last resort. The SHA is usually initiated during the early stages of development and updated as the system matures in order to reflect design changes and any new mission requirements or procedures that might affect system safety.

The SHA analyzes the effect that each subsystem has on all of the others during the normal and abnormal operation of each, but more importantly, it analyzes the operation of the system as a whole. The SHA should establish that separate units and subsystems can be integrated into a safe system. The operation of one unit or subsystem should not impair the safe performance of, or cause damage to, another unit or subsystem within the system. Because the human reactions required for normal system operation are considered part of the system, "human error" should be considered as a possible failure mode in the SHA. Lastly, the environment should have an effect on the system and must be considered in the SHA. The value of an SHA lies in its identification of

1. Interface problems
2. Dependent failure problems
3. Synergistic hazards
4. Additive hazards.

When a safety level has been defined for a specific system, proof that the design satisfies that safety requirement can be obtained only by preparing an SHA. Other safety analyses, studies, test reports, experience with related systems, and program data, such as reliability re-

ports, provide useful support of the SHA.

3-10.4 OPERATION AND SUPPORT HAZARD ANALYSIS

Operation and support hazard analyses (O&SHAs) are methods by which designers and analysts can evaluate the prescribed (and possible alternative) operation and maintenance procedures, foresee potential problems, and take corrective action.

There are two types of O&SHA, i.e., procedure analysis and contingency analysis. The procedure analysis is an evaluation of the adequacy of the various types of operating procedures. The contingency analysis is a study of operational situations that could develop into emergencies and ways to prevent these situations from happening. Each method can be applied equally well to all types of operation.

Most of the considerations in a procedure analysis O&SHA will generally review

1. The procedures by which the equipment will be used or could be misused
2. The consequences of material or procedural human failures
3. The means by which the consequences and failures can be minimized.

A contingency is considered to exist if a system is not in a normal operating state and conditions are such that an accident might occur unless corrective action is taken immediately. This definition assumes that

1. There is some corrective action that can be taken.
2. There is time to take corrective action before an accident occurs.

The contingency analysis should be conducted for any materiel that could

become involved in an accident. Even minor items might be improved through small design changes suggested by a contingency analysis. In addition to equipment redesign, the contingency analysis may also suggest changes to the operating procedures and the development of emergency procedures.

3-11 SAFETY CONSIDERATIONS IN NEW TECHNOLOGY

New technologies present unique system safety challenges because by their very nature little experience in their use has been collected and analyzed. The historical database is therefore lacking in determining safety aspects of new technologies. This fact highlights the need for thorough analysis and testing of new technologies prior to their incorporation into systems.

As a first example, consider the situation of a new composite material used in an air vehicle. The curing process might result in the release of hazardous materials during the manufacturing process, during normal use, in the course of maintaining or repairing the material, or during a postcrash fire. A subsystem hazard analysis would identify the new material as presenting such a potential hazard and would lead to the development of corrective actions to minimize the hazard.

As another example, consider a software programmable bus network controller that allows the transfer of data between electronic subsystems on an air vehicle. A latent “bug” in the control software might cause the loss or delay of critical information needed by another subsystem. An SHA would identify the bus network as a critical interface between subsystems and would underscore the need for thorough analysis and

evaluation of the proper functioning of the bus software.

Finally, consider an artificial intelligence (AI) or expert system onboard an air vehicle. The system processes threat information from various sensors and provides the pilot with recommended course information to navigate safely among the threat systems. Erroneous advice from such a system due to unforeseen contingencies could have disastrous effects. A properly conducted O&SHA would provide the mechanism for formally assessing contingencies, analyzing their impact on the system, and providing recommendations for corrective actions.

Software system safety deals with developing safety requirements for the system and the software within the system, ensuring accurate translation of safety specification requirements into the design and code of the software, identifying software that controls or influences safety-critical hardware functions, ensuring that the actual coded software does not cause identified or unidentified hazardous functions to occur or inhibit desired functions, and ensuring safety design requirements are thoroughly tested. The requirements for software system safety are delineated in MIL-STD-882. Procedures for conducting safety analyses of software are described in MIL-HDBK-764.

3-12 SAFETY TESTS

Safety tests should be incorporated into appropriate test plans. When approved by the procuring activity, partial verification of safety characteristics or procedures may be demonstrated by laboratory test, functional mock-ups, or model simulation. The detailed test plans for all tests should be reviewed to ensure that

1. Safety, as defined in the requirements documents, is demonstrated adequately.

2. The testing will be carried out in a safe manner.

3. All additional hazards introduced by testing procedures, instrumentation, test hardware, etc., are properly identified and minimized.

3-13 FLIGHT SAFETY PARTS (FSP) PROGRAM

The Flight Safety Parts (FSP) Program is intended to provide enhanced life cycle management and control of parts critical to the safe operation of air vehicles. The governing document for flight safety parts policy is US Army Aviation Systems Command (AVSCOM) Regulation 702-7, *Flight Safety Parts Program Management*, (Ref. 5).

The process of identifying and controlling FSPs should be a total life cycle activity. Because an FSP program generally remains critical throughout its life cycle, a program should be established to address identification and control of FSPs from development through procurement, production, and final disposition. The procuring activity (PA) should establish a program for FSPs. The PA should require that the air vehicle and engine contractors include management and control of FSPs as part of their overall program plan.

In general, the process of identification of FSPs should be based primarily on engineering judgment. Also past experience on similar systems and hazard analyses should play a vital role in the process. The intent is to identify each item that might create a critical condition in terms of safety or loss of the end-item if the part breaks, malfunctions, or is missing during use. Once an item

is designated as an FSP, the appropriate engineering drawings should be updated to identify all critical characteristics. FSPs should also be identified in all overhaul, repair, and maintenance publications.

A critical characteristic is any feature throughout the life cycle of an FSP, such as dimension, tolerance, finish, material or assembly, manufacturing or inspection process, operation, field maintenance, or depot overhaul requirement that if nonconforming, missing, or degraded, could cause the failure or malfunction of the FSP. Critical characteristics determined during the manufacturing process are termed "manufacturing-critical" characteristics. Critical characteristics that are not introduced during the manufacture of a part but are critical in terms of assembly and installation, e.g., proper torque, are termed "installation-critical" characteristics.

One of the most important aspects of the FSP program should be the control of critical characteristics. Control means those actions and techniques that receive special consideration and attention to detail, e.g., manufacturing and assembly procedures, frozen planning, certification of special processes, intensified inspection and verification procedures, recordkeeping and maintenance, traceability audits, vendor control, and nonconformance control. Once a part has been identified as an FSP, there are several key elements that should be used for its control:

1. All critical characteristics should be identified by the designers. Technical drawings and data packages (if any) should be updated to show the FSP and highlight its critical characteristics.

2. The planning documents by which the part is manufactured and

quality inspected should be approved by a "high-level" interdisciplinary board to ensure proper controls are in place to maintain the critical characteristics. Once approved, the procedures should be "frozen" and should not be changed, varied, or waived. Only a formal change, again approved by the board, should constitute any change in procedure.

3. All critical characteristics of the FSP that can be nondestructively inspected and tested should receive 100% inspection by qualified inspectors for every part manufactured. Parts having critical characteristics that require destructive testing, i.e., strength of material, heat treatment, etc., should be tested on the basis of statistical samples taken from every lot and every batch. A sample should be tested from every lot and batch without exception.

4. Manuals, including depot maintenance work requirements (DMWRs) should be revised as needed to include the critical characteristics. No repair or overhaul action should be permitted to deviate from the drawing specification for the critical characteristics. These documents are typically prepared by a contractor and submitted for Government approval.

Acceptance of parts that do not conform to the specified critical characteristics should not be authorized through actions of the Materiel Review Board. If possible, parts may be reworked to satisfy the specifications, or requirements, given on the drawing. Requests for waivers of and deviations from critical characteristics should be classified as major or critical and should be submitted for Government approval on a case-by-case basis. Any change of the critical characteristics usually requires reexamination of the product,

retest, or engineering analysis of the part and process before it is considered.

A description of the procedures to identify, qualify, maintain records, monitor, and dispose of FSPs may be found in the subparagraphs that follow.

3-13.1 IDENTIFICATION OF FLIGHT SAFETY PARTS

The process of identifying candidate flight safety parts should be primarily one of risk management involving engineering judgment and experience. This process should include review of drawings, materials, loads, flight spectrum, fatigue analyses, reliability analyses, form, fit, and function, installation requirements, and failure data. The criteria that follow should be used to identify flight safety-critical aircraft parts:

1. *Airframe*. Any part whose failure or malfunction affects the safe operation of an air vehicle is a candidate for an FSP. Final selection of an FSP should be considered if Item a and any other of Items b through e are affirmative:

a. Primary failure or malfunction affects the safe operation of the air vehicle.

b. A part has a predicted or demonstrated finite life.

c. A 10% reduction in laboratory working strength would result in an unlimited life becoming a finite life.

d. Loss of function could occur because of improper assembly or installation.

e. Fabrication of the part involves a manufacturing process that, if performed improperly, has a high probability of changing material properties significantly, i.e., degrading the strength of the part.

2. *Engine*. An FSP for engine-type parts is defined as any part, assem-

bly, or installation containing a critical characteristic whose failure, malfunction, or absence could cause an undirected engine shutdown or a catastrophic engine failure resulting in loss or serious damage to an air vehicle or serious injury or death to the occupants. Engine FSP identification should be based on assessment of potential associated risk using hazard severity and probability of occurrence as discussed in MIL-STD-882, *System Safety Program Requirement*, (Ref. 1).

3-13.2 FLIGHT SAFETY PARTS QUALIFICATION

To assure continuous availability of the product, FSP vendors should be qualified in advance of procurement actions. Vendor qualification provides a means for early completion of long, complex, or expensive tests, such as fatigue and flight tests, some of which would otherwise be required after each award and without any insurance that the vendor's parts would be acceptable. Typically, a Qualified Product List (QPL) is used to record all qualified vendors from whom FSPs can be procured. Vendors should qualify by meeting the test requirements, such as fatigue, interchangeability, and endurance, for each FSP. The requirements of establishing a QPL, testing, etc., are discussed in DoD 4120.3-M, *Defense Standardization Program Policies and Procedures*, (Ref. 6). Qualification of FSP vendors should include but not necessarily be limited to the demonstration of FSP critical characteristics. Engine FSP vendors might not be required to demonstrate full-life limits due to cost and other constraints. Engine endurance testing and low cycle fatigue testing plus spin-pit testing could be used to demonstrate a portion of part life in lieu of

demonstrating the full life. Also an increased level of quality assurance should be required for all FSPs even if previously qualified. See par. 3-13 for 100% inspection requirements, waivers, and deviations.

3-13.3 FLIGHT SAFETY PARTS RECORDS

All flight safety parts should be given a serial number whenever possible. Otherwise, lot or bag and tag procedures should be substituted. All manufacturing or inspection process control requirements relating to the flight safety part should be traceable to the time and location of production. Records should provide the traceability required to enable after-the-fact verification of all aspects of material, manufacture, special processing, assembly, and inspection of critical characteristics. These special records allow the rapid recall of fielded suspect flight safety parts if a deficiency in manufacturing or processing is encountered. Typically, these records are required to be kept by the manufacturer or delivered to the Government for retention until the last part in the record is removed from service.

3-13.4 FLIGHT SAFETY PARTS SURVEILLANCE

The FSPs Surveillance Program should include a formal process for sampling all FSPs on a recurring basis. The surveillance effort should use data obtained from the FSP Program for the following purposes:

1. To confirm the validity of requirements used during the initial design and qualification of FSPs
2. To monitor the effects of use on parts to demonstrate that replacement

and overhaul intervals are adequate and safe relative to actual use

3. To assess new parts continually to ensure minor design and manufacturing changes do not affect FSPs in a detrimental manner

4. To confirm degraded mode limits or effects due to wear, corrosion, fretting, and damage

5. To ensure that repair procedures do not degrade the critical characteristics

6. To determine the impact on FSPs of any previously unknown or known degraded conditions

7. To ensure that processes are adequate to control time-related internal procedures of previously approved vendors (if any) and that new vendors are not impacting the integrity of the FSPs

8. To ensure that undefined changes in rotorcraft usage, new environments, or long-term effects do not impact the integrity of FSPs.

3-13.5 FLIGHT SAFETY PARTS DISPOSITION

Flight safety parts that have been removed from service because they fail inspection criteria, fail in service, or whose life limit has been reached should be destroyed to preclude the inadvertent reinstallation of the part or its remanufacture. This extra effort is necessary because the reuse of such parts could lead to failures resulting in unsafe operation of the air vehicle. Air vehicle development programs should have a disposition clause to control flight safety parts and prevent installation of nonconforming FSPs on production units .

REFERENCES

1. MIL-STD-882C, *System Safety Program Requirement*, 19 January 1993.
2. MIL-HDBK-764(MI), *System Safety Engineering Design Guide for Army Materiel*, 12 January 1990.
3. AR 385-16, *System Safety Engineering and Management*, 3 May 1990.
4. AMC Supplement to AR 385-16, *System Safety Engineering and Management*, US Army Materiel Command, Alexandria, VA, 23 March 1992.
5. AVSCOM Regulation 702-7, *Flight Safety Parts Program Management*, US Army Aviation Systems Command, St. Louis, MO, 13 August 1990.
6. DoD 4120.3-M, *Defense Standardization Program Policies and Procedures*, July 1993.