"designing the safest possible systems consistent with mission requirements and cost effectiveness"

Air Force System Safety Handbook

Air Force Safety Agency
Kirtland AFB NM 87117-5670

Revised July 2000

FOREWORD

Purpose. ***The Air Force System Safety Handbook*** was prepared as a resource document for program office SYSTEM SAFETY MANAGERS AND SYSTEM SAFETY ENGINEERS. It is not designed to answer every question on the topic of system safety nor is it a cookbook that guarantees success. The handbook provides considerable insight to the general principles, objectives, and requirements of applying system safety concepts to the Air Force system acquisition and logistical support processes.

Programs vary greatly in their scope and complexity, requiring a tailored system safety effort. Assigned to this difficult task are military and government personnel with varied education and experience backgrounds. These system safety practitioners need a comprehensive understanding of the system safety process and the complexities of applying it to a given program. This handbook will assist in providing much of the necessary information but additional, more detailed guidance will be required from the program office and their higher headquarters system safety experts.

This handbook is published by AFSC. Lt Col James E. LaMarca (formerly from HQ AFSA/SESD) developed and edited this handbook, first published in Sep 91. The handbook was recently revised to incorporate the provisions of the DoD Acquisition reform program and the new MIL-STD-882D. Reference material and suggested text inputs will be greatly appreciated. Send your comments and materials to:

AF System Safety Handbook
HQ AFSC/SEPP
Kirtland AFB, NM 87117-5670

Sources. ***The Air Force System Safety Handbook*** has drawn information from many Army, Navy, and Air Force sources and selected articles by system safety professionals. Especially helpful in the preparation of this handbook were:

MIL-STD-882D, DoD Standard practice for *System Safety*
AFISC's *Introduction to System Safety for Managers*
AFSCP 127-1, *System Safety Program Management*
ASDP 127-1, *System Safety Management*
SDP 127-1, *System Safety Handbook for the Acquisition Manager*
Navy Program Manager's Guide for System Safety
Army's *DoD System Safety*
Army's DA PAM 385-16, *System Safety Management Guide*

MIL-STD-882. The handbook generally uses a generic reference of "MIL-STD-882D" without a letter postscript.

Acknowledgments. Special appreciation is extended to Mr. Chuck Dorney (AFMC/SES) for his significant contributions.

Air Force System Safety Handbook

TABLE OF CONTENTS

FIGURES

ABBREVIATIONS

ACAT	Acquistion Category
ACO	Administrative Contracting Officer
AE	Architecture and Engineering
AHMH	Acquisition Management of Haz Materials
ALC	Air Logistics Center
AFMC	Air Force Materiel Command
AFOSH	Air Force Occupational Safety & Health
AFSC	Air Force Safety Center
AFOTEC	Air Force Test & Evaluation Center
ANSI	American National Standards Institute
CCB	Configuration Control Board
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CI	Configuration Item
CLA	Code Level Analysis
CSHA	Combined Software Hazard Analysis
COTS	Commercial Off The Shelf
CPCI	Computer Program Configuration Item
CSSM	Center System Safety Manager
DID	Data Item Description
DOT	Department of Transportation
DT&E	Development Test and Evaluation
ECP	Engineering Change Proposal
EED	Electro-Explosive device
EMD	Engineering and Manufacturing Development
EOD	Explosive Ordnance Disposal
EPA	Environmental Protection Agency
FAR	Federal Acquisition Regulation
FCA	Final Configuration Audit
FHA	Fault Hazard Analysis
FMEA	Failure Mode and Effect Analysis
FMECA	Failure Mode and Effect Criticality Analysis
FOT&E	Follow-on Operational Test and Evaluation
FSD	Full-Scale Development
FTA	Fault Tree Analysis
GFE	Government Furnished Equipment
GFP	Government-Furnished Property
HRI	Hazard Risk Index
IFB	Invitation for Bid
ILS	Integrated Logistics Support
IOT&E	Initial Operational Test and Evaluation
ISSPP	Integrated System Safety Program Plan
MA	Management Activity
MSDS	Material Specifications Data Sheet
NDI	Nondevelopmental Item
NNMSB	Nonnuclear Munitions Safety Board
NRC	Nuclear Regulatory Commission
NWSSG	Nuclear Weapons System Safety Group
O&SHA	Operating and Support Hazard Analysis
OSHA	Occupational Safety and Health Administration
OT&E	Operational Test and Evaluation
PC	Product Center
PCA	Preliminary Configuration Audit
PCO	Principle Contracting Officer
PD	Product Division (now Product Center)
PDR	Preliminary Design Review
PEO	Program Executive Officer
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PM	Program Manager
PMD	Program Management Document
PMP	Program Management Plan
PO	Program Office
QD	Quantity-Distance
RDT&E	Research, Development, Test, and Evaluation
RFP	Request for Proposal
RFQ	Request for Quotation
RHA	Requirements Hazard Analysis
RHI	Real Hazard Index
RSP	Render Safe Procedures
RTO	Responsible Testing Organization
SAR	Safety Assessment Report
SAS	Safety Analysis Summary
SCA	Sneak Circuit Analysis
SCCSC	Safety Critical Computer Software Component
SCCSU	Safety Critical Computer Software Unit
SCF	Software Critical Function
SCN	Software Change Notice
SDHA	Software Design Hazard Analysis
SHA	System Hazard Analysis
SON	Statement of Need
SOW	Statement of Work
SPO	System Program Office
SSE	System Safety Engineer
SSG	System Safety Group
SSHA	Subsystem Hazard Analysis
SSM	System Safety Manager
SSMP	System Safety Management Plan
SSPP	System Safety Program Plan
SSWG	System Safety Working Group
TEMP	Test Evaluation Master Plan
TNSE	Technical Nuclear Safety Evaluation
TNSA	Technical Nuclear Safety Analysis
TO	Technical Order
USACE	US Army Corps of Engineers
WBS	Work Breakdown Structure

DEFINITIONS
(30:2-4)

Acceptable Risk. That part of identified risk which is allowed by the managing activity to persist without further engineering or management action.

Boilerplate. System safety contract requirements derived by copying requirements from previously written contracts without regard to their validity; i.e., using a "standard" list of requirements.

* 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 (e.g., 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, etc.

* 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.

Cut-Up Tailoring. Disjointed, fragmented system safety requirements that result when deleting, without SSM 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 (example: Fault Tree Analysis).

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 which will not cause a mishap.

* 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. A material that due to its chemical, physical, or biological nature causes safety, public health, or environmental concerns that elevate efforts to manage.

Identified Risk. That risk which has been determined through various analysis techniques.

Inductive Analysis. An analysis that reasons from the specific to the general to determine WHAT failed states or other outcomes are possible given certain conditions (example: FMEA).

Internal Interface. Information exchange between various members of the system program office.

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: (1) designated by the USD (A&T) as an MDAP, or (2) estimated by the Under Secretary of Defense (USD) for Acquisition and Technologies (A&T) to require an eventual total expenditure for research, development, test and evaluation of more than 355 million in FY 1996 constant dollars or, for procurement, of more than 2.135 billion in FY 1996 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.

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

Mishap 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.

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

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

Nondevelopmental Items. Items that have already been developed and used by any government agency, including armed forces.

Program Manager (PM). A government official who is responsible for managing an acquisition program. Also, a general term of reference to those organizations directed by individual managers, exercising authority over the planning, direction, and control of tasks and associated functions essential for support of designated systems. This term will normally be used in lieu of any other titles, e.g.; system support manager, weapon program manager, system manager, and project manager.

Qualitative. Relative evaluation methodology using nonmathematical processes.

Quantitative. Evaluations based on numerical values and mathematical calculations.

Residual Risk. The risk left over after system safety efforts have been fully employed. It is sometimes erroneously thought of as being the same as acceptable risk. Residual risk is actually the sum of acceptable risk and unidentified risk. This is the total risk passed on to the user.

* Risk Assessment. A comprehensive evaluation of the risk and its associated impact.

* 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 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; e.g., safety-critical function, safety-critical path, safety-critical component.

Smorgasbord. System safety requirements derived by including all parts of MIL-STD-882 without regard for a justified need for each.

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

* 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 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 system safety engineering 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 Group/Working Group. A formally chartered group of persons, representing organizations associated with the system acquisition program, organized to assist the MA system program manager 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 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 system safety engineering implemented by acquisition project managers.

* System Safety Program 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.

Technique. For analyses, refers to a specific method for analysis using specific engineering expertise (examples: Fault Tree, FMEA).

Total Risk. The sum of identified and unidentified risks.

Type of Analysis. Refers to the nature or purpose of the analysis, such as preliminary, subsystem, or system.

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 hasn't been determined. It's real. It's important. But it's not measurable. Some unidentified risk is subsequently determined when a mishap occurs. Some risk is never known.

REFERENCES

Articles/Papers

1. Clemens, P. L., "A Compendium of Hazard Identification and Evaluation Techniques for System Safety Application," Hazard Prevention, Mar/Apr 82
2. Clemens, P. L., "Readings in Fault Tree Analysis," Hazard Prevention, 1 Qtr 1990
3. Clemens, P. L., "Readings in Human Factors," Hazard Prevention, 4 Qtr 1989
4. Clemens, P. L., "Readings in Risk Analysis," Hazard Prevention, 1 Qtr 1990
5. Clemens, P. L., "Readings in System Safety," Hazard Prevention, 4 Qtr 1989
6. Frola, F. R. and C. O. Miller, "System Safety in Aircraft Acquisition," Logistics Management Institute, Washington DC, Jan 84
7. Forscher, F., "Understanding Risks," Hazard Prevention, Jul/Aug 86
8. Hill, E. J. and L. J. Bose, "Sneak Circuit Analysis of Military Systems," 2d ISSC, Jul 75
9. Hocevar, C. J. and C. M. Orr, "Hazard Analysis by the Energy Trace Method," 9th ISSC, Jul 89
10. Hulet, M. W., "System Safety Interfaces," Hazard Prevention, Jan/Mar 89.
11. Lorge, B. A., "Incorporating System Safety into Facility Design and Construction," 7th ISSC, Jul 85
12. McFarland, M. C., "Analysis of the Social Responsibilities of Engineers," IEEE Technology and Society, Magazine, Dec 86
13. Merz, H. A., "Who is Afraid of Risk Criteria?," Hazard Prevention, Nov/Dec 86
14. Miller, C. O., "The Role of System Safety in Aerospace Management," USC, Los Angeles CA, Aug 66
15. Pittenger, D. A. and M. G. Vogt, "Tailoring System Safety to Facility Acquisition," 9th ISSC, Jul 89
16. Rands, A. M., "A Realistic Approach to Tailoring MIL-STD-882," 9th ISSC, Jul 89
17. Ruff, G. F. and G. P. Haviland, "Early USAF Efforts to Develop System Safety," System Safety Symposium, Boeing Co./Univ of Washington, Seattle WA, Jun 65
18. Sweginnis, R. W., "Real Hazard Index - A System Safety Management Tool," 6th ISSC, Sep 83

Regulations

19. DODD 5000.1, Defense Acquisition, Feb 91
20. DODD 5000.1, Major System Acquisitions, Mar 86
21. DODD 500.1, Defense Acquistion, Mar 96
22. DOD 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAP) and Major Automated Information Systems (MAIS), Mar 98
23. DODI 5000.2, Major Systems Acquisition Policy and Procedures, Feb 91
24. DODI 5000.2, Major Systems Acquisition Procedures, Mar 86
25. DODI 5000.36, System Safety Engineering and Management, Apr 86
26. AFR 127-2, USAF Safety Program, Mar 87.
27. AFR 127-4, USAF Mishap Investigation and Reporting, Jan 90
28. AFR 800-16, USAF System Safety Programs, Aug 87
29. AFSCP 127-1, System Safety Program Management, Feb 87
30. ASDP 127-1, System Safety Management, Mar 85
31. MIL-STD-882B, System Safety Program Requirements, Jul 87 (Notice 1)
32. MIL-STD-882C, System Safety Program Requirements, Jan 96 (Notice 1)
33. MIL-STD-882D, DOD Standard Practice for System Safety, draft, Sep 99
34. MIL-STD-1574, System Safety Program for Space/Missile Systems, Aug 79
35. DA PAM 385-16, System Safety Management Guide, Sep 87
36. AFI 91-202, USAF Mishap Prevention Program, Aug 98
37. AFI 91-204, Investigation and Reporting of USAF Mishaps, Feb 98
38. AFI 21-101, Maintenance Management of Aircraft, Oct 98

Handbooks

39. DOD System Safety, US Army, 1990
40. Introduction to Acquisition Management, AFIT, Jul 89
41. Introduction to System Safety for Managers, AFISC, Aug 88
42. Navy Program Manager's Guide for System Safety, May 88
43. System Safety Handbook for the Acquisition Manager, SDP 127-1, Jan 87
44. System safety Design Handbook, DH 1-6, Apr 90
45. AFMCP 91-2, System Safety Groups, Jan 98

Books

46. Hammer, W., Occupational Safety Management and Engineering, Prentice-Hall, 1981
47. Rogers, W. P., Introduction to System Safety Engineering, Wiley, 1971
48. Roland, H. E. and B. Moriarty, System Safety Engineering and Management, Wiley, 1983

Other

49. USAF System Safety Study, AFISC, Jan 91
50. USAF Mishap Bulletin FY89, AFISC
51. AFISC Study, "Off-the-Shelf Aircraft Acquisitions," Apr 85
52. Clewell, Harvey, "Integrated Weapons System Management of Hazardous Materials,"
53. 10th International System Safety Society Conference, Jul 90
54. "Acquisition Management of Hazardous Materials", MITRE Working Paper, Apr 1991
55. DoD Deskbook Acquisition Tool, www.deskbook.osd.mil

CHAPTER 1

INTRODUCTION TO SYSTEM SAFETY

1.1 Definitions: System Safety and Safety System.

To employ the concepts of system safety, it is necessary to understand what system safety is and what system safety strives to do.

The ultimate objective of any organization within the Air Force is maximizing combat capability. One element in this maximizing process is protecting and conserving combat weapon systems and their support equipment. Preventing mishaps and reducing system losses is one important aspect of conserving these resources. System safety contributes to mishap prevention by minimizing system risks due to hazards consistent with other cost, schedule, and design requirements. The fundamental objective of system safety is to identify, eliminate or control, and document system hazards. This hierarchy of goals, illustrated in Figure 1-1, is the crucial framework for defining system safety. (41:15)

Figure 1-1

System Safety Goals

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. 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.

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. (30:3)

Some clarifications are needed with these definitions. Absolute safety is not possible because complete freedom from all hazardous conditions is not possible. Therefore, safety is a relative term that implies a level of risk that is both perceived and accepted. You will also note that "system" is also a relative term. A subsystem is a system itself with predetermined boundaries. System safety is not an absolute quantity either. System safety is an optimized level of risk that is constrained by cost, time, and operational effectiveness (performance). System safety requires that risk be evaluated and the level of risk accepted or rejected by an authority. This is the basic origin of system safety's requirement for both engineering and management functions. Finally, system safety is a discipline employed from the initial design steps through system demilitarization or disposal (a.k.a. "cradle to grave or "womb to tomb").

1.2 System Safety Objectives.

A safe system is achieved through the implementation and careful execution of a system safety program. As stated previously, the ultimate objective of system safety is MAXIMIZED COMBAT CAPABILITY. The objectives of a system safety program are to ensure: (30:2)

a. Safety, consistent with mission requirements is designed into the system in a timely, cost-effective manner.

b. Hazards are identified, evaluated, and eliminated, or the associated risk reduced to a level acceptable to the managing activity (MA) throughout the entire life cycle of a system.

c. Historical safety data, including lessons learned from other systems, are considered and used.

d. Minimum risk is sought in accepting and using new designs, materials, and production and test techniques.

e. Actions taken to eliminate hazards or reduce risk to a level acceptable to the MA are documented.

f. Retrofit actions are minimized.

g. Changes in design, configuration, or mission requirements are accomplished in a manner that maintains a risk level acceptable to the MA.

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

i. Significant safety data are documented as "lessons learned" and are submitted to data banks, design handbooks, or specifications.

j. Hazards identified after production are minimized consistent with program restraints.

1.3 Need for System Safety.

Why is system safety needed? The most obvious answer is it's too expensive not to have a system safety program. In the mid-1950s, Air Force aircraft mishap rates were over 10 per 100,000 flight hours and annual losses were around $100 million. Mishap rates in the late 1980s were drastically reduced to less than 2 per 100,000 flight hours, but the cost of the annual losses was rapidly approaching a billion dollars (Figure 1-2). The number of design failures is hard to determine. Approximately one-third were due to logistics

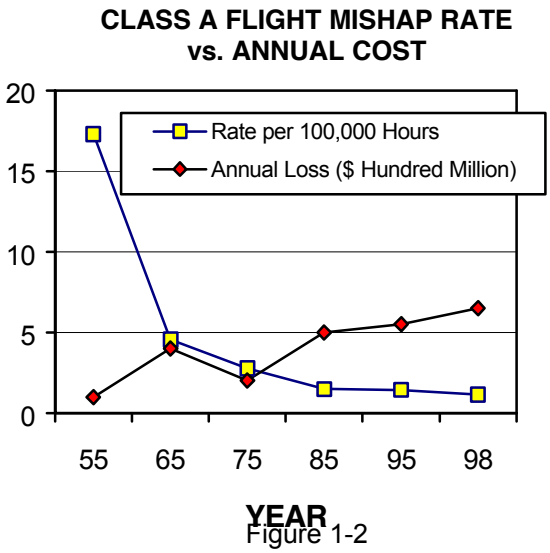


Figure 1-2

factors, but only a portion of the logistics factors were actually a design problem. Of the two-thirds that were caused by operations factors, some human factors design issues were also a problem. (42:1-2)

There is also an associated loss of combat capability. The approximately 50 aircraft lost in 1989 represent assets of an entire fighter wing. Considering the relatively small size of the B-1 or B-2 fleets, one aircraft loss represents a real loss in combat capability. With fewer new weapons programs being initiated and the cost of these new systems increasing significantly, any loss or major damage may very well threaten the continuation of the weapons program.

System safety programs are also a response to ethical demands made by society on industry in general. Engineers have a special responsibility in this social context. The engineers are involved with high-energy sources, hazardous materials, and new technologies that offer both tremendous benefits to society and the potential for catastrophic accidents. They have a special proximity to design problems. Their potential contribution is unique and irreplaceable. Because of their special training and their involvement in the design, they are best qualified to clarify the technical issues. They can define the risks involved and give the best available estimates of the costs of reducing or eliminating those risks. They are the first to see and to evaluate the dangers and risks of the technology. They work with and evaluate the systems while they are still in the design stage and are in a position to recognize potential dangers while something can still be done about them. Finally, engineers can propose and explore alternatives to the current technology that might avoid some problems altogether. (12:2-3)

Although engineers are usually strong influences in risk assessment decisions, there are other forces at play. Engineering professional societies, organized public advocacy groups, and political groups make their own demands on engineers to address technical and ethical safety issues. Public law, military regulations, standards, and specifications also address safety concerns. Corporate policy and actions have tremendous influence in safety issues as profits, continued contract awards, and corporate image are at stake. (12:3-6)

Besides the cost of mishaps and ethical considerations, there is also a need to reduce the cost of modifications that result from design shortfalls. It is difficult to identify precisely the cost of safety modifications. Using available data, it is conservatively estimated that at least $110 million was spent on 66 safety changes for the F-14 from 1973 to 1982. For the F-15, only the engineering change proposal costs were readily available. Those amounted to approximately $40 million for 35 safety modifications. Despite the difficulty in obtaining accurate safety modification cost data, safety modifications appear to add at least 15-20 percent to the reported costs of accidents. They, like the accidents themselves, represent quite a cost-saving target for system safety. (33:1-3)

1.4 System Safety Costs. (6:1-4 to 1-6)

How much does a system safety program cost? The implication of that question is whether system safety is worth the expense. Costs of system safety programs are quite small in proportion to contract costs. The contractor part of the F-14 system safety program was only about $5 million for 10 years (less than one-third of the cost of an airplane today). A really large program (e.g., B-1B) might have 30-40 government and contractor people involved at a peak period. Most programs need only one or two system safety personnel in the government program office and four or five at the peak of the contractor's effort. One person can monitor several subsystem programs simultaneously. Clearly, the saving of just one aircraft by a system safety program pays for that program many times over.

A specific assessment of system safety payoff is difficult at best. One can hardly "measure" something that does not happen such as an accident that has been prevented. Approaches other than absolute measurement can be significant as long as a reasonableness test is applied. Data concerning material failures accidents could be compared on a relative basis. Through 1981, the F-4 and F-14 aircraft had somewhat similar missions in the Navy. The F-4 did not have a formal system safety program, but the F-14 airframe did. Cumulative material failure accidents for the F-4 occurred at a rate of 9.52/100,000 hours. The comparable F-14 rate was 5.77/100,000 hours. These data do not "prove" the merit of a system safety program, however. Other factors such as differences in the state of the art applied in each program, different operational environments, design environments, and different contractors probably contributed to the difference between the F-4 and F-14 accident rates.

Another way of assessing the payoff of system safety is to examine case histories. Examples abound where system safety personnel identified hazards, which were corrected before accidents occurred. Some examples are:

- During the design of the F-18, fire hazard was minimized when a system safety engineer convinced program decision makers that a proposed increase in allowable bleed air duct temperature was dangerous and that a similar hazard could be avoided by ensuring that the bleed air shutoff valve closed when power was removed.

- During a modification to the B-52, a system safety engineer noted that if the front lugs of the air launched cruise missile attachment retracted but the rear ones did not, parts of the pylon would tear from the wing and, together

with the missile, would inflict severe structural damage to the wing and possibly the horizontal stabilizer.

- A safety engineer found in the PAVE LOW helicopter system that loss of voltage in a radar circuit would cause a command to the aircraft to fly at zero altitude with no warning to the pilot. He also checked with personnel on the RF-4C and A-7D programs, knowing they used the same system. All aircraft were quickly prohibited from flying certain low-level missions until the systems were corrected.

Investments in system safety pay off. The cost of system safety is not large compared to overall program costs or compared to a weapon system's cost. Preventing the loss of one aircraft could pay for system safety for the entire development effort of that system. Waiting for mishaps to point out design problems is not economically, politically, and ethically feasible. "Fly-fix-fly" has been replaced with identify-analyze-control. (Figure 1-4)

1.5 Development of System Safety.

System safety as we know it today began as a grass roots movement that was introduced in the 40s, gained momentum during the 50s, became established in the 60s, and formalized its place in the acquisition process in the 70s. The system safety concept was not the brain child of one man but rather a call from the engineering and safety community to design and build safer equipment by applying lessons learned from our accident investigations. It was an outgrowth of the general dissatisfaction with the fly-fix-fly approach to systems design.

The first formal presentation of system safety was by Amos L. Wood at the Fourteenth Annual Meeting of the Institute of Aeronautical Sciences (IAS) in New York in January 1946. Titled "The Organization of an Aircraft Manufacturer's Air Safety Program," Wood emphasized "continuous focus of safety in design," "advance and post-accident analysis," "safety education," "accident preventive design minimize personnel errors," "statistical control of post-accident analysis." (14:18)

Wood's paper was referenced in another landmark paper by William I. Stieglitz entitled "Engineering for Safety," presented in September 1946 at a special meeting of the IAS and finally printed in the IAS Aeronautical Engineering Review in February 1948. Mr. Stieglitz' farsighted views on system safety are evidenced by a few quotations from his paper:

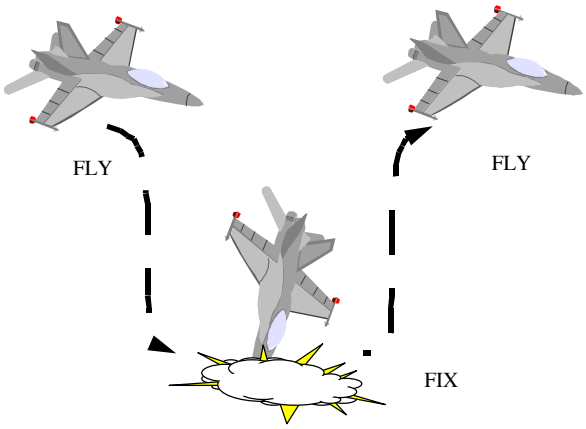
"Safety must be designed and built into airplanes, just as are performance, stability, and structural integrity. A safety group must be just as important a part of a manufacturer's organization as a stress, aerodynamics, or a weights group...."

"Safety is a specialized subject just as are aerodynamics and structures. Every engineer cannot be expected to be thoroughly familiar with all developments in the field of safety any more than he can be expected to be an expert aerodynamicist."

"The evaluation of safety work in positive terms is extremely difficult. When an accident does not occur, it is impossible to prove that some particular design feature prevented it." (14:18-19)

The Air Force was an early leader in the development of system safety. In 1950, the USAF Directorate of Flight Safety Research (DFSR) was formed at Norton AFB, California. It was followed by safety centers for the Navy in 1955 and Army in 1957. The DFSR began in 1954 sponsoring Air Force-industry conferences to address safety issues of various aircraft subsystems by technical and safety specialists. In 1958, the first quantitative system safety analysis effort was undertaken with the Dyna-Soar X-20 manned space glider. This significant approach to hazard prevention was required because of the unique emergency, rescue, and survival problems of the X-20. (14:21-22)

Figure 1-3
The Fly-Fix-Fly Approach to Safety



In July 1960, a system safety office was established at the USAF Ballistic Missile Division (BMD) at Inglewood, California. BMD facilitated both the pace and direction of system safety efforts when it published in April 1960 the first system-wide safety specification titled BSD Exhibit 62-41, "System Safety Engineering: Military Specification for the Development of Air Force Ballistic Missiles." The Naval Aviation Safety Center was among the first to become active in promoting an interservice system safety specification for aircraft, using BSD Exhibit 62-41 as a model. (17:4-6) In the fall of 1962, the Minuteman program director, in another system safety first, identified system safety as a contract deliverable item in accordance with BSD Exhibit 6282. (39:11)

The early 1960s saw many new developments in system safety. In 1963, the Aerospace System Society was formed in the Los Angeles area. The University of Southern California's Aerospace Safety Division began in 1964 a master's degree program in Aerospace Operations Management from which specific system safety graduate courses were developed. In 1965, the University of Washington initiated a short course in system safety analysis. (14:22-23) System safety had become institutionalized.

1.6 Evolution of System Safety Principles. (41:3-7)

MIL-STD-882 is the primary reference for system safety program information for Department of Defense weapon systems. Its evolution from BSD Exhibit 62-41 documents the development of vital system safety principles.

By studying the early documents, basic concepts begin to emerge. These founding principles include:

a. Safety must be designed in. Critical reviews of the system design identify hazards that can be controlled by modifying the design. Modifications are most readily accepted during the early stages of design, development, and test. Previous design deficiencies can be exploited to prevent their recurrence.

b. Inherent safety requires both engineering and management techniques to control the hazards of a system. A safety program must be planned and implemented such that safety analyses are

integrated with other factors that impact management decisions. Management activity must effectively control analytical and management techniques used to evaluate the system.

c. Safety requirements must be consistent with other program or design requirements. The evolution of a system design is a series of tradeoffs among competing disciplines to optimize relative contributions. Safety competes with other disciplines; it does not override them.

BSD Exhibit 62-41. First published in April 1962 and again in October 1962, BSD Exhibit 62-41 introduced all of the above principles but was narrow in scope. The document applied only to ballistic missile systems, and its procedures were limited to the conceptual and development phases "from initial design to and including installation or assembly and checkout." However, on the balance, BSD Exhibit 62-41 was very thorough. It defined requirements for systematic analysis and classification of hazards and the design safety preference: design to minimize the hazard, use of safety devices, use of warning devices, and use of special procedures. In addition to engineering requirements, BSD Exhibit 62-41 also identified the importance of management techniques to control the system safety effort. The use of a system safety engineering plan and the concept that managerial and technical procedures used by the contractor were subject to approval by the procuring authority were two key elements in defining these management techniques.

MIL-S-38130(A). In September 1963, the USAF released MIL-S-38130. The specification broadened the scope of our system safety effort to include "aeronautical, missile, space, and electronic systems." This increase of applicable systems and the concept's growth to a mil spec were important elements in the growth of system safety during this phase of evolution. Additionally, MIL-S-38130 refined the definitions of hazard analysis. These refinements included system safety analyses: system integration safety analyses, system failure mode analyses, and operational safety analyses. These analyses still resulted in the same classification of hazards but the procuring activity was given specific direction to address catastrophic and critical hazards.

MIL-S-38130 was ready for a revision in Jun 66. Revision A to the specification once again expanded the scope of the system safety program by adding a system modernization and retrofit phase to the conceptual phase definition. Additionally, this revision further refined the objectives of a system safety program by introducing the concept of "maximum safety consistent with operational requirements." On the engineering side, MIL-S-38130A also added another safety analysis: the Gross Hazard Study. This comprehensive qualitative hazard analysis was an attempt to focus attention on safety requirements early in the concept phase and was a break from other mathematical precedence. But changes weren't only limited to introducing new analyses. The scope of existing analyses was expanded as well. One example of this was the operating safety analyses which now included system transportation and logistics support requirements as well. The engineering changes in this revision weren't the only significant changes. Management considera-tions were highlighted by emphasizing management's responsibility to define the functional relationships and lines of authority required to "assure optimum safety and to preclude the degradation of inherent safety." This was the beginning of a clear focus on management control of the system safety program.

MIL-S-38130A served the USAF well, allowing the Minuteman program to continue to prove the worth of the system safety concept. (Ref 14) By August 1967, a triservice review of MIL-S-38130A began to propose a new standard that would clarify the existing specification as well as provide additional guidance to industry. By changing the specification to a standard, there would be increased program emphasis and

improved industry response to system safety program requirements. Some specific objectives of this rewrite were: obtain a system safety engineering plan early in the contract definition phase, and maintain a comprehensive hazard analysis throughout the system's life cycle.

MIL-STD-882(A)(B). In July 1969, a new standard was published, MIL-STD-882. This landmark document continued the emphasis on management and continued to expand the scope to apply to all military services in the DOD. The full life-cycle approach to system safety was also introduced. The expansion in scope required a reworking of the system safety requirements. The result was a phase-oriented program that tied safety program requirements to the various phases consistent with program development. This approach to program requirements was a marked contrast to earlier guidance, and the detail provided to the contractor was greatly expanded. Since MIL-STD-882 applied to even small programs, the concept of tailoring was introduced and allowed the procuring authority some latitude in relieving some of the burden of the increased number and scope of hazard analyses.

The basic version lasted until June 1977, with the release of MIL-STD-882A. The major contribution of MIL-STD-882A centered on the concept of risk acceptance as a criterion for system safety programs. This evolution required introduction of hazard probability and established categories for frequency of occurrence to accommodate the long-standing hazard severity categories. In addition to these engineering developments, the management side was also affected. The responsibilities of the managing activity became more specific as more emphasis was placed on contract definition.

The publishing of MIL-STD-882B in March 1984 was a major reorganization of the A version. Again, the evolution of detailed guidance in both engineering and management requirements was evident. The task of sorting through these requirements was becoming complex, and more discussion on tailoring and risk acceptance was expanded. More emphasis on facilities and off-the-shelf acquisition was added, and software was addressed in some detail for the first time. The addition of Notice 1 to MIL-STD-882B in July 1987 expanded software tasks and the scope of the treatment of software by system safety.

In January 1993, MIL-STD-882C was published. Its major change was to integrate the hardware and software system safety efforts. The individual software tasks were removed, so that a safety analysis would include identifying the hardware and software tasks together in a system. In January 1996, Notice 1 was published to correct some errors and to revise the Data Item Descriptions for more universal usage.

In the mid-1990s, the acquisition reform movement began along with the military specifications and standards reform (MSSR) movement. These two movements led to the creation of Standard Practice MIL-STD-882D in January 2000. Under acquisition reform, program managers will specify system performance requirements and leave up the specific design details up to the contractor. In addition, the use of military specifications and standards will be kept to a minimum. Only performance-oriented military documents are permitted. Other documents, such as commercial item descriptions and industry standards, are to be used for program details. MIL-STD-882 was considered to be important enough, that it was allowed to continue, as long as it was converted to a performance-oriented military standard. Until MIL-STD-882D was published, the DoD Standardization community continued to allow the use of MIL-STD-882C, but a

waiver was generally required for it to be specified by a military program manager. A contractor could freely use the standard without any waivers. Once MIL-STD-882D was published as a DoD Standard Practice in February 2000, its use did not require any waivers.

The evolution of the system safety program can best be summarized by a consistent increase of scope, coupled with an expanding number of system requirements. The principles defined earlier remained intact through this evolution, but the maturing of the system safety concept resulted in a very complicated system of engineering analyses, coupled with contractually defined management requirements. A complete summary of system safety principles, objectives, and requirements is presented in the following figures along with the initial source in which they were referenced.

Figure 1-4

SYSTEM SAFETY OBJECTIVES

OBJECTIVE	INITIAL REFERENCE
1. Prevent mishaps	6241
2. Define the safety requirements so the program manager can provide control and technical surveillance of system safety	6241
3. Identify and control hazards	6241
4. Avoid duplication of analyses efforts - Use data generated by design/other analyses	6241
5. Maximum safety consistent with requirement	38130A
5a. Principle objective of system safety - Ensure safety consistent with mission requirements is designed in	882A
6. Minimum personal injury, material failures, monetary losses	38130A
7. Minimum risk of new material	38130A
8. Hazards are identified, eliminated, or controlled	38130A
9. Retrofit actions reduced - Ensure that normal operation of subsystem cannot degrade the safety of another subsystem	38130A
10. Protect public	882
11. Conserve resources	882
12. Document actions to reduce risk	882B
13. Safety data documented as lessons learned	882B
14. Purpose of software hazard analysis - Ensure accurate translation of specs into CPCIs - CPCIs identify safety criteria used - Identify computer program inputs to safety critical functions - Analyze computer program for undesirable events relevant to safety - Ensure coded software not a hazard - Mitigate end item hazardous anomalies	882B
15. Combination of hardware and software system safety tasks - When analyzing a system or component, its hardware and software are considered together. (MIL-STD-882C)	
16. Acquisition Reform - Government specifies few details and leaves most of details to the contractor. In the system safety world, Government specifies that the contractor does a system safety effort to identify and control hazards. Contractor determines details and methods. (MIL-STD-882D)	

Figure 1-5

SYSTEM SAFETY PRINCIPLES

PRINCIPLE	INITIAL REFERENCE
1. System safety is a basic requirement of the total system	6241
2. Systems requiring safety management are: • AF ballistic missile systems (6241) • Aeronautical/missile/space/electronic systems (38130)	6241
3. System Safety must be planned • Integrated and comprehensive safety engineering effort • Interrelated, sequential, and continuing effort • Affects facilities, equipment, procedures and personnel • Applies to conceptual and acquisition (design/production/deployment) phases • Covers transportation and logistics support • Covers facilities and in-house programs • Applies to disposal and demilitarization processes	6241 “ “ “ “ 38130A 882 882A

• Covers off-the-shelf acquisitions	882A
4. Inherent safety comes from the basic system design	6241
• System safety is an inherent part of system's design	"
• Improvements to inherent safety are best achieved early	"
5. Program manager (SPO) provides management of system safety effort	6241
• Managerial and technical procedures to be used are submitted for procuring authority approval	"
• Resolves conflicts between safety and other design requirements	38130
6. Design safety preferences	6241
• Design to minimum hazard	"
• Safety devices	"
• Warning devices	"
• Special procedures	"
7. System safety requirements must be consistent with other program requirements	6241
• Design requirements can have priority over safety design	"
8. System analyses are basic tools for systematically developing design specifications	6241
• Ultimate measure of safety is not the scope of analysis but in satisfied safety requirements	"
• Analyses are performed to :	882
• Identify hazards and corrective actions	"
• Review safety considerations in tradeoffs	"
• Determine/evaluate safety design requirements	"
• Determine/evaluate operational, test, logistics requirements	"
• Validate qualitative/quantitative requirements have been met	"
• Analyses are hazard vs. safety analyses	

9. Nature and severity of hazards used to change design requirements	6241
• Called risk assessment (with categories and probability levels)	882A
• Hazard categories:	6241
• Safe: No functional damage/personnel injury	"
• Marginal: Degrade system/no major damage or injury	"
• Critical: Substantial system damage or injury	"
• Catastrophic: Severe degradation/extensive damage/multiple injuries or deaths	"
• Class I - IV defined for safe-catastrophic, respectively	38130A
• Categories reversed for catastrophic (I) to negligible (V)	882A
• Hazard probability:	
• Prediction is part of the safety analysis	38130
• Probability levels added to severity categories: A (frequent/likely to occur) to F (impossible/can't occur)	882A 882B
• Remote (level D probability level defined as "unlikely, but possible to occur in the life of an item"	"
• Level E renamed "improbable" and is defined as level D - 882A was defined: "so unlikely it can be assumed occurrence may not be experienced."	38130
• Risk Management:	38130A
• Catastrophic hazards will be eliminated	38130
• Safety specs have priority over design specs	38130A
• Critical hazards will be minimized	882B
• Safety specs have priority consistent with ops/mission objectives	
• Level of risk assumption and criteria are introduced	
10. System safety management	38130A
• Defines function, authority, and inter-relationships	"
• Exercises appropriate controls	"
• Assures optimum safety	"
• Precludes degradation of inherent safety	"
11. Degree of safety directly dependent upon management emphasis by government and contractors	882
12. Results of safety effort depend on procurement agency clearly stating objectives/requirements	882
13. Managing activity responsibilities	882A
• Plan, organize, and implement system safety program	"
• Establish safety requirements for system design	"
• State safety specifications in contract	"
• Requirement for activities in contract	"
• Contractually applicable safety data	"
• Ensure complete SSPP	"
• Review implementation of SSPP	"
• Supply historical data	"
• Review contractor system safety effort/data	"
• Ensure specifications are updated with test analyses results	"
• Review adequacy of all mil standards	"
• Establish system safety groups	
14. Software hazard analyses:	882B

• Begin early in development and may be updated • Are a flow-down requirements process followed by an upward-flow verification process	
15. Four elements of effective system safety program • Planned approach to accomplish tasks • Qualified people • Authority to implement tasks through all levels of management • Appropriate manning/funding	882B “ “ “ “

Figure 1-6

GENERAL SYSTEM SAFETY REQUIREMENTS

REQUIREMENT	INITIAL REFERENCE
1. Assure safety requirements are defined	6241
2. System safety plan is prepared (SSPP)	6241
3. Safety analysis conducted (PHA, SSHA, SHA, O&SHA)	6241
4. Interface requirements, responsibilities, and standards are set	6241
5. Progress reports submitted	6341
6. Define management responsibilities	6241
7. Listing of specific safety hazards (PHL) prepared	6241
8. Procedures for controlling safety tasks developed	6241
9. Areas needing safety studies identified	6241
10. Tests to be monitored identified	6241
11. Assemble all players for interactions (SSG/SSWG)	6241
12. Identify training requirements	6241
13. Establish a file on safety design activities	6241
14. Safety validation tests shall be conducted	6241
15. Tech data: system safety-peculiar information documented • In tech manuals, orders, checklists • Cautions, Warnings, Emergency procedures prepared • Submitted to procuring agency IAW contract	6241
16. Review environmental hazards	38130
17. Review specs, standards, regs, handbooks for applicability	38130
18. Consider alternate approaches	882A
19. Protect critical components and power sources	882A
20. Mods do not degrade inherent safety	882A

Figure 1-7

SYSTEM SAFETY PHASE REQUIREMENTS

REQUIREMENT	INITIAL REFERENCE
CONCEPT EXPLORATION	
• Evaluate system safety design features	882
• Identify possible safety interface problems	"
• Highlight special safety considerations	"
• Describe safety tests/data needed for next phase	"
• PHA required to identify inherent hazards	"
• Update requirements based on this phase	882
• Review designs of similar systems	882A
• Use past experience with similar systems for requirements	"
• Identify waiver requirements	"
• Prepare a report for milestone reviews	"
• Tailor subsequent phase system safety programs	"
PRODUCTION DEFINITION AND RISK REDUCTION	
• SSPP with contractor's safety effort proposed	882
• Establish criteria for validating contractor performance	"
• Update specs, requirements, safety characteristics	"
• PHA for hazards and inherent risks	"
• Safety interface study of subsystems (SSHAs)	"
• Tradeoff Studies	"
• Identify qual/quantitative system safety requirements	"
• Methods to control hazards	"
• Perform system and equipment interface (SHA/O&SHA)	"
• Update test plans	"
• Project activities in production and operational phases	"
• Prepare summary report for milestones briefs	"
• Perform SSHA, SHA, and O&SHA	882A
• Review test plans	"
• Review training plans	"
• Evaluate mishap and failures for corrective actions	"
• SHA on test configuration model	882B
• Expanded production analysis requirements	"
• Identify need for special tests	"
• Review O&M pubs	"
• Review safety information from DOT, EPA, and OSHA	"

ENGINEERING AND MANUFACTURING DEVELOPMENT	882
• Effective/timely implementation of SSPP	"
• Update system safety requirements	"
• Perform hazard analyses (SHA/O&SHA)	"
• Evaluate system design for hazards and safety improvements	"
• Establish test requirements and ensure verification of design	"
• Participate in design reviews	"
• Inputs to manuals, tech orders, emergency procedures	"
• Evaluate mishaps/failures and make recommendations	"
• Review/input to tradeoff studies	"
• Review drawings/specs for safety	"
• Identify safety/protective equipment	"
• Provide safety input to training	"
• Ensure design incorporated safely	882A
• Hazards identified in production definition and risk reduction phase corrected	"
• Evaluate storage, packing, handling	"
• Review production plans	"
• Set disposal/demilitarization requirements	"
• Prepare report for milestone reviews	"
• Tailor requirement for production/deployment	"
• Review logistics support consideration	"
• Expanded production analysis requirements	
PRODUCTION, FIELDING/DEPLOYMENT, AND OPERATIONAL SUPPORT	
• Monitor system for adequacy of design safety	882
• Evaluate design changes to prevent degraded inherent safety	"
• Review operations and maintenance pubs for safety information	"
• Evaluate mishaps: recommend design changes	"
• Review efficiency reports for operator	"
• Review disposal of hazardous materials	"
• Update SSPP	882A
• Production line safety for safety control of system	"
• Production manuals/procedures have warnings, etc.	"
• Verify test and eval early production hardware	"
• Review procedures for storage, handling, packaging	"
• Monitor field inspections; identify critical aging problems	"
• Update O&SHA	"
• Identify follow-on changes needed	"
• Identify critical parts, procedures, facilities inspections	"
• Quality control to achieve design during production	882
• Identify new hazards from engineering designs	"
• Ensure corrective action is taken on new hazards	"
• Review test plans for safety	"

CONSTRUCTION (facilities)	
• Ensure building, fire, and ACE requirements are met	882B
• Facility and installed systems interfaces reviewed	“
• Review equipment plans	“
• Update hazard tracking system	“
• Evaluate mishaps for deficiencies/oversights	“
• Review hazards due to changes in design	“

CHAPTER 2

SYSTEM SAFETY POLICY AND PROCESS

2.1 DoD Directives.

DODD 5000.1 states overall policies and principles for all DOD acquisition programs and identifies key DOD acquisition officials and forums. DOD 5000.2-R spells out the specific acquisition procedures for major defense acquisition programs. It is a streamlined document that spells out overall top-level requirements.

Para 3.3.7, Environmental, Safety, and Health Considerations, states:
The acquisition strategy shall include a programmatic environmental, safety, and health (ESH) evaluation. The PM shall initiate the ESH evaluation at the earliest possible time in support of a program initiation decision (usually Milestone I) and shall maintain an updated evaluation throughout the life-cycle of the program. The ESH evaluation describes the PM's strategy for meeting ESH requirements (see 4.3.7), establishes responsibilities, and identifies how progress will be tracked.

Para 4.3.7, Environment, Safety, and Health, states:
All programs, regardless of acquisition category, shall comply with this section and be conducted in accordance with applicable federal, state, interstate, and local environmental laws and regulations, Executive Orders (EOs), treaties, and agreements. The PM shall ensure that the system can be tested, operated, maintained, and repaired in compliance with environmental regulations and the requirements of this section.
Environmental, safety, and health (ESH) analyses shall be conducted, as described below, to integrate ESH issues into the systems engineering process and to support development of the Programmatic ESH Evaluation (see 3.3.7).

Para 4.3.7.3, System Safety and Health, states in part:
The PM shall identify and evaluate system safety and health hazards, define risk levels, and establish a program that manages the probability and severity of all hazards associated with development, use, and disposal of the system. All safety and health hazards shall be managed consistent with mission requirements and shall be cost-effective. Health hazards include conditions that create significant risks of death, injury, or acute chronic illness, disability, and/or reduced job performance of personnel who produce, test, operate, maintain, or support the system.
Each management decision to accept the risks associated with an identified hazard shall be formally documented. The CAE shall be the final approval authority for acceptance of high risk hazards. All participants in joint programs shall approve acceptance of high risk hazards. Acceptance of serious risk hazards may be approved at the PEO level.
It should be noted that the regulation does not define High or Serious risk hazards. Accordingly, AFI 91-202, Chapter 9, provides specific definition to these levels of hazards.

2.2 USAF Policy.

USAF Responsibilities. Historically, Air Force responsibilities had been defined in DODI 5000.36, System Safety Engineering and Management. DODI 5000.36 was replaced by DODI 5000.2, Part 6, Section I, and later by DOD5000.2-R, para 4.3.7. which did not specifically call out DoD components' responsibilities. However, the USAF system safety duties are still valid. They are:

(1) Establish system safety programs for each system acquisition.
(2) Summarize system safety at design and program reviews.
(3) Establish programs to ensure application of MIL--STD-882.
(4) Maintain historical system safety data for use by all DoD components and contractors.
(5) Support DoD system programs with trained system safety personnel.
(6) Maintain records of system safety lessons learned.
(7) Develop guidelines for evaluating contractors' safety efforts.
(8) Consider safety technologies which could reduce risk.
(9) Integrate system safety and human factors engineering.
(10) Consider contractor incentives for lower mishap rates.
(11) Establish a system safety point of contact.
(12) Develop and promote improved system safety engineering techniques.

USAF Program Requirements. These requirements remain valid for system safety programs.

(1) Define safe operating limits.
(2) Ensure that historical safety data are considered.
(3) Provide for preliminary hazard analyses during system concept exploration to define the scope and level of detail of the required system safety effort.
(4) Apply MIL-STD-882 to identify hazards and associated risk with the system and determine remedial priorities.
(5) Establish procedures to ensure timely follow-up on identified hazards and implement corrective action.
(6) Formally document each management decision to accept the risks associated with an identified hazard.
(7) Ensure that the Test and Evaluation Master Plan addresses safety-critical issues to validate the results of system safety analyses. When normal testing cannot demonstrate safe system operation, prepare and monitor special safety tests and evaluations.
(8) Integrate system safety engineering and management into the total system acquisition program.
(9) Ensure that system safety requirements are consistent with the technology of other disciplines, such as reliability, maintainability, and human factors engineering.
(10) Eliminate or control hazards in systems before the production and deployment phase.
(11) Ensure, when applicable, the transfer of the system safety program and its associated documentation from the developing organization to the appropriate support organization after system deployment.
(12) Require a follow-on system safety effort after initial operational capability to ensure that:

(a) Mission or design changes made after deployment do not introduce hazards or degrade

existing levels of system safety and that changes to enhance system safety are implemented.

(b) Appropriate hazard analyses take place throughout the deployment phase of systems.

(c) Procedures for identifying, tracking, storing, handling, and disposing of hazardous materials and equipment associated with systems are developed and implemented.

USAF OPRs. Within the Air Force, specific offices of primary responsibility (OPRs) and duties for system safety were outlined in AFR 800-16, USAF System Safety Program. With the many organizational and regulatory changes recently in DOD acquisition, AFR 800-16 required replacement with other appropriate guidance. Chapter 9 of AFI 91-202l contains this guidance. A recent study by the Air Force Safety Center gives a good outline of duties by OPRs. It is based on a historical review of system safety duties and then is updated with current trends affecting the acquisition process. Figure 2-1 lists these responsibilities by OPR.

2.3 Designing for Safety.

Meeting the objectives of system safety stated in paragraph 1.2 is done within the constraints of cost, schedule, and performance. Maximum effectiveness is obtained by applying system safety principles early and throughout the life cycle of the system. By Milestone I, it is estimated that 70 percent of the cost of building and operating a system is predetermined. Thus, comprehensive early planning can provide substantial benefits. Early attention to engineering considerations minimizes design changes to correct safety deficiencies. Late hardware changes historically add weight, complexity, decrease reliability, increase maintenance time, and cost money and time. (36:3)

Specific design requirements are found in standards, specifications, regulations, design handbooks, and other guidance. Some general system safety design requirements have evolved over the last 40 years and are summarized in Chapter 4.

2.4 System Safety Process. (28:17-19)

Before discussing the various aspects of a system safety program, the general system safety process must be understood. The system safety process is a logical, engineering approach for obtaining system safety objectives.

A simplified model of the process is shown in Figure 2-2. This closed loop process can be realistically followed for systems of any complexity without losing the effectiveness of the process or overburdening the program management. The system safety process can be applied at any point in the system life cycle, but the greatest advantages are achieved when it is used early in the acquisition life cycle. This process is normally repeated as the system evolve or changes and as problem areas are identified.

The System Safety Process

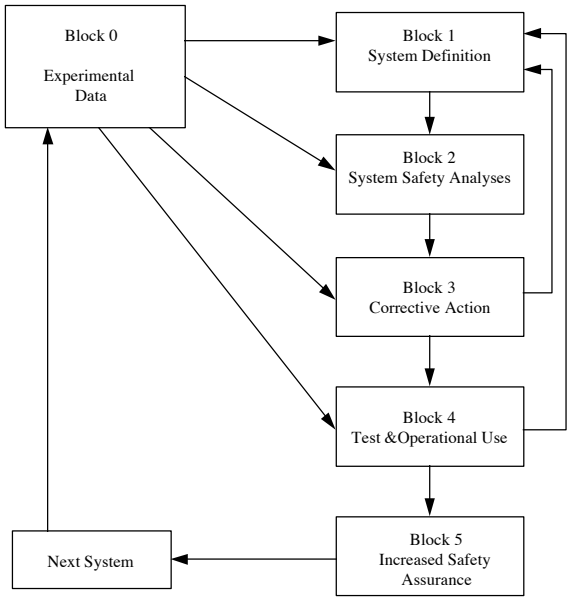


Figure 2-2

Block 0--Experimental Data. Experimental data represent corporate memory/lessons learned or knowledge gained from operation of previous systems similar to the one under consideration. This information is usually scattered in many different sources and must be identified and collected to be useful. Of particular interest is previous action taken to correct design features that have resulted in accidental damage, loss, injury, or death. This corrective action includes design changes, production/operational retrofits, and operating/maintenance procedures changes. This collection of reference information can be useful as inputs to the preliminary hazard analysis.

Block 1--System Definition. The first step in the process is to clearly define the system under consideration. The system elements must be specified as early as possible and revised as required during the system life cycle. System definitions must also include major system interfaces such as system operating condition, environmental situation, and the human role in system operation. The object of good system definition is to set limits for the following steps in the process and reduce complex systems to manageable parts.

Figure 2-1

FUTURE SYSTEM SAFETY STRUCTURE

1. **General (all levels)**
   - (a) Define objectives
   - (b) Set policy
   - (c) Clarify lines of responsibility
   - (d) Establish appropriate organizational structures
   - (e) Determine funding issues
   - (f) Assist subordinate organizations
   - (g) Advise higher headquarters
   - (h) Evaluate performance of subordinate organizations
   - (i) Determine procedures for their own organization
2. **System Safety Manager (Product or Logistics Center)**
   - (a) Focal point of system safety for a program
   - (b) Develop system safety program and plan IAW MIL-STD-882
   - (c) Ensure identification of hazards and risks
   - (d) Establish hazard-tracking system
   - (e) Coordinate system safety group meetings
   - (f) Ensure system safety in program documents
   - (g) Assist with source/contract issues
   - (h) Monitor contractor's effort
   - (i) Identify system safety requirements
   - (j) Ensure feedback on tested/fielded systems
   - (k) Ensure safety incorporation into technical orders
   - (l) Monitor safety impacts of configuration changes
3. **Program manager**
   - (a) Establish an adequate system safety program
   - (b) Accept minor residual risks
   - (c) Document risk acceptance
   - (d) Report all residual risks to PEO
   - (e) Determine risk reduction priorities/actions
   - (f) Integrate system safety into total acquisition program
   - (g) Chair SSG meetings; periodically review hazards/risks
   - (h) Formalize system safety requirements
   - (i) Direct contractor efforts
4. **Program Executive Officer (PEO)**
   - (a) Assess risks for all residual hazards
   - (b) Report major risks to AFAE
   - (c) Establish system safety design criteria
   - (d) Establish safe operating limits
   - (e) Review system safety at milestones
5. **Air Force Acquisition Executive (AFAE)**

(a) Provides risk assessments to SAF

(b) Informs OSD of significant residual risks

6. User

(a) Submit system safety requirements and safety features

(b) Present user requirements/priorities at system safety meetings/reviews

(c) Review mission changes for impact on requirements

(d) Provide system safety effort for in-house programs

(e) Assist as requested with system safety tasks

(f) Participate in independent safety assessments

(g) Provide focal points for system safety user inputs

(h) Identify command-unique hazards

(i) Review acquisition documents for user system safety inputs

7. Product Centers/Air Logistics Centers (PC/ALC)

(a) Provides system safety manager for programs

(b) Train system safety personnel

(c) Review program documents for system safety

(d) Ensure adequate staff and engineering support to perform system safety tasks

(e) Evaluate system safety effectiveness

(f) Provide technical expertise program offices

(g) Participate in SSGs

8. AFMC

(a) Accept risk on command programs

(b) Ensure adequate and independent assessment of program risks for command programs

(c) Review system safety in appropriate specs and standards

(d) Assist in independent safety analysis

(e) Ensure lab system safety; safety enhancements developed

(f) Safety audit on major systems

9. HQ AFSC

(a) Provide independent assessment of system safety at each milestone

(b) Develop guidance/policy for AF system safety

(c) Represent AF in safety matters

(d) Reviews mishap reports for system safety lessons/causal validation

(e) OPR for AF system safety program (AFI 91-202)

(f) Develop AF system safety training options

(g) Provide assistance to higher/lower headquarters

(h) Evaluate the effectiveness of system safety in AF

(i) Provide independent engineering expertise

(j) Foster government/civilian interface in system safety

(k) Investigate and advocate new safety technologies

10. HQ USAF

(a) Issue guidance and policy for AF system safety

(b) Promote USAF objectives and policies for system safety with other DoD and higher level authorities

(c) Appoint OPRs for system safety standards/specifications

(d) Advocate and sponsor safety technologies that reduce risk and improve methods

(e) Fund training of system safety personnel

(f) Manage system safety manpower and career development programs

g) Provide for system safety in acquisition/budget document

(h) Be AFAE for minor programs

(i) Prepare/review AF acquisition/budget documents

11. OSD

(a) Review high-level acquisition documentation to ensure consideration of appropriate safety concepts and programs

(b) Ensure component headquarters have allocated adequate resources for safety programs

(c) Identify funds for system safety engineering research projects

(d) Ensure system safety reviewed before/during DSARC

(e) Establish DoD objectives (goals) for system safety

(f) Establish DoD policy for system safety (a decision that bounds the discretionary limits of lower level managers)

Block 2--System Safety Analyses. The heart of the system safety process is a comprehensive, methodical analysis of the system and its elements. The search for possible system hazards is the state of before-the-fact accident prevention. To be comprehensive, the analyses must consider every undesired event that might occur to the system and either the conditions that produce the undesired event or the consequences from it. To do this without getting hopelessly bogged down in complex details requires a methodical or systematic approach for the analyses. The result is a high degree of confidence that no stone has been left unturned in the search for potential accidents. A thorough analysis should identify possible hazards, classify the hazard for severity, determine the probability of occurrence of the hazard, and suggest possible corrective action. The corrective action should also be worked into the analysis and be examined to evaluate it for effectiveness. (Refer to Chapter 7 for more information on analyses.) It is essential to maintain a closed loop hazard identification and tracking system so that all identified hazards are followed through the corrective action or program decision to not implement any action, including the rationale for each decision. This type of documentation, while not part of the analyses, is the administrative foundation work over which the system safety program lies and is essential in assuring completed action on identified hazards as well as following the progress of benefits derived from the system safety program.

Block 3--Corrective Action to Eliminate/Control Hazard. Nothing that has been done so far in the system safety process will prevent the first mishap. The process produces no useful result until some action is actually taken to eliminate or control the hazards that have been identified. However, all steps taken up to this point have been designed so that the most appropriate action can be taken. Again, the program manager (PM) is responsible for this step. This responsibility includes the decision and direction for action, plus the allocation of resources required to do the job. This is perhaps the most crucial step in the entire process because it is here that practical results are actually achieved. Any action taken in this step will modify or change some element of the system. The modification need not involve only hardware. For example, procedures can be revised. Initial assumptions on operating conditions can be amended or basic specifications can be changed. Because the system is modified, the initial definition of the system and its elements in Block 1 must also be revised. The process is then repeated, as required, until any additional hazards introduced by system modification are acceptable. These repeated steps ensure that actions taken to correct one hazard do not induce more hazards elsewhere in the system.

Block 4--Test and Operational Use. Up to this point in the process, hazards identified through analysis have been eliminated or controlled (within program limitations). However, since analyses are never 100-percent complete and accurate, new hazards are identified when the system is exercised through test and operational use. The occurrence of an accident or incident is examined critically to determine causes and evaluate effects. The causes and effects could range from something already predicted as possible, or even probable under certain conditions, to something entirely new and surprising. The results of this mishap analysis should then reveal any deficiencies in the system design or procedures and serve to direct corrective action back to the system safety process. In this way, maximum use is made of the mishap experience without having to go back and continually rediscover new truths. Most, if not all, development programs for complex systems include testing to verify performance and the demonstration of system capabilities. They are conducted to assure the user that this system performs as required. Tests and demonstrations normally performed on a system or its components are also planned and conducted to reveal any safety inadequacies. At the same time, these tests and demonstrations serve to verify the results of the process and give greater confidence in the assurances provided. As with the results of mishap analyses, deficiencies uncovered are directed to the system safety process for corrective action.

Block 5--Increased Safety Awareness. In those areas where effectiveness evaluation and test and demonstration indicate that the system safety process has produced the desired results, assurance that the system safety objective has been met is increased correspondingly. This increased assurance is then applied the next time we go through the process, as an element of system qualification, or in applying the process to another system. In this manner, we continually build on past successes while correcting deficiencies.

2.5 The Acquisition Cycle.

The DOD has defined a structure for translating operational needs into stable, affordable acquisition programs. The structure, as shown in Figure 2-3, is a combination of requirements generation, acquisition management, and planning, programming, and budgeting systems. As shown in Figure 2-4, this results in the following key interactions of these systems:

- Broad mission needs must be initially identified by the requirements generation system.
- The acquisition system must identify and assess alternative ways of satisfying these needs in light of current and projected technology development, producibility, industrial capability, and support constraints.
- Initial affordability decisions on proposed new acquisition programs must be made in the planning, programming, and budgeting system process based on the Defense Planning Guidance, the approved long-range investment plans, and overall funding constraints.
- The initial broad mission need statements must be progressively translated into performance objectives, system-specific performance requirements, and a stable system design that can be efficiently produced.
- Major cost-performance-schedule tradeoffs must be made throughout the course of program implementation. They are based on validated threat assessments, the status of program execution, risk assessment, testing results, and affordability constraints brought about by changes in topline fiscal guidance.

DoD has defined acquisition cycle phases and milestones as shown in Figure 2-5. Each phase is preceded by a milestone decision point. The milestone reviews are comprehensive evaluations of program cost, schedule, and performance status of the present phase, plans for the next phases, and all associated risk considerations. Program-specific results, called exit criteria, are established for the next phase.

2.6 System Safety in the Acquisition Cycle.

Using system safety analyses and other management tools, the system safety program evaluates and documents the risks associated with identified hazards. The system safety process must provide the program manager with the necessary information to allow for timely inputs into the integrated management framework at defined program milestones. Specific phase-based system safety activities are detailed in Chapter 10.

Figure 2-3

DOD INTEGRATED MANAGEMENT SYSTEM

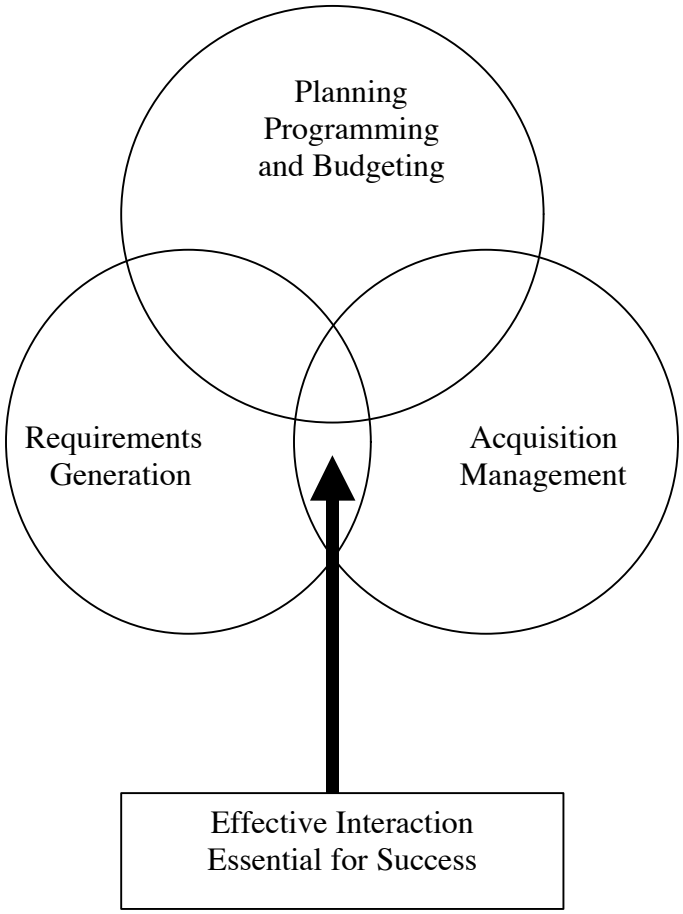


Figure 2-4

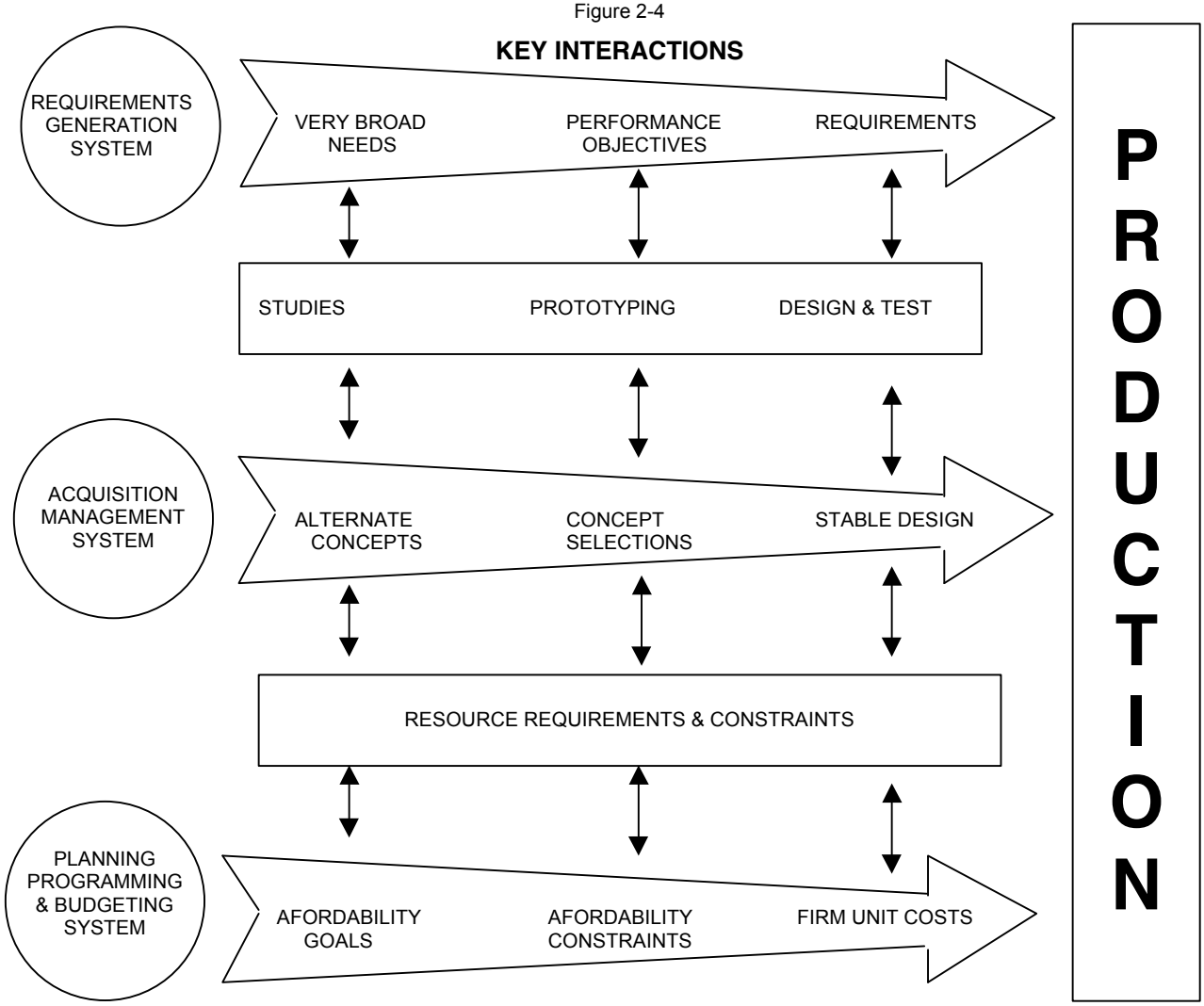
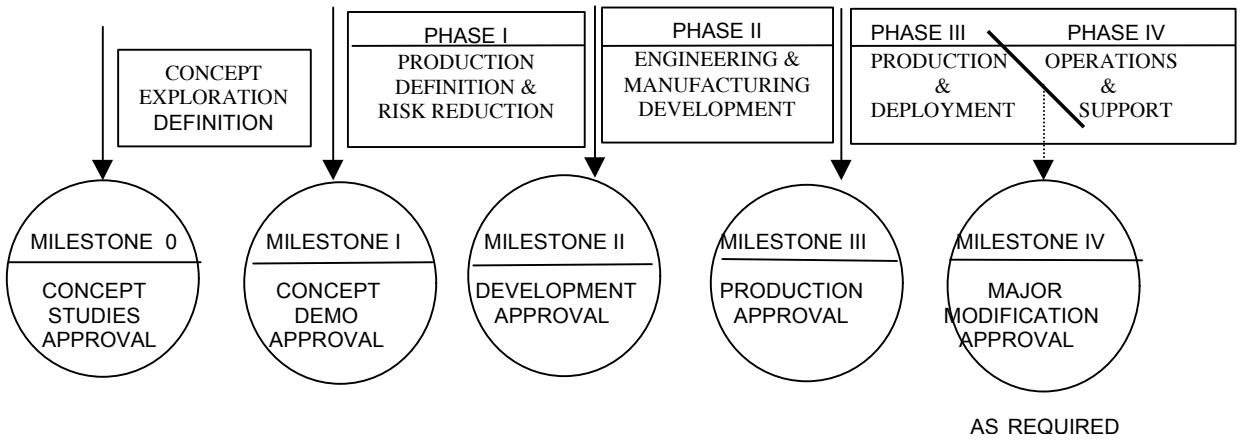


Figure 2-5

ACQUISITION MILESTONES AND PHASES



CHAPTER 3

RISK ASSESSMENT

3.1 Definitions.

System safety is an organized effort to identify and evaluate risk and to find an optimized solution to resolve the risk while satisfying various constraints. To understand the process, key definitions from MIL-STD-882 must be understood.

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.

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

Safety is freedom from those conditions that cause mishaps. Safety is not a measurable quantity and, therefore, not manageable. Mishaps, however, are measurable. And the conditions that lead to a mishap are also measurable. A hazard, as a condition, may or may not be a problem. To determine if there is cause for alarm, we must know two things about the hazard.

Mishap Probability. The aggregate probability of occurrence of the individual events/hazards that might create a specific mishap.

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

These aspects of hazards are measurable and, when combined, give us risk.

Mishap Risk. An expression of the impact of a mishap in terms of mishap severity and probability of occurrence.

Risk Assessment: A comprehensive evaluation of risk and its associated impact.

Program Manager (PM). A government official who is responsible for managing an acquisition program. Sometimes also referred to as the Managing Activity (MA).

The evaluation process requires that judgments and decisions be made. The person making these decisions is the managing activity. System safety personnel are, therefore, involved in assessing risk and bringing the assessment to the managing authority who makes program decisions based on these assessments.

The significance of the definitions can better be understood in a historical perspective. System safety began within the context of 'looking for safety.' Hazards soon became the focus since safety was immeasurable. But the focus hazards neglects the likelihood of a hazard causing a mishap or the relative consequences of mishaps. Quantifying probability and severity has led to the present emphasis on risk assessment and management.

3.2 Types of Risk.

There are various models describing risk. The model in Figure 3-1 follows the system safety concept of risk reduction.

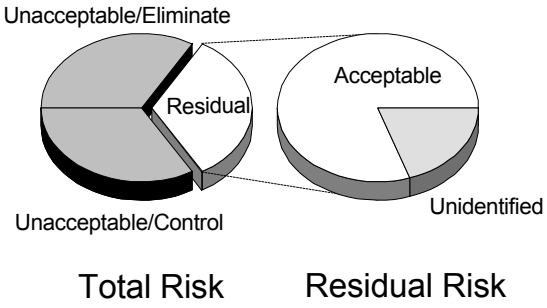
Total risk is the sum of identified and unidentified risks.

Identified risk is that risk which has been determined through various analysis techniques. The first task of system safety is to make identified risk as large a piece of the overall pie as practical. The time and costs of analyses efforts, the quality of the safety program, and the state of technology impact the amount of risk identified.

Unidentified risk is the risk that hasn't been determined. It's real. It's important. But it's not measurable. Some unidentified risk is subsequently determined when a mishap occurs. Some risk is never known.

Figure 3-1

Types of Risk



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

Acceptable risk is the part of identified risk which is allowed to persist without further engineering or management action. It is accepted by the managing activity. However, it is the user who is exposed to this risk.

Residual risk is the risk left over after system safety efforts have been fully employed. It is sometimes erroneously thought of as being the same as acceptable risk. Residual risk is actually the sum of acceptable risk and unidentified risk. This is the total risk passed on to the user.

3.3 System Safety Order of Precedence. (30:5)

The overall goal of a system safety program is to design systems that do not contain hazards. However, the nature of most complex systems makes it impossible or impractical to design them completely hazard-free. As hazard analyses are performed, hazards will be identified that will require resolution. System safety precedence defines the order to be followed for satisfying system safety requirements and reducing risks. The alternatives for eliminating the specific hazard or controlling its associated risk will have to be

evaluated so that an acceptable method for risk reduction can be pursued.

The order of precedence for satisfying system safety requirements and resolving identified hazards is:

a. Design for Minimum Risk. From the first, design to eliminate hazards. If an identified hazard cannot be eliminated, reduce the associated risk to an acceptable level, as defined by the MA, through design selection. Defining minimum risk is not a simple matter. It is not a cookbook process that can be numerically developed without considerable thought. Minimum risk will vary from program to program. See paragraph 3.6 for more information.

b. Incorporate Safety Devices. If identified hazards cannot be eliminated or their associated risk adequately reduced through design selection, that risk shall be reduced to a level acceptable to the MA through the use of fixed, automatic, or other protective safety design features or devices. Provisions shall be made for periodic functional checks of safety devices when applicable.

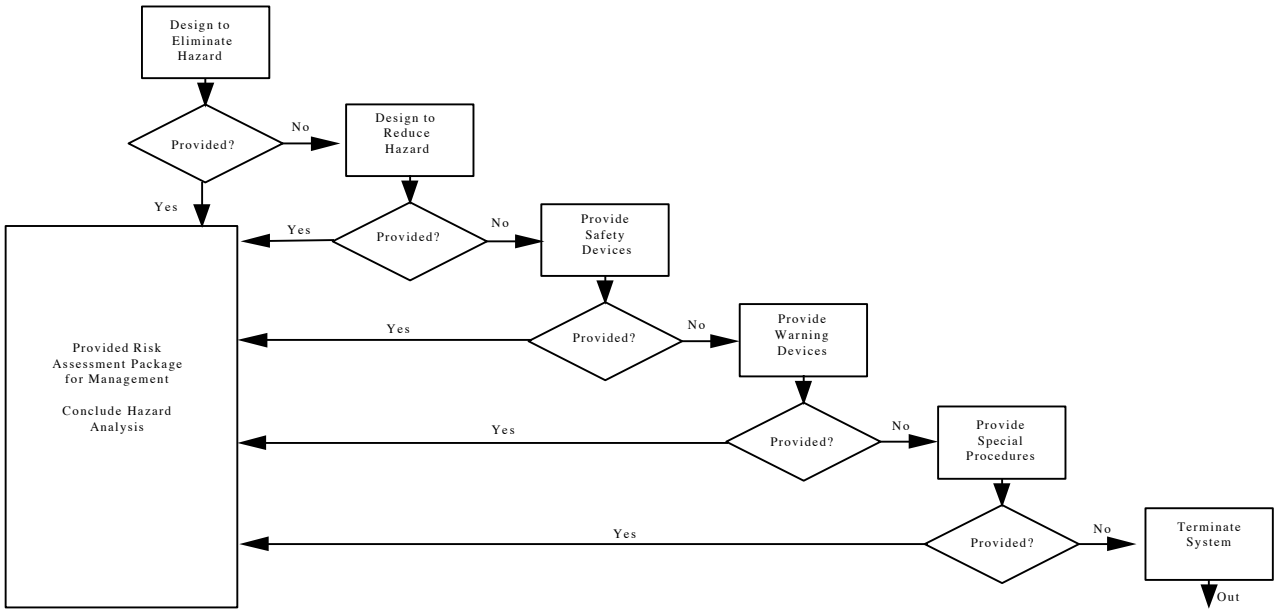
c. Provide Warning Devices. When neither design nor safety devices can effectively eliminate identified hazards or adequately reduce associated risk, device shall be used to detect the condition and to produce an adequate warning signal to alert personnel of the hazard. Warning signals and their application shall be designed to minimize the probability of incorrect personnel reaction to the signals and shall be standardized within like types of systems.

d. Develop Procedures and Training. Where it is impractical to eliminate hazards through design selection or adequately reduce the associated risk with safety and warning devices, procedures and training shall be used. However, without a specific waiver, no warning, caution, or other form of written advisory shall be used as the only risk reduction method for Category I or II hazards. Procedures may include the use of personal protective equipment.

The process for reducing risk due to a hazard is illustrated in Figure 3-2. (40:40) It is an obvious interaction of both engineering and management considerations to bring about an optimal resolution of risk. Final resolution rests in the decision made by the managing activity.

Figure 3-2

HAZARD REDUCTION PRECEDENCE



3.4 Mishap Severity Categories and Probabilities. (30:8)

Hazards do not necessarily result in mishaps. But if it does occur, the hazard creates mishaps of certain severity.

Mishap severity categories (Figure 3-3) are defined to provide a qualitative measure of the worst credible mishap resulting from personnel error, environmental conditions; design inadequacies; procedural deficiencies; or system, subsystem, or component failure or malfunction. These mishap severity categories provide guidance to a wide variety of programs. However, adaptation to a particular program is generally required to provide a mutual understanding between the MA and the contractors as to the meaning of the terms used in the category definitions. The adaptation must define what constitutes system loss, major or minor system damage, and severe and minor injury and occupational illness. The probability that a hazard will be created during the planned life

expectancy of the system can be described in potential occurrences per unit of time, events, population, items, or activity (Figure 3-4).

Assigning a quantitative hazard probability to a potential design or procedural hazard is generally not possible early in the design process. A qualitative hazard probability may be derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning a hazard probability shall be documented in hazard analysis reports. Fig 3-3 and 3-4 definitions of descriptive words may be modified based on quantity involved. Also. The size of the fleet or inventory should be defined.

An example of a modified hazard probability definition is presented below.

LEVEL	APPROXIMATE FREQUENCY
Frequent	1 failure in 100 (10^{-2}) cycles
Probable	10-2 to 10-4 cycles
Occasional	10^{-4} to 10^{-5} cycles
Remote	10^{-5} to 10^{-6} cycles
Improbable	Less than 10^{-6} cycles

Figure 3-3

EXAMPLE MISHAP SEVERITY CATEGORIES

Description	Category	Mishap definition
CATASTROPHIC	I	Death or
CRITICAL	II	Severe injury, occupational illness or major system damage
MARGINAL	III	Minor injury, minor occupational illness, or minor system damage
NEGLIGIBLE	IV	Less than minor injury, occupational illness, or minor system damage

Figure 3-4

EXAMPLE HAZARD PROBABILITY LEVELS

Description	Level	Specific Individual Item	Fleet or Inventory
FREQUENT	A	Likely to occur frequently	Continuously experienced
PERIODIC	B	Will occur several times in life of an item	Will occur frequently
OCCASIONAL	C	Likely to occur sometime in life of an item	Will occur several times
REMOTE	D	Unlikely, but possible to occur in life of an item	Unlikely, but can be reasonably be expected to occur
IMPROBABLE	E	So unlikely it can be assumed occurrences may not be experienced	Unlikely to occur, but possible

3.5 Mishap Risk Assessment.

By combining the probability of occurrence with mishap severity, a matrix is created where intersecting rows and columns are defined by a Mishap Risk Assessment Value. The value forms the basis for judging both the acceptability of a risk and the management level at which the decision of acceptability will be made. The value may also be used to prioritize resources to resolve risks due to hazards or to standardize hazard notification or response actions.

Prioritization may be accomplished either subjectively by qualitative analyses resulting in a comparative mishap risk assessment or through quantification of the probability of occurrence resulting in a numeric priority factor for that hazardous condition. Figures 3-5 and 3-6 show two sample matrices for mishap risk assessment which can be applied to provide qualitative priority factors for assigning corrective action. In the first matrix, an identified hazard assigned a mishap risk assessment value of 1A, 1B, 1C, 2A, 2B, or 3A might require immediate corrective action. A value of 1D, 2C, 2D, 3B, or 3C would be tracked for possible corrective action. A value of 1E, 2E, 3D, or 3E might have a lower priority for corrective action and may not warrant any tracking actions. In the second matrix, risk values of 1 through 20 (1 being highest risk are assigned somewhat arbitrarily. This matrix design assigns a different value to each frequency-category pair, thus avoiding the situation caused by creating values as products of numbers assigned to frequency and category which causes common results such as 2 X 6 = 3 X 4 = 4 X 3. This situation hides information pertinent to prioritization. These are only examples of a risk assessment methods and do not fit all programs. (30:9)

The mishap risk assessment value will be more useful if the severity and probability scales are carefully defined. Some suggestions for each are as follows. (18:14-17)

"Severity ranges should be sized so that events within each category are of comparable severity....Equating the severity of event and conditions which can cause one fatality with those which can cause 100 or 1,000 does not make sense. The potential problems associated with sizing of the severity ranges grow as the size of the system grows. Program managers need to be provided with risk information that has the fidelity to distinguish the hazardous events that meet general criteria.

Severity range thresholds for each severity category should be comparable when considering personal, system, or facility losses....For example, events or conditions which could cause the loss of an E-4 Airborne Command Post would be categorized by MIL-STD-882 as catastrophic. Loss of a single crewman, mechanic, or passenger would also fall in the catastrophic category....Severe injuries, such as total loss of sight of a mechanic, and system damage of several million dollars are not normally considered to have equal value, even though both are considered as values for the critical category.

If the ranking criteria use risk as a function of severity and probability, quantitative scales or qualitative scales based on quantitative logic should be used. If the concept that the expected losses (or risk) associated with a hazardous event or condition may be estimated by multiplying the expected severity of the accident by the probability of the accident, then some sort of quantitative basis is necessary....Failure to provide a quantitative basis for the scales can cause significant confusion and dissipation of safety resources when an arbitrary risk ranking scale is used.

Develop the severity values using order of magnitude ranges. This gets severity values far enough apart to avoid hair--splitting arguments and simplifies severity assessment during PHAs.

Quantify the threshold values for the probability ranges. Quantification reduces confusion associated with strictly qualitative definitions. Although it is impossible to quantify the ranges in MIL-STD-882 due to its extremely broad application, developing quantified probability ranges for specific systems is a relatively easy task to accomplish.

The probability of occurrence should refer to the probability of an accident/consequence as opposed to the probability of an individual hazard/basic event occurring. The typical accident sequence is much more complicated than a single line of erect dominos where tipping the first domino (hazard) triggers a clearly predictable reaction.

Develop the probability values using order of magnitude ranges. Do this for the same reason you did it when developing the severity ranges."

Figure 3-5

FIRST EXAMPLE MISHAP RISK ASSESSMENT VALUES

FREQUENCY OF OCCURRENCE	I CATASTROPHIC	II CRITICAL	III MARGINAL	IV NEGLIGIBLE
(A) FREQUENT	1	3	7	13
(B) PERIODIC	2	5	9	16
(C) OCCASIONAL	4	6	11	18
(D) REMOTE	8	10	14	19
(E) IMPROBABLE	12	15	17	20

HAZARD RISK ASSESSMENT VALUE	SUGGESTED CRITERIA
1-5	High (Accepted by Component Acquisition executive)
6-9	Serious (Accepted by Program Executive Officer)
10-17	Medium (Acceptable by Program Manager)
18-20	As directed (Usually acceptable without review)

Figure 3-6

SECOND EXAMPLE MISHAP RISK ASSESSMENT VALUES

FREQUENCY OF OCCURRENCE	I CATASTROPHIC	II CRITICAL	III MARGINAL	IV NEGLIGIBLE
(A) FREQUENT	1A	2A	3A	4A
(B) PERIODIC	1B	2B	3B	4B
(C) OCCASIONAL	1C	2C	3C	4C
(D) REMOTE	1D	2D	3D	4D
(E) IMPROBABLE	1E	2E	3E	4E

HAZARD RISK INDEX	SUGGESTED CRITERIA
1A, 1B, 1C, 2A, 2B, 3A	High (Accepted by Component Acquisition Executive)
1D, 2C, 2D, 3B, 3C	Serious (Accepted by Program Executive Officer)
1E, 2E, 3D, 3E, 4A, 4B	Medium (Accepted by program Manager
4C, 4D, 4E	As directed (Usually acceptable without review)

3.6 Risk Acceptance.

Risk Acceptability. Accepting risk is a function of both risk assessment and risk management. Risk acceptance is not as simple a matter as it may first appear. Several points must be kept in mind.

(1) Risk is a fundamental reality.
(2) Risk management is a process of tradeoffs.
(3) Quantifying risk doesn't ensure safety.
(4) Risk is a matter of perspective.

Day and night, everywhere we turn, we are surrounded by a multitude of risks, some large and some so minimal that they can easily be overlooked, but all demanding, sooner or later, to be recognized (i.e., assessed) and dealt with (i.e., managed). Risks seem like the invisible radio signals that fill the air around us, some clear and some very faint, but all want to be heard. (16:26)

We view taking risks as foolhardy, irrational, and to be avoided. Training children to avoid risk is an all-important duty of parenthood. Risks imposed on us by others are generally considered to be entirely unacceptable. Unfortunately, life is not like that. Everything we do involves risk. There are dangers in every type of travel, but there are dangers in staying home--40 percent of all fatal accidents occur there. There are dangers in eating—food is probably the most important cause of cancer and of several other diseases—but most people eat more than necessary. There are dangers in breathing—air pollution probably kills at least 10,000 Americans each year, inhaling natural radioactivity is believed to kill a similar number, and many diseases are contracted by inhaling germs. There are dangers in working--12,000 Americans are killed each year in job-related accidents, and probably 10 times that number die from job-related illness. But most alternatives to working are even more dangerous. There are dangers in exercising and dangers in not getting enough exercise. Risk is an unavoidable part of our everyday lives. Truly: Living is Dangerous. (16:26-27)

Realistically, some mishap risk must be accepted. How much is accepted, or not accepted, is the prerogative of management. That decision is affected by many inputs....As tradeoffs are being considered and the design progresses, it may become evident that some of the safety parameters are forcing higher program risk. From the program manager's perspective, a relaxation of one or more of the established parameters may appear to be advantageous when considering the broader perspective of cost and performance optimization. The program manager frequently will make a decision against the recommendation of his system safety manger. The system safety manager must recognize such management prerogatives. However, the prudent program manager must make his decision whether to fix the identified problem or formally document acceptance of the added risk. An adjustment of the original parameters would be required. Of course, the addition of personnel loss changes the picture considerably. When the program manager decides to accept the risk, the decision must be coordinated with all affected organizations and then documented so that in future years everyone will know and understand the elements of the decision and why it was made. (37:1-7)

Quantitative Assessment. In any discussion of mishap risk management and risk assessment, the question of quantified acceptability parameters arises. While it is not impossible to obtain meaningful results from such a program, care should be exercised so that the program balance is not disturbed. In any high-risk system, there is a strong temptation to rely totally on statistical probability because it looks on the surface like a convenient way to measure safety. Before embarking in this direction, be sure that the limitations and principles of this approach are well understood and that past engineering experience is not ignored. Quantitative acceptability parameters must be well defined, predictable, demonstrable, and above all, useful. They must be useful in the sense that they can be converted easily into design criteria. Many factors fundamental to system safety are not quantifiable. Design deficiencies are not easily examined from a statistical standpoint. Additionally, the danger exists that system safety analysts and managers will become so enamored with the statistics that simpler and more meaningful engineering processes are ignored. Quantification of certain specific failure modes, which depend on one of two system components, can be effective to bolster the decision to accept or correct it. Be careful! Arbitrarily assigning a quantitative measure for a system creates a strong potential for the model to mask a very serious risk. (37:1-8)

In the design of certain high-risk systems such as nuclear power or weapon systems, there is a strong tendency to rely solely on statistical analysis. To program management, this appears reasonable because it provides a convenient medium to express safety in terms to which the uninitiated can relate. One trap for the unwary is the failure of occurrence. On one such program, risks with a probability of occurrence of 10^{-42} were considered unacceptable! Let's consider this in terms that we can easily relate to—money. If it can be assumed that a single dollar bill is three thousandths of an inch thick, the probability of selecting that bill from a stack of bills, which is 3 inches high (or 1,000 dollars), is 1×10^{-3} (or 1 chance in 1,000). One million dollars is a stack 250 feet tall. The chance of selecting that single dollar bill from the stack is now 1×10^{-6} or one chance in a million. When we go to 1×10^{-9}, or one chance in a billion, our stack is now over 47 miles high. One chance in a trillion--47,000 miles! When we talk in terms of 1×10^{-42} our stack probably won't fit in the galaxy! The probability of an undesired event approaches one occurrence in many times the life of the universe. The point is that we have to establish realistic, reachable safety goals so that management can make intelligent decisions. In this particular instance, the safety analysis dwelled upon the probability of the impossible, and allowed a single human error, with a probability of occurrence in the range of 1×10^{-3}, to cause a near disaster; mainly, because it was not a quantifiable element. It is doubtful if the decision makers were fully aware of the mishap risks they were accepting but were placated by a large, impressive-looking number. (37:1-9)

General risk management principles are: (37:1-9 to 1-10)

a. All human activity involving a technical device or process entails some element of risk.
b. Do not panic at every hazard; there are ways of controlling them.
c. Keep problems in proper perspective.
d. Weigh the risk and make judgments according to your own knowledge, experience, and program need.
e. Encourage other program disciplines to adopt the same philosophy.
f. System operations represent a gamble to some degree; good analysis tilts the odds in favor of the house.
g. System safety analysis and risk assessment does not free us from reliance on good engineering judgment.
h. It is more important to establish clear objectives and parameters for risk assessment than to find a cookbook approach and procedure.
i. There is no "best solution" to a safety problem. There are a variety of directions to go. Each of these directions may produce some degree of risk reduction.

j. To point out to a designer how he can achieve a safety goal is much more effective than to tell him his approach will not work.
k. Safety is a condition which seldom can be achieved totally in a practical manner.
l. There are no "safety problems" in system planning or design. There are only engineering or management problems which, if left unresolved, can cause mishaps.

Risk Perspectives. When talking about risks, we always have to distinguish between three different standpoints:

1. Standpoint of an INDIVIDUAL exposed to a hazard. An individual exposed to a hazard is primarily concerned with the questions: How large is the probability that I will be killed or injured in an accident? How much does my individual risk due to this hazard increase my normal fatality rate? In order to account for this standpoint in a risk analysis, it is therefore necessary to introduce the so-called INDIVIDUAL RISK defined as the (usually annual) probability that an identified person will be killed or injured as a consequence of an accident.

2. Standpoint of the SOCIETY. Besides being interested in guaranteeing minimum individual risk for each of its members, society is concerned about the total risk to the general public: How large are the total losses (e.g., per year) from a hazardous activity? To describe this standpoint, the aforementioned definition of risk as the expected damage of an activity applies. In the following, this risk, describing the standpoint of society, will be called the real COLLECTIVE RISK. If expressed in terms of annual risks, it corresponds to the respective value shown in actual accident statistics.

3. Standpoint of the INSTITUTION RESPONSIBLE FOR THE ACTIVITY. The institution responsible for an activity can be a private company or a government agency. From their point of view, it is not only essential to keep individual risks of employees or other persons and the collective risk at a minimum. An institution's concern is also to avoid catastrophic and spectacular accidents. As experience clearly demonstrates (Bhopal, Seveso, Challenger, etc.), such catastrophic accidents damage the reputation, the image, and even the prosperity of the, institution responsible for the activity. (13:9)

3.7 Residual Risk.

The PM must know what residual risk exists in the system being acquired. For significant hazards, the PM is required to raise residual risk to higher levels of authority such as the Program Executive Officer or Air Force Acquisition Executive for action or acceptance. This requirement causes the contractor to document the actions taken within the scope of the contract. The PM may be able to apply additional resources or other remedies to help the contractor satisfactorily resolve the issue. If not, the PM can add his position to the contractors information and forward the matter to a higher decision level. Figure 3-7 is an example of a decision authority based on the hazard risk index.

Figure 3-7

EXAMPLE DECISION AUTHORITY MATRIX FOR RESIDUAL RISK

	FREQUENT	PERIODIC	OCCASIONAL	REMOTE	IMPROBABLE
CATASTROPHIC	HIGH	HIGH	HIGH	SERIOUS	MEDIUM
CRITICAL	HIGH	HIGH	SERIOUS	MEDIUM	MEDIUM
MARGINAL	SERIOUS	SERIOUS	MEDIUM	MEDIUM	LOW
NEGLIGIBLE	MEDIUM	MEDIUM	LOW	LOW	LOW

HAZARD RISK LEVEL	DECISION AUTHORITY
HIGH	COMPONENT ACQUISITION EXECUTIVE
SERIOUS	PROGRAM EXECUTIVE OFFICER
MEDIUM	PROGRAM MANAGER
LOW	ACCEPTABLE WITHOUT REVIEW

CHAPTER 4

SYSTEM SAFETY PROGRAM

4.1 System Safety Program Objectives and Requirements.

Employing good management and engineering principles is the heart of the system safety function. It is the system safety program that integrates all these efforts and ensures a minimum risk weapon system consistent with other program constraints. A system safety program consists of a system safety plan, various specific management tasks, several time-phased analyses, and periodic reviews and evaluations. Chapter 5 will discuss the system safety plan in detail. Chapter 6 outlines other management tasks. Chapter 7 reviews various analyses. Chapter 8 discusses the several assessment and verification tasks.

In this chapter, the system safety program will be discussed in general. Chapter 1 explained the need for system safety, and Chapter 2, DOD and Air Force policy and participants in system safety efforts. These efforts are the systematic, well-defined process called a system safety program. It is fundamentally a management process employing certain engineering tasks.

The principal objective of a system safety program within the DOD is to make sure safety, consistent with mission requirements, is designed into systems, subsystems, equipment, facilities, and their interfaces and operation. The degree of safety achieved in a system depends directly on management emphasis. Government agencies and contractors must apply management emphasis to safety during the system acquisition process and throughout the life cycle of each system, making sure mishap risk is understood and risk reduction is always considered in the management review process.

A formal safety program that stresses early hazard identification and elimination or reduction of associated risk to a level acceptable to the managing activity is the principal contribution of effective system safety. The success of the system safety effort depends on definitive statements of safety objectives and requirements.

Specific system safety program objectives are outlined in paragraph 1.2.

Specific time-phased requirements will be discussed in Chapter 10. General system safety program requirements are: (30:3)

a. Eliminate identified hazards or reduce associated risk through design, including material selection or substitution.

b. Isolate hazardous substances, components, and operations from other activities, areas, personnel, and incompatible materials.

c. Locate equipment so that access during operations, servicing, maintenance, repair, or adjustment minimizes personnel exposure to hazards.

d. Minimize risk resulting from excessive environmental conditions (e.g., temperature, pressure, noise, toxicity, acceleration, and vibration).

e. Design to minimize risk created by human error in the operation and support of the system.

f. Consider alternate approaches to minimize risk from hazards that cannot be eliminated. Such approaches include interlocks, redundancy, fail-safe design, fire suppression, and protective clothing, equipment, devices, and procedures.

g. Protect power sources, controls, and critical components of redundant subsystems by separation or shielding.

h. When alternate design approaches cannot eliminate the hazard, provide warning and caution notes in assembly, operations, maintenance, and repair instructions, and distinctive markings on hazardous components and materials, equipment, and facilities to ensure personnel and equipment protection. These shall be standardized in accordance with MA requirements.

i. Minimize the severity of personnel injury or damage to equipment in the event of a mishap.

j. Design software-controlled or monitored functions to minimize initiation of hazardous events or mishaps.

k. Review design criteria for inadequate or overly restrictive requirements regarding safety. Recommend new design criteria supported by study, analyses, or test data.

Management Responsibilities. System safety management (especially in the program office), in order to meet the objectives and requirements of system safety, must: (29:A1-A2)

a. Plan, organize, and implement an effective system safety program that is integrated into all life cycle phases.

b. Establish definitive system safety program requirements for the procurement or development of a system. The requirements must be set forth clearly in the appropriate system specifications and contractual documents.

c. Ensure that a system safety program plan (SSPP) is prepared that reflects in detail how the total program is to be conducted.

d. Review and approve for implementation the SSPPs prepared by the contractor.

e. Supply historical safety data as available.

f. Monitor contractors' system safety activities and review and approve deliverable data, if applicable, to ensure adequate performance and compliance with system safety requirements.

g. Ensure that the appropriate system specifications are updated to reflect results of analyses, tests, and evaluations.

h. Evaluate new design criteria for inclusion into military specifications and standards and submit recommendations to the respective responsible organization.

i. Establish system safety groups as appropriate to assist the program manager in developing and implementing a system safety program.

j. Establish work breakdown structure elements at appropriate levels for system safety management and engineering.

Management's Risk Review. The system safety program examines the interrelationships of all components of a program and its systems with the objective of bringing mishap risk or risk reduction into the management review process for automatic consideration in total program perspective. It involves the preparation and implementation of system safety plans; also, the performance of system safety analyses on both system design and operations, and risk assessments in support of both management and system engineering activities. The system safety activity provides the program manager with a means of identifying what the mishap risk is, where a mishap can be expected to occur, and what alternate routes the design may take. Most important, it verifies implementation and effectiveness of hazard control. What is generally not recognized in the system safety community is that there are no safety problems in system design. There are only engineering and management problems, which if left unresolved, can result in a mishap. When a mishap occurs, then it is a safety problem. Identification and control of mishap risk is an engineering and management function. Determining what went wrong is a function of the safety activity. (37:1-2)

System safety activity provides the program manager with an effective means of identifying what risk elements exist and evaluating their interrelationship to all elements of the program. These risk elements are most significant in the preventative mode and are detected by design analysis (i.e., determine where a mishap can be expected to occur and provide an alternate design approach) and corrected by design action to control, eliminate, or soften the effects of the resultant mishap. Most importantly, system safety activity verifies implementation and effectiveness of hazard control by the design hazard analysis process. An equally significant and beneficial element in the program life cycle is acquisition of empirical data and performance verification feedback. The operational hazard analysis provides an effective method, during the integrated operations life cycle, for initial and continuous monitoring and tracking as the program comes into its maturity. Also, the subsequent feedback can be used to validate design and development predictions; moreover, it creates an iterative process in failure prediction and the corrective action process toward prevention of an incident or mishap event. Through effective feedback, it is possible to learn from such an event and generate the capability to translate this knowledge to a similar program endeavor. (37:1-3)

An excellent summary of management function required for a system safety program is presented in Figure 4-1. Although written for contractor system safety efforts, it is a good review of the many government-required functions as well.

4.2 Program Balance.

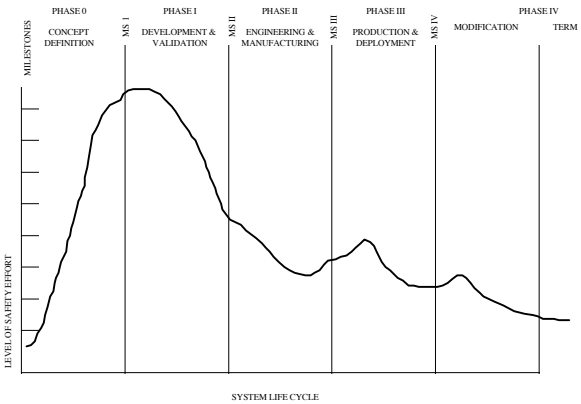
The system safety effort is an optimizing process that varies in scope and scale over the lifetime of the system. System safety program balance is the result of the interplay between system safety and the three very familiar basic program elements: cost, performance, and schedule. Without an acute awareness of the system safety balance on the part of both program management and the system safety manager, they cannot discuss when, where, and how much they can afford to spend on system safety. We cannot afford mishaps which will prevent the achievement of primary mission goals; nor can we afford systems which cannot perform because of overstated safety goals.

From the beginning of the program, the desired result is to have the safety pendulum balance, with safety placed in the proper perspective. Proper system safety balance cannot be achieved without clearly defining acceptable and unacceptable risks. This is the first task that needs to be completed. These acceptability parameters must be established early enough in the program to allow for selection of the optimum design or operational alternatives. For cost-effective mishap prevention, defining acceptable and unacceptable risk is as important as defining cost and performance parameters. (37:1-5)

Figure 4-2 graphically displays how the scale of effort varies with life cycle phase. (40:38) System safety is applied early in the life cycle, but some system safety efforts are required until and during system operations termination.

Figure 4-2

SYSTEM SAFETY LIFE CYCLE EFFORTS



System safety management applies the safety technology of all applicable safety disciplines to the development and utilization of a military system. During acquisition of a system, the system safety effort is focused on design engineering and system engineering. While planning for system safety is of major concern in the conceptual phase, the full application of system engineering principles in design is an integral part of the validation and full-scale development phases. For test operations and evaluation activities, the system safety function includes responsibilities for system, personnel, and environmental protection. Production and operational phases are approached with the concept that human error can void all standards incorporated by design. Effective planning to

implement the system safety task is commensurate with each phase of the total program. (28:21)

Figure 4-1

FUNCTIONS OF SAFETY ORGANIZATIONS

1. Ensure that company safety policies are carried out by all personnel concerned.

2. Develop guidance by which the safety program will be carried out during design, development, production, test, transportation, handling operation, maintenance, and repair.

3. Keep management informed on the safety program, its status, significant problems, deficiencies, or methods off improvement.

4. Review all safety requirements affecting the company product to ensure customer satisfaction. These requirements may be expressed in a contract, specification, federal or state law, transportation commission regulation, technical code, or good engineering practice. to focus attention on these safety requirements, the safety organization must know their contents, implications, and changes.

5. Review design reliability, maintenance, production test, quality assurance, transportation, human engineering, and training plans and criteria to ensure proper integration of safety activities into product development.

6. Are cognizant of new processes, materials, equipment, and information that might benefit the safety program. Recommend those safety developments that should be beneficial to the proper organization.

7. Analyze the product and its components to ensure that all hazards are eliminated or controlled to the greatest degree possible. Recommend containment measures to minimize damage that might result form an accident. Update analyses as development, testing and production proceed.

8. Review histories of hazards, failures, and mishaps In existing systems to ensure that design deficiencies are not repeated in the new system or product.

9. Participate in design preparations and reviews to ensure that incompatible or unsafe components, arrangements, subsystems, or procedures are not incorporated.

10. Participate in tradeoff studies to ensure that safety is not compromised by changes in mission, hardware, configuration, or procedures.

11. Monitor failure and incident reports to determine discrepancies, deficiencies, or trends that ,might affect safety. Take suitable recommendations for corrective action.

12. Prepare safety analyses required by the customer or his integrating contractor.

13. Determine the effects of overall safety of operations and failures of equipment being produced by associate contractors.

14. Develop safety analysis requirements , procedures, and milestones to be observed by subcontractors. ensure that they understand all aspects of the safety program, the requirements imposed, and how their date and analyses will be integrated in to the system effort.

15. Ensure that subcontractors safety analyses are prepared and submitted and that their items will not degrade the safety of the company's product

16. Ensure that safety training programs are adequate to meet organizational needs. Initiate action for improvements of such training.

17. Determine whether detection and warning devices, protective equipment, or emergency and rescue equipment are required for the system. Ensure that equipment selected is suitable for the specific hazard that might be encountered.

18. Ensure that safety warning and caution notes are incorporated in procedure, checklists, and manuals to warn personnel of hazardous conditions that might exist.

19. Disseminate information on hazards to other organizations that might be interested or affected.

20. Maintain liaison with safety organizations of the customer, associate contractors, subcontractors, other suppliers, consultants, and government safety agencies.

21. Serve on boards and committees dealing with industrial safety, bioenvironmental; engineering, human engineering, and related fields.

22. Develop investigation plans for any mishaps involving the product.

23. investigate mishaps involving the product while it is the responsibility of the company. Assist the user, at his request, in investigating mishaps that are the user's responsibility.

24. Ensure corrective action is taken to prevent recurrences of mishaps through similar deficiencies or practices.

Control of the foregoing process must be maintained through a disciplined documentation and review system. All pertinent details of the safety-critical aspects of any end item must be capable of being traced from the initial identification of the potential hazard to its ultimate control solution. The system engineering documents which control the system safety process are the system specifications, milestone/time lines, and operating procedures. Other supporting documentation, such as preliminary hazard analyses and subsystem hazard analyses, only identify the problems and the controls to be imposed. The actual control is within the specifications and procedures. (28:22)

System safety programs are conducted in accordance with a system safety plan. Control is achieved by contractual instruments to ensure that the agencies responsible for the design engineering effort are responsive to the requirements generated by the system safety process. Documentation of the analyses and results can be contractually enforceable to make sure that the engineering process is responsive to the engineering requirements and solutions proposed by the system safety function. (28:22)

The progress of the safety tasks is normally monitored by system safety participation in the contractually required program reviews, such as preliminary design review and critical design review. At these reviews, the results of hazard analyses should be discussed, including the identified safety-critical aspects of the system, the controlling criteria generated, and identification of the specification which contains the criteria. Progress of the system safety analysis should be reviewed, along with the identification of operational safety problems, when and where they exist, as well as the operational sequence which potentially initiates each hazard. (28:23)

4.3 Safety Interfaces.

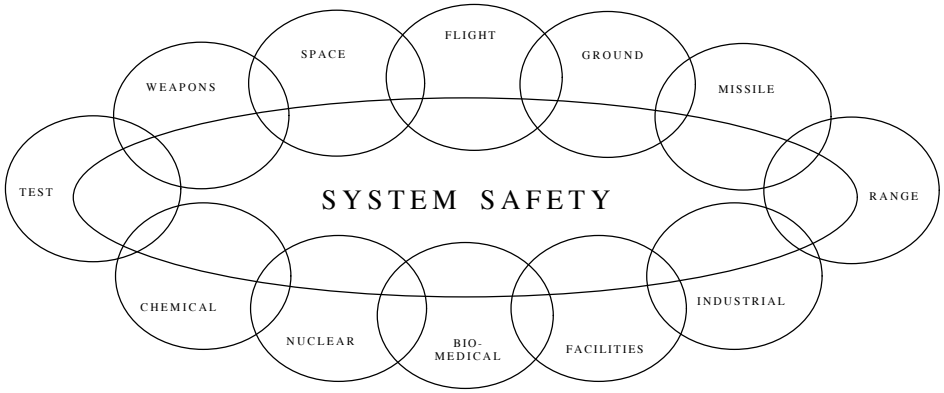
At the heart of the system safety management task is the requirement to integrate information from many sources to ensure effective risk management. These interfaces are both internal and external to the program office. Internal interfaces, those between different parts of the program office, are covered in detail in Chapter 11. The external interfaces discussed below are between program system safety personnel and others outside of the program office in safety disciplines. System safety is an integrator of the many other safety disciplines. See Figure 4-3. These disciplines are discussed in detail in Chapter 15 but are summarized below.

Operational safety includes flight, ground, and weapons safety. These safety disciplines have separate programs that guide the system user in safe operational procedures and practices and also provide a variety of feedback mechanisms of interest to system safety. Mishap investigations, hazardous situation reports, and materiel deficiency reports provide post-design hazard identification from the field. System safety efforts need to identify, through various system documents given to the user, the residual hazards of their systems and the procedures to control the risks presented by these hazards. Operational safety disciplines also help define system requirements and are an important part of the prioritization process for optimizing safety with other program constraints.

Nuclear safety is an integral part of all developmental, testing, and operational phases of components or systems containing or using radioactive materials. This includes nuclear weapon systems, nuclear power systems, systems using depleted uranium, radioactive sources in space, components which become radioactive during use, and future state-of-the-art development. As with all safety programs, nuclear safety must be considered in view of the total system and not just the component which is, or will become, radioactive. Therefore, nuclear safety must be considered as part of the overall risk assessment. Whenever a contractor, for the purpose of accomplishing assigned studies or tasks, proposes the use of radioactive material which requires specific licensing under the Atomic Energy Act of 1954 (as set forth in the Code of Federal Regulations, Title 10, Parts 20, 30, 40, and 70) or any other hazardous radioactive material, it is required that they identify safety considerations or problems arising as a result of these proposal and the possible impact on personnel, facilities, testing, maintenance, and transportation. If this isn't done, as with many other critical functions, launch or operational approval cannot be obtained. (37:8-1)

Figure 4-3

SAFETY-SYSTEM SAFETY INTERFACES



An explosive safety program encompasses all explosives safety criteria and actions necessary to prevent mishaps or to minimize damage. Implementation of this program requires compliance with all directives that control the design, development, test, production, transportation, handling, storage, and use of explosives. The term explosives includes all ammunition, munitions fillers, demolition material, solid rocket motors, liquid propellants, cartridges, pyrotechnics, mines, bombs, grenades, warheads of all types, explosive elements of ejection and aircrew egress systems, air-launched missiles and those explosive components of missile systems and space systems, and assembled kits and devices containing explosives material. Explosives, explosives weight, net weight, and other like terms also refer to the fillers of an explosive item. Fillers may be explosive mixtures, propellants, pyrotechnics, military chemicals, and other toxic substances. This term does not include liquid fuels and oxidizers that are not used with missiles, rockets, and other such weapons or explosive items. In general, explosives are used for "nonnuclear" applications, and the requirements of the Air Force Instructions 91-204 and AFJI 32-3002. (37:9-1)

The term biomedical, as used in the Air Force and in this manual, refers to physical and chemical agents which impact on the health and well being of humans. Chemical agents, which may have a negative effect on man, may be hazardous because of their toxic, corrosive, flammable, or reactive nature. Physical agents include all forms of sound and vibration, all forms of electromagnetic radiation, and all forms of particle radiation. The recognition, evaluation, and recommendations for control of biomedical hazards are the responsibility of bioenvironmental engineering. Air Force policy requires that the workplace be safe, healthful, free from recognized hazards and that pollution from weapon systems, operations, and other activities be controlled. This cannot be accomplished with passive avoidance of hazards but requires an aggressive effort beginning with the acquisition of all systems and continuing through the establishment of health and safety programs. (37:10-1)

Facility safety is used to verify safety criteria and interfaces between noncritical and safety-critical facilities. Support requirements for all safety-critical events during test, as well as during the operational phases, will be included. The system safety planning for facility acquisition is often over-looked. There is considerable lead time associated with facility construction. Therefore, it is essential that facility system safety requirements be defined at the earliest possible time. While facility development may appear to be relatively unimportant in comparison to the overall program, the lack of consideration for safety in facility design can seriously jeopardize the entire project. The Occupational Safety and Health Act will not permit contractor personnel to work in any area that does not meet some very basic safety requirements. In addition, handling and storage of dangerous materials in a facility requires certain design and operational planning for the conduct of these activities. Failure to plan in this area can cause extensive program delays and considerable additional cost. (37:3-24)

Missile systems range from ground-launched or air-launched systems to ICBMs and remotely piloted vehicles and drones. The aerospace vehicle is only a part of the mishap potential. Ground support and operational equipment, personnel, and the operational environment are also likely sources of mishaps. Safe operations within the missile environment are possible only if positive mishap prevention programs are established and faithfully followed. Some areas and equipment that missile safety addresses are: missile receipt and delivery areas; storage, handling, and maintenance facilities; transportation routes; mission and training facilities; and missile launch facilities and environments. (24:35)

Range safety for aeronautical systems is concerned with test operations on the range. Space systems have some unique range considerations. One results in the event of an accident during the ascent phase of flight, which would cause debris to impact in uncontrolled areas; the other results during the post-orbital flight phase, when the orbital hardware reenters and impacts in an uncontrolled area. The system safety engineer must consider the associated potential risks and responsibilities associated with these situations. Airborne operation requirements are a concern because of inherent dangers in missile and space vehicle flight operations. The general approach in obtaining airborne operation approval is the preparation of a flight plan approval request and supporting data. The supporting data package defines the proposed flight plan and flight hardware; the content of this submittal is specified in the respective range safety manuals. Additional information in the form of a flight safety hazards analysis may be required. This is generally the case when the proposed flight azimuth/trajectory is outside of the usual flight azimuth sector or a new launch vehicle is used. This hazard analysis addresses the risk to people and property, with the primary emphasis on the safety of the general public. (37:11-2)

4.4 Program Interfaces.

As seen in Figure 4-4, there are many program interfaces that interact with system safety. (38:3-2) Design engineers are obviously key players in the system safety effort. Design engineers are both the problem and solution to hazard control. They translate user requirements into system design and, as such, are required to optimize many often conflicting constraints. In doing so, they eliminate or mitigate known hazards but create unidentified hazards as well. System safety provides design engineers with safety requirements, validation and verification requirements, and advice and knowledge based on system safety's active interfacing with the many participants in the design and acquisition processes.

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 (distance or other measure) between failure or a failure rate. The failure mode, effects, and criticality analysis is an important document to system safety in identifying which failure modes and effects require further system safety analysis and review. (32:31)

Maintainability is the measure of the ease with which an item may be maintained and repaired. It is usually expressed as a mean time to repair. The system safety program ensures that safety-critical items and procedures have been identified and evaluated and receives maintenance-related information for the operations and support hazard analysis. (32:31)

Survivability is a general term used to describe a system's ability to avoid and/or withstand manmade damage-causing mechanisms. Within the area of vulnerability and susceptibility, the survivability and system safety disciplines share a goal of eliminating single-point failures and incorporating crashworthiness and emergency egress features. (32:31)

Figure 4-4

OTHER ENGINEERING ORGANIZATIONS INVOLVED IN SAFETY PROGRAMS

ORGANIZATION	NORMAL FUNCTIONS	SAFETY FUNCTIONS
Design Engineering	Prepares Equipment and system designs that will meet contractual specifications for performance and mission accomplishment.	Conduct analyses of most appropriate and safest designs and procedures. Ensures that safety requirements in end item specifications and codes are met. Incorporates safety requirements for subcontractors and vendors in company specifications and drawings.
Human (Factors) Engineering	Ensures optimal integration of man, machine, and environment.	Conducts analyses to ensure well being of personnel involved in equipment operation, maintenance, repair, testing, or other tasks in the proposed environment, especially to minimize fatigue and possible human error. Makes procedures analyses.
Reliability Engineering	Is concerned that equipment will operate successfully for specific periods under stipulated conditions.	Makes failure modes and effects analyses. Performs tests on parts and assemblies to establish failure modes and rates. Makes special studies and tests. Reviews trouble and failure reports, indicating any safety connotations.
Maintainability engineering	Ensures that hardware will be in suitable condition for successful accomplishment of its prescribed mission.	Ensures that system or equipment will be at design safety level by minimizing wear-out failures through replacement of failed items and by surveillance over possible degrading environments. Participates in analyzing proposed maintenance procedures for safety aspects.
Test Engineering	Conducts laboratory and field tests of parts, subassemblies, equipment, and systems to determine whether their performance meets contractual requirements.	Evaluates hardware and procedures to determine whether they are safe in operation, whether changes are required, or whether additional safeguards are necessary. Determines whether equipment has any dangerous characteristics or dangerous energy levels or failure modes. Evaluates effects of adverse environments on safety.
Product (Field) Support	Maintains liaison between customer and producing company.	Assists customer on safety problems encountered in the field. Constitutes the major channel for feedback of field information on performance, hazards, mishaps, and near misses.
Production Engineering	Determines most economical and best means of producing the product in accordance with approved designs.	Ensures that designed safety is not degraded by poor workmanship or unauthorized production process changes.
Industrial Engineering	Ensures that the company personnel are not injured nor company property damaged by accidents.	Provides advice and information on accident prevention measures for industrial processes and procedures that are similar to those in system operations.
Training	Is concerned with improving technical and managerial capabilities of all company personnel.	Ensures that personnel involved in system development, production, and operation are trained to levels necessary for safe accomplishment of their assigned tasks and can produce a safe system or product. Certifies workers on safety critical operations, especially for test operations.

Quality assurance establishes policies and procedures to identify and control critical item throughout the life cycle of a system. Thorough acceptance tests and service life surveillance efforts, safety-critical items are part of the overall system design tracked through manufacture, transportation, and maintenance to the user. (32:31)

Human factors engineering analyzes the system to identify physiological and psychological capabilities and limitations of all human interfaces. A variety of human factors inputs affect the way safety-critical items and tasks impact the production, employment, and maintenance of a system. Environmental factors that affect the man-machine interface are also investigated and safety issues identified. (32:31)

Testing is the gathering and summarizing of empirical system data under controlled conditions. It is a vital part of the verification process and validates the accomplishment of safety requirements. Testing may be at the level of laboratories or in development or operational test and evaluation efforts. Analytical modeling, such as computer simulations, may also be helpful. System safety may require special tests of safety requirements or analyze results from other tests for safety validation.

Product support is an area that looks at personnel and man-power factors of design. System safety ensures that these areas address concerns related to identified hazards and the procedures. Manning and training implications of hazards that are passed on to the user as a result of the design optimization process affect the operator and maintainer of the system.

Integrated logistics support employs a logistic management information (LMI) system according to MIL-PRF-49506, Logistics Management Information, and MIL-HDBK-502, Acquisition Logistics. to identify key support issues, including safety. An LMI is used for most acquisition programs Normally, Government LMI 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 LMI 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 LMI efforts.

(NOTE: Add the two new documents to the Bibliography)

4.5 Tailoring.

System safety programs are instituted as the result of contract negotiations. MIL-STD-882 was created to provide means for establishing or continuing system safety programs of varying sizes at each phase of system development. MIL-STD-882D itself is not intended to be tailored - it is specified as a complete document on a contract, (e.g., apply System safety according to MIL-STD-882D). Paragraph 4.1 of MIL-STD-882D specifies the essential steps for achieving a system safety program. These are:

a. Document the approach to be taken . This is similar to a system safety program plan but is usually submitted with a proposal. Note that MIL-STD-882D does not mention a separate deliverable SSPP. This documentation will describe both the developers's and the manager's approach to performing the efforts in the following sub-paragraphs.

b. Identify the hazards in the system using a systematic process. The choice of individual analyses will be left to the developer or contractor.

c. Assessment of mishap risk. Assess the severity and probability of the mishap risk associated with each identified hazard, i.e., determine the potential impact of the hazard on personnel, facilities, equipment, operations, the public, and the environment, as well as on the system itself.

d. Identification of mishap risk mitigation measures. Identify potential mishap risk mitigation alternatives and the expected effectiveness of each alternative or method. Mishap risk mitigation is an iterative process that culminates when the residual mishap risk has been reduced to a level acceptable to the appropriate authority.

e. Reduction of mishap risk to an acceptable level. Reduce the mishap risk through a mitigation approach mutually agreed to by both the developer and the program manager. Residual mishap risk and hazards shall be communicated to the associated test effort for verification.

f. Verification of mishap risk reduction. Verify the mishap risk reduction and mitigation through appropriate analysis, testing, or inspection. Document the determined residual mishap risk.

g. Review of hazards and acceptance of residual mishap risk by the appropriate authority. Notify the program manager of identified hazards and residual mishap risk. Unless otherwise specified, the suggested tables A-I through A-III of the MIL-STD-882D appendix will be used to rank residual risk. The program manager will ensure that remaining hazards and residual mishap risk are reviewed and accepted by the appropriate risk acceptance authority. The appropriate risk acceptance authority will include the system user in the mishap risk review. The appropriate risk acceptance authority will formally acknowledge and document acceptance of hazards and residual mishap risk.

h. Tracking of hazards, their closures, and residual mishap risk. Track hazards until closed. Track residual mishap risk throughout the system life cycle. The program manager shall keep the system user advised of the hazards and residual mishap risk.

These steps are intended to be used for all system safety programs for all acquisitions. The level of effort will vary as will the exact techniques to be used. The specific Tasks are no longer be part of MIL-STD-882, and they are not spelled out by the procuring activity. Instead, they can be used by the contractor as he/she sees fit to be the above requirements. The tasks are now reference documents and can be found in the DOD acquisition Deskbook. For ease of reference, the Deskbook Tasks use the same numbers as the tasks in MIL-STD-882C. Because they are reference documents, the Tasks can not be applied on contract by reference; however, portions of the Tasks can be extracted and be included in the contract if necessary.

A major challenge which confronts all government and industry organizations responsible for a system safety program is the selection of those tasks which can materially aid in attaining program safety requirements. Schedule and funding constraints mandate a cost-effective selection, one that is based on identified program needs. The considerations presented herein are intended to provide guidance and rationale for this selection. They are also intended to jog the memory for lessons learned to provoke questions which must be answered and to encourage dialogue with other engineers

and operations and support personnel so that answers to questions and solutions to problems can be found.

Once appropriate tasks have been selected, the tasks themselves must be tailored to fit the level of effort It is also important to coordinate tasks requirements with other engineering support groups, such as logistics support, reliability, etc., to eliminate duplication of tasks and to be aware of any additional information of value to system safety which these other groups can provide

The timing and depth required for each task, as well as action to be taken based on task outcome, are largely dependent on individual experience and program requirements. For these reasons, hard and fast rules are not stated. Figure 4-5 can be used as an initial guide to tailoring requirements.

Figure 4-5

APPLICATION MATRIX FOR SYSTEM PROGRAM DEVELOPMENT

TASK	TITLE	TASK TYPE	PHASE 0	PHASE I	PHASE II	PHASE III	PHASE IV
101	SYSTEM SAFETY PROGRAM	MGT	G	G	G	G	G
102	SYSTEM SAFETY PROGRAM PLAN	MGT	G	G	G	G	G
103	INTEGRATION OF ASSOCIATE CONTRACTORS, SUBCONTRACTORS AND AE FIRMS	MGT	S	S	S	S	S
104	SYSTEM SAFETY PROGRAM REVIEW/AUDITS	MGT	S	S	S	S	S
105	SSG/SSWG SUPPORT	MGT	G	G	G	G	G
106	HAZARD TRACKING AND RISK RESOLUTION	MGT	S	G	G	G	G
107	SYSTEMS SAFETY PROGRESS SUMMARY	MGT	G	G	G	G	G
201	PRELIMINARY HAZARD LIST	ENG	G	S	S	S	N/A
202	PRELIMINARY HAZARD ANALYSIS	ENG	G	G	G	GC	GC
203	REQUIREMENTS HAZARD ANALYSIS	ENG	G	S	S	S	GC
204	SUBSYSTEM HAZARD ANALYSIS	ENG	N/A	G	G	GC	GC
205	SYSTEM HAZARD ANALYSIS	ENG	N/A	G	G	GC	GC
206	OPERATING & SUPPORT HAZARD ANALYSIS	ENG	S	G	G	GC	GC
207	HEALTH HAZARD ANALYSIS	ENG	G	G	G	GC	GC
301	SAFETY ASSESSMENT	MGT	S	S	S	S	S
302	TEST AND EVALUATION SAFETY	MGT	G	G	G	G	G
303	SAFETY REVIEW OF ECPS & WAIVERS	MGT	N/A	G	G	G	G
401	SAFETY VERIFICATION	ENG	S	G	G	S	S
402	SAFETY COMPLIANCE ASSESSMENT						
403	EXPLOSIVES HAZARD CLASSIFICATION/ CHARACTERISTICS	MGT	S	S	S	S	S

NOTES

TASK TYPE

ENG - System Safety Eng
MGT - System Safety Mgt

PROGRAM PHASE

I - Concept Exploration
II - PDRR*
III - Eng/Manufacturing/Development
IV - Production/Deployment
V - Operations/Support

APPLICABILITY CODES

S - Selectively Applicable
G - Generally Applicable
GC - General Applicable to Design Changes Only
N/A - Not applicable

*Production Definition and Risk Reduction

4.6 Tailoring Checklists. (16:C-2 to C-4)

A guide to tailoring has been developed for both the customer (Air Force) and the contractor. The key to having an effective system safety program is to provide an approach which is appropriate to the particular product. To accomplish this goal, one must understand the product and what analyses in MIL-STD-882 will uncover the information necessary to ensure the safety of the product. At the very beginning of each task description in Deskbook, the task purpose is stated. It is extremely important to fully understand these purposes before attempting to apply any tasks. Figure 4-6 contains a checklist for applying individual system safety Tasks.

There are three basic steps to using the checklist with separate approaches depending on whether the person using the checklist is the customer or the contractor. As a customer, the first step is to formulate a wish list. The contractor would read through the contract documents to find what system

safety requirements have been imposed. The second step is to relate the requirements to the product complexity and program length. The third step may conflict with the ideal that safety is of prime importance and there should be no restraints on funding/manpower. However, contracts which do not take manpower into account, will most likely overburden the personnel involved. This is not to suggest that the system safety effort is of little importance. On the contrary, both the customer and the contractor want a safe product. However, the approach and methodology in achieving that goal can be varied.

Figure 4-6

TASK SELECTION CHECKLIST

CUSTOMER	CONTRACTOR
1. Determine everything you would like to have done (wish list).	1. Determine what is listed in all contract documents.
1A. Figure out what you want to learn and then decide which tasks will provide that information. Example: Knowledge of detail component failures (SSHA) or overall confirmation of continued compliance (safety compliance assessments), etc.	1A. Try to understand the depth/emphasis of customer requirements. What items are deliverable? What's required but not deliverable?
1B. Utilize MIL-STD-882, appendix b to aid in relating program requirements to life cycle phases.	1B. Do the requirements relate to the phase of the contract?
2. Ensure the requirements relate to product complexity and program length	2. Do the requirements relate to product complexity and program length?
2A. Understand the item(s) you are buying. Example: Whole airplane vs. small modification	2a> Understand the item(s) you are producing. Example: Whole airplane vs. small modification.
2B. Consider length of program. Is it practical to fit all requirements in this phase or cam some items be postponed to the next phase?	2B. Determine what you would need if you were the customer.
2C. Revise the wish list to relate to the product.	2C. Determine what it will take (man-hrs) to accomplish the given tasks. Is it possible to add or reduce depth in some areas?
3. Estimate the manpower I numbers and areas of expertise that are available to review and critique analyses and participate in the program.	3. Estimate the manpower in numbers and areas of expertise that are available to participate in the program.
3A. Determine who and how many people will be available to perform managing activity duties.	3A. Determine who and how many people will be available to perform tasks.
3B. Are available personnel qualified to monitor/ evaluate contractor? (Especially in area of software.)	3B. Are available personnel qualified to perform tasks
3C. Delete/scale-down/simplify tasks to relate to personnel available.	3C. Tailor requirements in the plan (or memorandum of understanding) based on personnel availability and qualifications.

After using the checklist, there are some hints that may be helpful in selecting Tasks. For the customer, it is often better to time safety analyses deliverables based upon significant program milestones (like a preliminary design review) than to specify a certain number of days after contract award. This allows greater flexibility in case the design schedule changes. Whenever practical, consider requesting an update to an existing report instead of a whole new report. This can be a cost saver. If uncertainties exist in design which make a difference in what analysis is requested (ex. unsure if flight controls will be fly-by-wire or mechanical), leave the option to decide after the program has progressed. An example would be to add to the statement of work to perform fault tree analysis on a set number of topics mutually agreed upon at the system safety working group. Contractors should be particularly careful with contracts that require many analyses but few deliverables. It is especially important to keep an orderly backup file of all information that was used to support the deliverables. This file should be made available to the customer for review. This checklist can form part of a substantiation for additional budget or could surface areas for renegotiating or trading of tasks. Both customer and contractor can go beyond just identifying the particular MIL-STD-882 tasks.

4.7 Abuses. (16:C-1 to C-2)

Various abuses to the process are noteworthy, such as boilerplate, smorgasbord, invisible, and cutup tailoring.

The boilerplate utilizes verbiage that has been used numerous times before. It references the original MIL-STD-882, not the current version. Defenders of this method claim it is “proven effective” and has “management approval.” New start programs should use the latest version. It may be valuable as a method of time savings to utilize similar requirements from previous similar programs; however, it is often used for all programs regardless of similarities.

The smorgasbord contains practically everything in MIL-STD--882. Many times, there is a long list of tasks with only a few deliverables. The theory behind this is if a little bit of 882 is good to have, a lot must be better. This burdens the contractor to programs; however, it is often used for all programs regardless of similarities.

The smorgasbord contains practically everything in MIL-STD--882. Many times, there is a long list of tasks with only a few deliverables. The theory behind this is if a little bit of 882 is good to have, a lot must be better. This burdens the contractor to produce a lot of programs; however, it is often used for all programs regardless of similarities.

The smorgasbord contains practically everything in MIL-STD--882. Many times, there is a long list of tasks with only a few deliverables. The theory behind this is if a little bit of 882 is good to have, a lot must be better. This burdens the contractor to This method suggests the customer views safety as a spectator sport. Customer involvement is essential to success. The application of MIL-STD-882D as a whole document should prevent this from occurring.

Invisible tailoring of tasks is accomplished by omitting the very last paragraph of each task. This paragraph describes what the managing authority shall do. This is of no concern to the contractor. So, it is as if this task were never tailored. This misses the whole point of tailoring.

Cutup contracts are ones which bear little resemblance to the original input by the customer’s safety department because it was “revised” before final transmittal to the contractor. Unfortunately, the contractor will have to work with the customer’s safety department and try to satisfy their original needs without exceeding the bounds of the actual content.

4.8 Small Programs. (33:123-132)

A major program may need most or all of the tasks in Deskbook applied to the program. Small programs are much different. There is a need for the further delineation of a set of recommended procedures for conducting a small system safety program. Such a program may be called for in such cases as small projects (e.g., the design and fabrication of a missile transport cart), projects with obviously minimal hazards (e.g., development of a new mechanical typewriter), projects that do not fit into the normal life cycle process (e.g., military facilities design and construction) and, unfortunately, projects for which the safety activity is dollar limited.

The following are recommended as a minimum effort in a system safety program:

1. Prepare a preliminary hazards list (PHL).
2. Conduct a preliminary hazard analysis (PHA).
3. Assign a Risk Assessment Value for each item.
4. Assign a priority for taking the recommended action to eliminate or control the hazards, according to the Risk Assessment Values.
5. Evaluate the possibility of deleterious effects from interfaces between the recommended actions and other portions of the system.
6. Take the recommended actions to modify the system.
7. Prepare a System Safety Assessment Report as a wrap-up of the system safety program.

The PHL can be derived in several ways. One of these is by the examination of the energy transfer in the system. This is based on the concept that all losses are created by an interference with the normal exchange of energy. The system is examined for incorrect, untimely, or omitted energy exchanges as a base for the PHL. There are also available hazard review checklists in which hazards are listed, together with the usual occurrence mode, the possible cause and the possible effects.

The PHA is the initial development of the relationships between hazard causes (faults), effects, and recommended actions to be taken to eliminate or control the hazards.

An in-depth hazard analysis generally follows the PHA with a subsystem hazard analysis, a system hazard analysis, and an operating and support hazard analysis, as appropriate, but for a small safety program, the PHA will usually suffice as the only formal analysis.

A comprehensive evaluation is needed of the safety risks being assumed prior to test or evaluation of the system or at contract completion. It identifies all safety features of the hardware and system design and procedural hazards that may be present in the system being acquired and specific procedural controls and precautions that should be followed.

It is to be remembered that the hazards encountered in a small program can be as severe and as likely to occur as those of a major program. Usually one can expect fewer hazards in a small program. Caution needs to be exerted to ensure that in tailoring the system safety effort to fit a small program, one does not perform a wholesale slashing, but

instead uses the tailoring process to obtain the optimum safety in the optimum system.

4.9 Government-Furnished Equipment.

As part of a system acquisition effort, equipment may be specified by the government as part of the contract as providing necessary inputs or receiving outputs from the system being developed. This government-furnished equipment (GFE) must be analyzed for its interface with the new system, if such analysis hasn't been previously accomplished in sufficient detail. The analysis was once considered a separate MIL-STD-882 task. However, GFE is now considered a part of the overall system and is analyzed as necessary as part of the overall systems analyses. The contract, therefore, must for GFE:

a. If hazard data are available, identify the system safety analyses needed and when they are needed.
b. Identify and perform any additional system safety analyses needed for interfaces between GFE and the rest of the system. (29:213-1)

Usually, GFE has been in the military inventory long enough that unsatisfactory operating characteristics are well known or have been identified in previous hazard analyses. The SPO should identify these unsatisfactory characteristics or provide the analyses, if available, to the contractor, who will then compensate for these characteristics by using their interface design. However, some GFE may predate system safety concepts, adequate safety analyses may not have been done, or unsatisfactory operating characteristics of a new or modified system may not be known. Then, the contractor or the Air Force must do the necessary analyses for proper interface design. (27:5)

4.10 Commercial and Nondevelopmental Items.

Commercial items, or "off-the-shelf" equipment, are commercially developed systems already being marketed publicly. Non-development items are systems that have been procured previously for other branches of the federal government, a state government, or for some foreign governments. By buying non-developmental items or off-the-shelf commercial equipment, the Air Force can save on development costs but can cause you some problems. As with GFE, the amount of attention required will vary, depending on the history and documentation available. Whether a subsystem (radio) or system (aircraft), the manufacturer should have done some type of failure mode analysis for their item. If the off-the-shelf equipment is used in a contractor-developed system, failure mode analysis, if well prepared, should be sufficient to allow the contractor to incorporate system safety in their design. For off-the-shelf equipment, or equipment with poorly prepared analyses, risk assessment gets trickier, especially if the equipment meets commercial safety requirements but has not been proven to meet all Air Force requirements. (27:5)

While the off-the-shelf concept provides significant up-front cost and schedule benefits, major concern centers on ensuring adequate levels of safety and supportability. For the Air Force to benefit fully from off-the-shelf acquisitions, the system safety program must be able to ensure the operational safety of the final system without adding unnecessarily to its acquisition cost through extensive analysis efforts or signif icant modifications. DOD 5000.2-R, discusses commercial items and nondevelopmental items, their intended use, and requirements and procedures for safe, cost-effective use consistent with mission requirements.

In theory, FAA-certified passenger and cargo aircraft should be safe for similar roles in the Air Force. However, the Air Force Safety Agency conducted safety reviews of several off-the-shelf aircraft acquisitions and discovered problem areas:

- AF training schedules require multiple touch-and-go landings.
- AF tends to operate aircraft closer to their design limits; i.e., loads, speed, T/O run, landing, etc.
- AF often modifies aircraft to a large extent.

Some off-the-shelf aircraft manufacturers do not have system safety programs/staffs that can analyze these changes for their effect on the system and report the results as required of normal AF aircraft acquisitions. The end result is that the AF buys an aircraft configuration that was not fully FAA certified and uses it in a manner not totally analogous to the civilian usage on which its original safety record was based. It is safe to assume that neither the requirement for nor the effects of these necessary changes has been fully appreciated before the decision to acquire a given "off-the-shelf" aircraft.

The safety lessons learned from a safety survey by AFSC of off-the-shelf AF acquisition are:

- The AF needs to establish minimum requirements for up-front mission/usage analysis to define any differences and their potential safety impact on the system.
- The AF needs to tell the bidding contractors what is required in the area of system safety analysis of Air Force-unique configuration/operations.
- Once operational, the AF needs to restrict these aircraft to the missions intended unless in-depth analysis is done to assess the effects of new missions. (Ref 43)

Program size and procurement schedules may severely limit the scope of the system safety program and require skillful, creative tailoring for the program. A small program may only require Tasks 101 and 301, while the MA could add Tasks 102, 105, and 203 for larger programs. The following are additional considerations(30:B-10):

Market Investigation. It is suggested that the MA conduct a market investigation to determine, among other things, to which safety or other appropriate standards the system was designed. The MA must determine the extent to which the system is certified by agencies such as the FAA, Underwriters Labs, etc. and what those certifications mean when compared to mission requirements. Some basic questions in the market investigation include:

a. Has the system been designed and built to meet applicable/any safety standards? Which ones?
b. Have any hazard analyses been performed? Request copies.
c. What is the mishap history for the system? Request specifics.
d. Is protective equipment and/or procedures needed during operation, maintenance, storage, or transport. Request specifics.
e. Does the system contain or use any hazardous materials, have potentially hazardous emissions, or generate hazardous waste?
f. Are special licenses or certificates required to own, store, or use the system?

Hazard Assessment. A safety assessment (Task 301) or safety compliance assessment (Task 402) report may be all that is necessary or available to gather detailed hazard information concerning an NDI program. If the selected system must be modified to meet mission requirements, other hazard analyses may be required, especially if the modifications are not otherwise covered. The full analysis uses Task 202, 204 or 205, and possibly 206 or 207.

System Safety Groups. Requiring a system safety group meeting early in the program will help clarify system characteristics versus mission requirements and allow time to address issues. An additional SSG can be used to assure satisfactory closure of issues and smooth fielding of the system. Periodic SSGs through the remainder of the life cycle can be used to address on going concerns and special issues.

CHAPTER 5

SYSTEM SAFETY PROGRAM PLAN (SSPP)

5.1 SSPP--Task 102. (Note: Task numbers came from MIL-STD-882C and are continued in the DoD Deskbook acquisition tool)

The SSPP is a basic tool used by the MA to assist in managing an effective system safety program. It can be used to evaluate the various contractors' approaches to, understanding of, and execution of their system safety tasks, their depth of planning to make sure their procedures for implementing and controlling system safety tasks are adequate, and their organizational structure to make sure appropriate attention will be focused on system safety activities. (30:A-8)

The purpose of the Task 102 is to develop an SSPP. MIL-STD-882D does not mention a specific SSPP. Instead, it requires documentation of an overall approach to achieving system safety objectives. Task 102 is no longer called out in the standard, but has been placed in the DOD Deskbook reference tool as a guide. Its principles still apply to current system safety efforts, so it is covered in this handbook. The task describes in detail the tasks and activities of system safety management and system safety engineering required to identify, evaluate, and eliminate hazards, or reduce the associated risk to a level acceptable to the MA throughout the system life cycle. An SSPP provides a basis of understanding between the contractor and the MA as to how the system safety program will be accomplished to meet contractual safety requirements included in the general and special provisions of the contract. (30:102-1)

Proper preparation of an SSPP requires coming to grips with the hard realities of program execution. It involves the examination and reexamination of anticipated problems and establishing a management system which will ensure effective solutions. The program offices specifies the system safety planning requirements by the inclusion of MIL-STD-882 in contracts. The plan can be either developed by the program managing activity or as a contractor requirement. The contractor-prepared plan, submitted normally with the proposal, describes the contractor's approach to implementation of the requirements specified on the contract.. The plan is prepared to reflect an integrated program management and engineering effort. It includes details of those methods the contractor uses to implement each system safety task described by the statement of work and by those documents listed for compliance. The plan defines all requirements to perform the system safety task, including all appropriate related tasks and complete breakdown of all system safety tasks, subtasks, and resource allocations for each program element through the term of the contract. A basic plan is required at program initiation (prior to milestone 0) to identify system safety mission element needs for existing or projected capability. This will aid in identifying opportunities to improve mission capability and reduction of life-cycle costs. The plan will be updated at the beginning of each subsequent program phase to describe the tasks and responsibilities for the following phase. (37:3-9)

Never apply a plan prepared by one contractor to the contract of another. Each plan is unique to the corporate personality and management system. The plan is prepared so that it describes a system safety approach and involves system safety in all appropriate program activities. It also describes the contractor's approach in defining the critical tasks leading to system safety certification. The plan describes methods by which critical safety problems are brought to the attention of program management and for management approval of close-out action. (37:3-9)

The plan should describe an organization with a system safety manager who is directly accountable to the program manager as his agent for system safety. This agent must not be organizationally inhibited from assigning action to any level of program management. The plan describes methods by which critical safety problems are brought to the attention of program management and for management approval of close-out action. Organizations which show accountability through lower management levels are ineffective, therefore, are unacceptable. (37:3-9)

This chapter discusses the significant information necessary for an effective SSPP. Specific contractual direction for the system safety program is contained in MIL-STD-882, while the format for presenting that program is directed by Data Item Descriptions (DI-SAFT-80102 to DI-SAFT-80106). It is important to understand that each data item explains the minimum level of information to be delivered to the government and describes the format for presenting it. The MIL-Standard levies the minimum performance requirements on the contractor. The discussions that follow are meant to give an understanding of the importance of required information, not to describe the specific information. (37:3-10)

The SSPP is normally valid for a specific period of time. This time period is associated with a particular phase of the system life cycle because separate contracts are awarded as development of equipment proceeds through each phase of the life cycle. For example, a contract is awarded to develop a prototype during the validation phase, another contract is awarded to develop hardware and software during full-scale engineering development, and still another contract is awarded when the equipment enters the production phase. Progressing from one phase of the life cycle to the next, the new contract may specify that the SSPP prepared from the former contract simply be revised to meet the requirements of the new contract. (32:44)

5.2 Program Scope.

Each SSPP shall describe, as a minimum, the four elements of an effective system safety program: a planned approach for task accomplishment, qualified people to accomplish tasks, authority to implement tasks through all levels of management, and appropriate resources, both manning and funding, to assure tasks are completed. The SSPP should define a program to satisfy the system safety requirements imposed by the contract. (30:1)

Each plan should contain a systematic, detailed description of the scope and magnitude of the overall system safety task. This includes a breakdown of the project by organizational component, safety tasks, subtasks, events, and responsibilities of each organizational element, including resource allocations and the contractor's estimate of the level

of effort necessary to effectively accomplish the contractual task. It is helpful to the evaluator if this section contains a matrix identifying applicable proposal sections which have been allotted resources to implement the system safety task and describes how these

resources are controlled by the system safety manager. The referenced proposal task should describe how the system safetytasks associated with the function will be implemented and monitored. (37:3-10)

For management purposes, with the listing of each document applicable to the system safety effort, list those functions within the contractor's organization which have the responsibility for assuring that the requirements in each compliance document are met. . Those responsible for using, implementing the information in applicable documents, or complying with their provisions must be clearly identified for effective planning. (37:3-10)

5.3 System Safety Organization. (30:102-1)

The SSPP describes:

a. The system safety organization or function within the organization of the total program using charts to show the organizational and functional relationships and lines of communication.
b. The responsibility and authority of system safety personnel, other contractor organizational elements involved in the system safety effort, subcontractors, and system safety groups. Identify the organizational unit responsible for executing each task. Identify the authority in regard to resolution of all identified hazards. Include the name, address, and telephone number of the system safety program manager.
c. The staffing of the system safety organization for the duration of the contract to include manpower loading, control of resources, and the qualifications of key system safety personnel assigned, including those who possess coordination/approval authority for contractor-prepared documentation.
d. The procedures by which the contractor will integrate and coordinate the system safety efforts, including assignment of the system safety requirements to action organizations and subcontractors, coordination of subcontractor system safety programs, integration of hazard analyses, program and design reviews, program status reporting, and system safety groups.
e. The process through which contractor management decisions will be made, including timely notification of unacceptable risks, necessary action, mishaps or malfunctions, waivers to safety requirements, program deviations, etc. (30:102-2)

Internal control for the proper implementation of system safety requirements and criteria affecting hardware, operational resources, and personnel are the responsibility of the system safety managers through their interface with other program disciplines. The program system safety manager is responsible for initiation of required action whenever internal coordination of controls fail in the resolution of problems. System safety responsibilities are an inherent part of every program function and task. Resolution and action relating to system safety matters will be affected at the organizational level possessing resolution authority. For this reason, the system safety program must be integrated into the total management and engineering effort. The contractor must provide a description of a system safety function with centralized mishap risk management authority, as the agent of the program manager, to maintain a continuous overview of the technical and planning aspects of the total program. While the specific organizational assignment of this function is a bidders' responsibility, to be acceptable the plan must show a direct accountability to the program manager with unrestricted access to any level of management. (37:3-10 to 3-11)

The program directors are responsible for all decisions relating to the conduct and implementation of their system safety program; it is expected that they will hold each element manager fully accountable for the implementation of safety requirements in their respective area of responsibility. The system safety manager must be responsible to the program director for the implementation of the total mishap prevention program. (37:3-11)

In the normal performance of their duties, system safety program managers must have direct approval authority over any safety-critical program documentation, design, procedures, or procedural operation or rejection if it does not meet minimum safety standards. A log of nondeliverable data can be maintained showing all program documentation reviewed, concurrence or nonoccurrence, reasons why the system safety engineer concurs or nonconcurs and actions taken as a result of nonoccurrence. The program office system safety manager should periodically review this log to monitor program progress. The task breakdown and manning necessary to support the program through the term of the contract will be contained in this section. For full application of the MIL-Standard program, including integration tasks, it is expected that contractor hours assigned for the system safety task could be within a range of 5 to 7 percent of engineering resources assigned to the program. More or less time will be required depending upon system complexity and how the standard is tailored. The contractor is required to assign a system safety manager who meets specific educational and professional requirements and who has had significant, full--time assignments in the professional practice of system safety. For major programs, consider (it's not absolute) a registered professional engineer with no less than 6 years of full-time assignments in the implementation of system safety programs or functional tasks. On approval of the contractor's specific request, 3 additional years of full-time assignments may be substituted for educational requirements. Substitution of the professional recognition is acceptable providing equivalent professional recognition shown such as recognition by the Board of Certified Safety Professionals as a Certified System Safety professional. In any case, assignment as a contractor system safety manager requires significant system safety experience. (37:3-11)

5.4 Program Milestones.

The SSPP should:

a. Define system safety program milestones.
b. Provide a program schedule of safety tasks, including start and completion dates, reports, reviews, and estimated manpower loading.
c. Identify integrated system safety activities (i.e., design analysis, tests, and demonstration) applicable to the system safety program but specified in other engineering studies to preclude duplication. Included in this section shall be the estimated manpower to do these tasks. (30:102-2)

This section of the plan contains the scheduled start and completion dates of tasks or events affecting the safety program, the paragraph within the plan that contains reference to the task, action responsibility, procedures or input required, and final results to be reviewed when the task or event is complete. Each task will be listed. Evaluation of safety program progress must be made at critical checkpoints. The milestone chart, like other tools, forces the contractor to organize his effort and plan it. If he can present that effort graphically, in a logical manner, you can assume that he has studied the requirements to some degree. If the chart is done properly you can tell just how well the contractor understands the requirements and how they are interrelated. If a progressive manloading chart is included as part of the milestone chart, you can tell how well the contractor understands the scope and flow of the effort as well. (37:3-12)

5.5 Requirements and Criteria.

The SSPP should:

a. Describe general engineering requirements and design criteria for safety. Describe safety requirements for support equipment and operational safety requirements for all appropriate phases of the life cycle up to, and including, disposal. List the safety standards and system specifications containing safety requirements that shall be complied with by the contractor. Include titles, dates, and where applicable, paragraph numbers.

b. Describe the risk assessment procedures. The hazard severity categories, hazard probability levels, and the system safety precedence that shall be followed to satisfy the safety requirements of this standard. State any qualitative or quantitative measures of safety to be used for risk assessment, including a description of the acceptable risk level. Include system safety definitions which deviate from or are in addition to those in this standard.

c. Describe closed-loop procedures for taking action to resolve identified hazards, including those involving GFE and off-the-shelf equipment. (30:102-2)

The contractor must have a method of identifying potential hazards in the program. Once identified, he must be able to categorize and prioritize those hazards for corrective action. Many of those methods and procedures are specified in the military standards. Discussion of the requirements and how they will be implemented and controlled gives you a picture of how well your contractor understands the task and how effectively he has planned to accomplish it. (37:3-19)

The system safety program is planned and implemented in a manner which will produce all design safety criteria and standards on which design judgments or decisions may be based. The system is analyzed to ensure that all of the established criteria have been interpreted correctly and applied effectively. (37:3-19)

System safety standards and criteria are extracted from program-applicable documents, handbooks, manuals, and regulations, and those specified by an approval agency. From these documents, the contractor will establish a safety basis for system design. Design principles, as applied to a specific program, reflect the lessons learned from Air Force or industry technical experience in the design and operation of similar type systems or systems containing similar hazards. (37:3-19)

The only effective method open to the system safety engineer for assuring a safe design in a cost-effective manner is to include safety requirements or criteria in each safety-critical CI specification. Safety requirements and safety verification criteria must be included in those portions of specifications specifically reserved for safety. Safety design requirements appear in section 3, paragraph 3.3.6, and their respective verification criteria in section 4. (37:3-19)

5.6 Hazard Analyses.

The SSPP should describe:

a. 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.

b. The depth within the system to which each technique is used, including hazard identification associated with the system, subsystem, components, personnel, ground support equipment, GFE, facilities, and their interrelationship in the logistic support, training, maintenance, and operational environments.

c. The integration of subcontractor hazard analyses with overall system hazard analyses. (30:102-3)

Analysis is the means of identifying hazards. A sound analytical approach is a must if the end product is to be worth anything. The wrong analytical approach will be evident from the contractor's discussion in the SSPP. Once the analysis is performed, it must be presented in a methodical manner. (37:3-20)

Each program is required to assess the mishap risk of the basic design concept as it relates to major injury to personnel and damage to equipment. The result of this assessment is a definition of those factors and conditions that present unacceptable accident/mishap risk throughout the program. This definition provides a program baseline for formulation of design criteria and assessment of the adequacy of its application through systems analysis, design reviews, operation planning, and operation analysis. System safety analyses are accomplished by various methods. Initially, however, the basic safety philosophy and design goals must be established prior to initiation of any program analysis task. Without this advanced planning, the system safety program becomes a random identification of hazards resulting in operational warnings and cautions instead of design correction. Therefore, the plan is used to describe methods to be used to perform system safety analyses. The methods may be quantitative, qualitative, inductive, or deductive but must produce results consistent with mission goals. (37:3-20)

The system safety plan should describe proposed actions which will initiate design change or safety trade studies when safety analyses indicate such action is necessary. Specify criteria for safety philosophy will guide trade studies or design changes. Whenever a management decision is necessary, an assessment of the risk is presented so that all facts can be weighed for a proposed decision. There are many documented cases where monetary considerations were presented as design drivers without proper risk assessment. Consequently, mishap costs far exceeded the savings. Include the requirement for the responsible activity, within the contractor organization, to review and approve the results of trade studies to assure that the intent of the original design

criteria is met. The contractor system safety engineers are required to be involved in all trade studies to establish a baseline and determine program impact of safety changes to be made as a result of safety tradeoff analysis. Reference should be made, by CDRL or contractor's identification number, to specific paragraphs of the contractor's proposal to verify or amplify this information. (53:3-20 to 3-21)

This section of the SSPP describes in detail the activities which will identify the impact of changes and modifications to the mishap or mishap potential of existing systems. All changes or modifications to existing systems will be analyzed for impact on the mishap risk baseline established by the basic system safety analysis effort. The results will be included for review as a part of each engineering change proposal. (37:3-21)

5.7 Safety Data. (37:3-20)

The program plan normally will illustrate the basic data flow which will provide a continuous overview of contractor organizational safety efforts. It will show how the system safety organization makes certain that contractually required submittal documents contain adequate safety inputs. This paragraph should contain system safety tasks, CDRL requirements having safety significance but no specific safety reference, and the requirement for a contractor system safety data file. The data in the file is not deliverable but is to be made available for procuring activity review on request. (53:3-21)

5.8 Safety Verification. (30:102-3)

The SSPP should describe:

a. The verification (test, analysis, inspection, etc.) requirements for making sure that safety is adequately demonstrated. Identify any certification requirements for safety devices or other special safety features.

b. Procedures for making sure test information is transmitted to the MA for review and analysis.

c. Procedure for ensuring the safe conduct of all tests.

5.9 Audit Program. (32:48)

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

5.10 Training. (32:48)

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

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

5.11 Mishap Reporting. (32:48)

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

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

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

5.12 Interfaces. (32:48)

Since the conduct of a system safety program will eventually touch on virtually every other element of a system development program, a concerted effort must be made to effectively integrate support activities. Each engineering and management discipline often pursues its own objectives independently, or at best, in coordination only with mainstream program activities such as design engineering and testing.

To ensure that the system safety program for a development program is comprehensive, the contractor must impose requirements on subcontractors and suppliers that are consistent with and contribute to the overall system safety program. This part of the SSPP must show the contractor's procedures for accomplishing this task. The prime contractor must evaluate variations and specify clear requirements tailored to the needs of the system safety program. Occasionally, the government procures subsystems or components under separate contracts to be integrated into an overall system. Each subsystem contract should include implementation of a system safety program.

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

The government system safety manager should be aware that the prime contractor is not always responsible for integration of the system safety program. For example, in some major system developments, the government is the system safety program integrator for several associate contractors.

5.13 SSPP Authorship. (27:11)

The SSPP may be written by either the contractor in response to an RFP or by the government as part of the RFP. Every acquisition program should have and follow a good SSPP. You may choose to require the contractor to write it or you may write it yourself. In either case, the system safety

program tasking should be sufficiently detailed so the contractor will have enough information to write the SSPP or will not be surprised by new or additional requirements in the government-written SSPP.

A good contractor-written SSPP depends on you carefully and completely specifying exactly what you want..

a. Advantages of a Contractor SSPP:

(1) Proposal discussions and planning for the contractor system safety program can be evaluated before contractor selection.

(2) The contractor assumes major responsibility for the system safety program. Thus, the contractor's incentive for a strong system safety program increases

.

(3) The contractor has more staff to get the job done. In the early stages of a program, you will be busy with contracting chores, source selections, and other elements and will not have a lot of spare time.

(4) From a contractor-written SSPP, you will get a good indication how well the contractor understands and can meet your program's safety requirements.

b. Disadvantages of a Contractor SSPP:

(1) A contractor-written SSPP might only restates what is written in the RFP and might lack sufficient detail to define the system safety program.

(2) It may take considerable time to get a satisfactory SSPP due to the time required for the contractor to submit a proposed SSPP to the government for disapproval or approval, for the government to review, and for the contractor to resubmit the SSPP.

(3) Contractor-written SSPPs cost money.

c. Advantages of a Government SSPP. A government-prepared SSPP released with the RFP does the following:

(1) Defines the minimum system safety program acceptable to the government. The contractor can then accurately bid this effort.

(2) Saves the amount of time needed to prepare a contractor-written SSPP and get it approved.

(3) Forces the government, before contract award, to agree on what constitutes an acceptable safety effort.

(4) Saves money the contractor would spend preparing and updating the SSPP.

d. Disadvantages of a Government SSPP.

(1) The government must assume responsibility for the system safety program.

(2) Your office must have adequate staff or your local staff safety office must be able to provide sufficient support to assume the task of writing the SSPP.

CHAPTER 6

OTHER MANAGEMENT TASKS (Ref 30)

6.1 Tasks List. (Note: Task numbers came from MIL-STD-882C and are continued in the DoD Deskbook acquisition tool)

The system safety program plan is a first and necessary task for an effective system safety effort. However, other management actions are sometimes required and, therefore, may be specified in MIL-STD-882. These tasks are:

Task 103--Contractor Integration

Task 104--Program Reviews

Task 105--System Safety Groups/System Safety Work Groups

Task 106--Hazard Tracking/Risk Resolution

Task 107--System Safety Progress Summary

This chapter extracts key information concerning these tasks .

6.2 Task 103--Contractor Integration.

Major programs or construction projects will often have multiple associate contractors, integrating contractors, and architect and engineering (AE) firms under contract. An integrating contractor or a facilities acquisition contractor will often have the responsibility to oversee system safety efforts of associate contractors or AE firms. Task 103 provides the authority for management surveillance needed by the integrating or facilities acquisition contractor by assigning the various system safety roles of associate contractors, subcontractors, integrators, and construction firms. The integrator should be tasked to write an integrated system safety program plan (ISSPP) according to the requirements outlined in Task 102. The integrator and construction contractor should be tasked to perform system hazard analyses and assessments to cover the interfaces between the various contractors' portions of the system or construction effort. All contractors and AE firms should be made aware of the integrator's or facilities acquisition contractor's role of overall system safety management. The integrator needs to resolve differences between associates in safety-related areas. The MA will aid the integrator in these efforts to make sure all contractors and firms mutually understand the system safety requirements and their respective responsibilities to comply with them.

The contractor designated as integrator for the safety functions of all associated contractors may (as defined in the contract):

a. Prepare an ISSPP as the SSPP required by Task 101 defining the role of the integrator and the effort required from each associate contractor to help integrate system safety requirements for the total system. In addition to the other contractually imposed requirements from MIL-STD-882, the plan may address and identify:

   (1) Definitions of where the control, authority, and responsibility transitions from the integrating contractor to the subcontractors and associates.
   (2) Analyses, risk assessment, and verification data to be developed by each associate contractor with format and method to be utilized.
   (3) Data each associate contractor is required to submit to the integrator and its scheduled delivery keyed to program milestones.
   (4) Schedule and other information considered pertinent by the integrator.
   (5) The method of development of system-level requirements to be allocated to each of the associate contractors as a part of the system specification, end-item specifications, and other interface documentation.
   (6) Safety-related data pertaining to off-the-shelf items.
   (7) Integrated safety analyses to be conducted and support required from associates and subcontractors.
   (8) Integrating contractor's roles in the test range, nuclear safety, explosives, or others certification processes.

b. Initiate action through the MA to make sure each associate contractor is required to be responsive to the ISSPP. Recommend contractual modification where the need exists.
c. When conducting risk assessments, examine the integrated system design, operations, and specifically the interfaces between the products of each associate contractor. Data provided by associate contractors shall be used in the conduct of this effort.
d. When performing a safety assessment, summarize the mishap risk presented by the operation of the integrated system.
e. Provide assistance and guidance to associate contractors regarding safety matters.
f. Resolve differences between associate contractors in areas related to safety, especially during development of safety inputs to system and item specifications. Where problems cannot be resolved by the integrator, notify the MA for resolution and action.
g. Initiate action through the MA to make sure information required by an associate contractor (from the integrating contractor or other associate contractors) to accomplish safety tasks is provided in an agreed-to format.

h. Develop a method of exchanging safety information between contractors. If necessary, schedule and conduct technical meetings between all associate contractors to discuss, review, and integrate the safety effort.
i. Implement an audit program to make sure the objectives and requirements of the system safety program are being accomplished. Notify in writing any associate contractor of their failure to meet contract program or technical system safety requirements for which they are responsible. The integrator for the safety effort will send a copy of the notification letter to the MA whenever such written notification has been given.

Details to be specified include, as applicable:

a. Imposition of Tasks 101, 102, and 103 as tailored.
b. Designation of the system safety integrating contractor.
c. Designation of status of the other contractors.
d. Requirements for any special integration safety analyses.
e. Requirements to support test range, nuclear safety, explosives, environmental, and/or other certification processes.

6.3 Task 104--System Safety Program Reviews.

In addition to the system safety reviews required by other DoD or service regulations and MIL-STDs (at milestone design reviews and audits), the MA may require special safety reviews or audits. Early in a major program, system safety reviews should be held at least quarterly and as the program progresses, time between reviews can be extended. In addition to more detailed coverage of those items discussed at milestone design reviews, the reviews should address progress on all system safety tasks specified in the contract.

All program reviews/audits provide an opportunity to review and assign action items and to explore other areas of concern. A mutually acceptable agenda/checklist should be written to make sure all system safety open items are covered and that all participants are prepared for meaningful discussions.

Details to be specified include, as applicable:

a. Imposition of Tasks 101 and 104.
b. Identification of reviews/audits, their content, and location(s).
c. Method of documenting the results of system safety reviews/audits.
d. Schedule for system safety reviews/audits.

6.4 Task 105--System Safety Groups/Work Group Support.

Individual service regulations require formation of SSG/SSWGs for acquisition of expensive, complex, or critical systems, equipment, or major facilities. Contractor support of an SSG/SSWG is very useful and may be necessary to make sure procured hardware or software is acceptably free from hazards that could injure personnel or cause unnecessary damage or loss. The level of support desired from the contractor must be detailed in the contract through imposition of Task 105.

The contractor may participate as an active member of MA SSG/SSWGs. Also, when needed, the contractor may support presentations to government certifying activities such as phase safety reviews, munitions safety boards, nuclear safety boards, or flight safety review boards. These may also include special reviews such as first flight reviews or preconstruction briefings. Such participation shall include activities specified by the MA such as:

a. Presentation of the contractor safety program status, including results of design or operations risk assessments.
b. Summaries of hazard analyses, including identification of problems and status of resolution.
c. Presentation of results of analyses of R&D mishaps and hazardous malfunctions, including recommendations and action taken to prevent recurrences.
d. Responding to action items assigned by the chairman of the SSG/SSWG.
e. Developing and validating system safety requirements and criteria applicable to the program.
f. Identifying safety deficiencies of the program and providing recommendations for corrective actions or preventions of recurrence.
g. Planning and coordinating support for a required certification process.
h. Documentation and distribution of meeting agendas and minutes.

Details to be specified include, as applicable:

a. Imposition of Tasks 101 and 105.
b. Contractor membership requirements and role assignments; e.g., recorder, member, alternate, or technical advisor.
c. Frequency or total number of SSG/SSWG meetings and probable locations.
d. Specific SSG/SSWG support tasks.

6.5 Task 106--Hazard Tracking and Risk Resolution.

A method or procedure must be developed to document and track hazards and progress made toward resolution of the associated risk. Each prime or associate contractor may maintain their own hazard log or assessment report, or the integrator or MA will maintain the document. If the contractor is to maintain the log, Task 106 must be imposed. Each hazard that meets or exceeds the threshold specified by the MA should be entered on the log when first identified and each action taken to eliminate the hazard or reduce the associated risk thoroughly documented. The MA will detail the procedure for closing out the hazard or acceptance of any residual risk. The hazard log may be documented and delivered as part of the system safety progress summary using DI-SAFT-80105, System Safety Engineering Report, or it can be included as part of an overall program engineering/management report.

Details to be specified include, as applicable:

a. Imposition of Tasks 101 and 106.
b. Hazard threshold for inclusion in the hazard log.
c. Complete set of data required on the hazard log, including format.
d. Procedure by, and detail to, which hazards are entered into the log.

e. Procedure by which the contractor shall obtain close out or risk acceptance by the MA of each hazard.

6.6 Task 107--System Safety Progress Summary.

The system safety progress summary provides a periodic written report of the status of system safety engineering and management activities. This status report may be submitted monthly or quarterly. It can be formatted and delivered according to DI-SAFT-80105, System Safety Engineering Report, or it can be included as part of an overall program engineering/management report.

The contractor may prepare a periodic system safety progress report summarizing general progress made relative to the system safety program during the specified reporting period and projected work for the next reporting period. The report shall contain the following information:

a. A brief summary of activities, progress, and status of the safety effort in relation to the scheduled program milestone. It shall highlight significant achievements and problems. It shall include progress toward completion of safety data prepared or in work.
b. Newly recognized significant hazards and significant changes in the degree of control of the risk of known hazards.
c. Status of all recommended corrective actions not yet implemented.
d. Significant cost and schedule changes that impact the safety program.
e. Discussion of contractor documentation reviewed by safety during the reporting period. Indicate whether the documents were acceptable for safety content and whether or not inputs to improve the safety posture were made.
f. Proposed agenda items for the next system safety group/working group meeting, if such groups are formed.

Details to be specified include, as applicable:

a. Imposition of Tasks 101 and 107.
b. Specification of progress reporting period.

CHAPTER 7

DESIGN AND INTEGRATION TASKS

7.1 Analyses. (28:39-40)

Role of Analyses. Hazard analyses are performed to identify and define hazardous conditions/risks for the purpose of their elimination or control. Analyses should examine the system, subsystems, components, and their interrelationships, as well as logistic support, training, maintenance, operational environments, and system/component disposal. Such analyses should:

a. Identify hazards and recommend appropriate corrective action.
b. Assist the individual(s) actually performing the analyses in better evaluating the safety aspects of a given system or element.
c. Provide managers, designers, test planners, and other affected decision makers with the information and data needed to permit effective tradeoffs.
d. Demonstrate compliance with given safety-related technical specifications, operational requirements, and design objectives.

Basic Elements. There are three key elements which must be properly balanced within any formal analytical approach if safety considerations are to be effectively integrated into mainstream of program systems engineering activity. These are identification, evaluation, and timely communication. A thorough appreciation of these basic elements is needed by those planning and performing analyses.

a. The timely identification of a hazard is the first step in evaluating and selecting proper safety provisions. But, identifying hazards provides little assurance that it will be properly resolved unless it is adequately evaluated and highlighted to those having the decision-making responsibilities.
b. Not all hazards are of equal magnitude, frequency, or importance. Hazard evaluation involves the determination of the likelihood of the mishap actually occurring. This may be reported in nonnumeric (qualitative) terms; or in numeric (quantitative) terms such as one in one million flight hours (1×10^{-6}/flight hour). The final phase of the evaluation process is the assignment of a severity level and probability of occurrence for the undesired event. The purpose of assigning these in the analysis document is to flag those findings which require the more immediate attention.
c. Timeliness. Safety design changes should be identified early in the system's life cycle to minimize the impact on cost and schedule. Analysis should coordinate closely with the designers to feed their recommendations into designs before publication of the analysis. Early in the full-scale development phase is the best time to incorporate safety design changes.

Safety Relationship to Reliability. Reliability and system safety analyses complement each other. The purpose of a reliability failure mode and effect analysis (FMEA) is to assess the system reliability by determining the effect of a single critical component malfunction and its repair or replacement. The reliability FMEA has been called hazardous failure mode and effect and numerous other titles; however, the analysis remains basically the same. These analyses are single-component-failure oriented and usually do not consider multiple or sequential hazards.

There are three general shortcomings of a reliability analysis when used as a safety analysis. First, Category II (Critical) and Category I (Catastrophic) hazards are often left dangling in the analyses. There have been examples of hazards being identified but not resolved. The second disadvantage to this type of analytical approach is that upstream and downstream system effects are not always identified. We need to know the effects hazards will have through their interfaces as opposed to specifics of the failed components. The third shortcoming of this type of analysis is that it generally does not always examine sequential or multiple hazards. There is a great amount of effort to identify single-point failures, repair and replacement times, but normally little effort to evaluate hazards. The fourth shortcoming is that reliability does not address the possibility of human error.

7.2 Procedures and Types. (33:38-40)

Procedures. To perform a hazard analysis, one must first consider the system restraints such as detailed design requirements (specifications), how the system is expected to operate (mission requirements), general statutory regulations such as noise abatement (regulatory requirements), standardized procedures such as switches 'up' or 'forward' for ON (good engineering practices), and lessons learned from previous mishaps and near mishaps (accident experience and failure reports).

One then looks at general and specific potential accident causal factors in the equipment (hardware and software), where the equipment is operated (environment), the man-in-the-loop (personnel), the proposed use of the system (mission), the techniques for using the system (procedures), and the specific nature of the system when in operation (configuration).

For each of the mishap causal factors, one must evaluate the individual hazards, such as the hazards caused by the operating environment and the interface hazards, such as the hazards due to personnel operating in a specified environmental condition.

To evaluate the damage possibility of a hazard, one may use either a qualitative analysis, a quantitative analysis, or both. The qualitative analysis, in general, looks for possible safeguards against damage. These include alternative designs, alternative procedures, and/or damage containment. For each safeguard, one must return to the system restraints to question if the proposed solutions exceed the imposed restraints.

A quantitative hazard evaluation requires the development of a mathematical model of the system. This may impose a problem in that not all of the required data are available. Some data can be mathematically synthesized, but other data may not be amenable to quantification and, as a result, the model may have to be modified to accommodate these gaps.

From these analyses, one determines a relativistic safety level (from qualitative analysis) or a probabilistic safety level (from quantitative analysis) and then determines corrective actions, keeping in mind all the while procedural and operational tradeoffs and cost comparisons.

Analyses Outputs. The following are some of the outputs that one might expect from a proper system safety hazard analysis:

1. Initial assessment of the significant safety problems of the program.
2. A plan for follow-on action such as additional analyses, tests, training, etc.
3. Identification of failure modes and improper usages.
4. Selection of pertinent criteria, requirements, and/or specifications.
5. Safety factors for tradeoff considerations.
6. Evaluation of hazardous designs and establish corrective/preventative action priorities.
7. Identification of safety problems in subsystem interfaces.
8. Identification of factors leading to the hazardous events.
9. Evaluation of probability of hazardous events quantitatively and identify critical paths of cause.
10. Description and ranking of the importance of hazardous conditions.
11. Developing a basis for program-oriented precautions, personnel protection, safety devices, emergency equipment-procedures-training, and safety requirements for facilities, equipment, and environment.
12. Providing evidence of compliance with program safety regulations.

7.3 Qualitative and Quantitative Analyses. (37:5-10 to 5-19)

Qualitative Analyses. A hazard analysis, predesign or postdesign, also can be designated as qualitative or quantitative. A qualitative analysis is a nonmathematical review of all factors affecting the safety of a product, system, operation, or person. It involves examination of the actual design against a predetermined set of acceptability parameters. All possible conditions and events and their consequences are considered to determine whether they could cause or contribute to injury or damage. Since a quantitative analysis is a mathematical measure of how well energy is controlled, a qualitative analysis must always precede a quantitative analysis. This is done to identify where the energy controls are applied. Any mention of quantitative analysis, therefore, infers that qualitative analysis also will be made.

In a qualitative analysis, there is no regard for the mathematical probability of occurrence of any specific event such as a mishap. The end objective is to achieve maximum safety by minimizing, eliminating, or establishing some kind of control over significant hazards in some manner, regardless of their mathematical probability. Limits are established by acceptability parameters. Conclusions of a qualitative analysis may be used as the basis on which needs for design or procedural changes can be predicted. Considerations of cost and mission requirements may limit accomplishment of all preventive and corrective measures. Quantitative evaluations may be necessary to establish frequencies of occurrence, either in terms of expected number of occurrences; or relative hazards, magnitudes of risks, and costs involved.

The qualitative analysis verifies the proper interpretation and application of the safety design criteria established by the preliminary hazard study. It also must verify that the system will operate within the safety goals and parameters established by the CONTRACT. This analysis uses the safety-critical listing and the design criteria produced to establish the scope and parameters of the verification effort. Also, it ensures that the search for design weakness is approached from the common base of the safety design instructions and acceptability parameters established in each specification. Possible modes of failure and hazardous consequences must be considered during these analyses in order to verify proper application of safety design criteria applicable to each safety-critical area. The end result determines the adequacy of the initial hazard assessment and provides recommendations for reduction in hazard potential. Qualitative systems evaluation constantly monitors each safety-critical item design as it progresses to assure proper application of criteria. The initial criteria will, in many cases, be modified as newly identified problems arise. This identification requires extensive knowledge of not only the safety design criteria that was developed but also of the technical details of the design itself.

Constant review of each safety-critical system must begin with initial design planning since the number of practical alternatives to correct design problems decrease rapidly as the program progresses. After the specifications are formulated, problems that are identified are costly to correct. Such Hazard Identification Flow Sheet analysis, therefore, usually results only in procedural warnings and attempts to avoid problems during system operation.

Beginning with the established acceptability parameters, qualitative hazards analyses are conducted in the following sequence:

a. Identify both design and operational primary hazards (i.e., sources of danger) that could generate injury, damage, loss of function, or loss of material. Each type of system has a limited number of potential mishaps. These constitute the top-level events. All other factors contribute to or affect these top-level items.

b. Identify factors contributing to the top-level events (i.e., energy sources and events occurring if the energy source is not controlled). These are listed as they come to mind. The analyst lists everything that he believes could have an adverse effect on the product or system. No effort is made at this time to consider frequency of occurrence or severity of damage. The list can be developed from theoretical considerations of possible hazards, from results of past failures of equipment, or from knowledge of problems with similar systems or subsystems.

c. Items on the preliminary list are rearranged according to the effects that they will produce. Generally, this rearrangement is done by continuing the analysis down through additional cause and effect levels. In some instances, certain conditions or events may be included in more than one area.

d. Any other events, that consideration indicates should be included are then added to the analysis. It generally will be found that listing the affecting factors will conjure up other factors in a process or reiteration and refinement. Additional levels of events are listed gradually. The number of levels depend on the depth and detail of analysis desired. In many instances, analyses eventually will reach levels involving failures as specific components of the analysis. The analyses prepared for reliability studies are, or should be, available. The results of such analyses may be utilized to avoid duplication of effort.

e. Determine failures, events, sequences, processes, errors, or other factors specific to the system that will trigger the event. All factors or questions should be addressed. Those that are considered noncredible are dispensed with after a thorough explanation of why the analyst felt the factor was not a credible risk.

f. Determine what action most practically will control the triggering mechanism considering time sequencing, severity, frequency, etc.

Quantitative Analyses. This type of analysis is a determination of how well hazards are controlled in a system, subsystem, or event. The result is expressed generally in terms of probability of occurrence. In any case, quantitative safety analysis must be based on a qualitative analysis. Numerical values are then applied. A probability analysis may be accomplished in a number of ways depending on the desired end result.

A probability is the expectancy that an event will occur a certain number of times in a specific number of trials. Probabilities provide the foundations for numerous disciplines, scientific methodologies, and risk enterprises. Actuarial methods employed by insurance companies involve predictions of future occurrences based on past experience. Reliability engineering has developed complex methods for the evaluation of probabilities that hardware will operate successfully. System safety analyses evaluate the probability that the system will not operate correctly or will operate at an inappropriate time. In addition, system safety analysis determines what effect the failure will have on the system. Statistical quality control, maintainability, and system effectiveness are other applications of probabilities in engineering. Little by little, the increased use of computer technology for evaluations of safety levels has generated an increase in the use of probabilities for this purpose.

The concept underlying this use of numerical evaluations is that the safety level of a system, subsystem, or operation can be indicated by determining the probability that mishaps will be generated by specific hazards or combinations of hazards whose presence has been established through qualitative analyses. Probabilities may be derived from experience data on operations of similar systems, preliminary tests, synthesized combination values, or extensions of all of these. The quantitative expression may include not only the expected rate at which the hazard will cause accidents but also the severity of damage that could result, or it may include both.

The probability of damage or injury is not synonymous with the probability of success or failure upon which reliability is based. The expression fail-safe itself is an indication that conditions and situations exist in which equipment can fail and no damage or injury results. Conversely, many situations exist in which personnel are injured using equipment designed and manufactured for high reliability because it operated precisely the way it was designed but at precisely the most inappropriate time.

Care must be exercised when trying to use probabilities as indicators of safety levels or risks.

a. A probability guarantees nothing. Actually, a probability indicates that a failure, error, or mishap is possible even though it may occur rarely over a period of time or during a considerable number of operations. Unfortunately, a probably cannot indicate exactly when, during which operation, or to which person a mishap will occur. It may occur during the first, last, or any intermediate operation in a series without altering the analysis results. For example, a solid propellant motor developed as the propulsion unit for a new missile had an overall reliability indicating that two motors of every 100,000 fired would probably fail. The first one tested blew up. Again, it must be noted that this failure does not change the probability of failure from 2/100,000 firings. It may shake your confidence a bit, but the probability does not change even if the first 10 firings were failures.

b. It is morally and legally unjustifiable to permit a hazard to exist unless appropriate effort is applied to eliminate it, control it, or limit any damage that it possibly could produce. The loss of the Titanic, during its maiden voyage, can be blamed only on the fact that hazards were ignored because the ship was considered to be the safest ship in the world. Also, procedures to confine the water were not initiated. Use of a numerical goal also may result in designers working to achieve that goal only and proceeding no further, even where additional corrective action could be taken.

c. Probabilities are projections determined from statistics obtained from past experience. Although equipment to be used in programmed operations may be exactly the same as that with which the statistics were obtained, the circumstances under which it will be operated probably will be different. Also, variations in production, maintenance, handling, and similar processes generally preclude two or more pieces of equipment being exactly alike. In numerous instances, minor changes in component production have caused failures and accidents when the item was used. If a mishap occurs, correcting the cause by changing the design, material, procedures, or production process immediately nullifies certain portions of the data.

d. Sometimes, data are valid only in special circumstances. For instance, statistics derived from military or commercial aviation sources may indicate that specific numbers of aircraft mishaps due to birdstrikes take place every 100,000 or million flying hours. On a broad basis involving all aircraft flight time, the probability of a birdstrike is comparatively low. At certain airfields, such as Boston, the Midway Islands, and other coastal and insular areas where birds abound, the probability of a birdstrike mishap is much higher. The same reasoning holds that generalized probabilities will not serve well for specific, localized areas. This applies to other environmental hazards such as lightning, fog, rain, snow, and hurricanes.

e. Reliability is the probability of successful accomplishment of a mission within prescribed parameters over a specific period of time. It may become necessary to operate equipment outside these prescribed parameters and time limits. Replacement parts for equipment vital to an operation may not be available. In certain cases such as an orbiting satellite, items cannot be replaced. The high reliability designed into the equipment could be degraded under these conditions and result in an increase in failure rates.

f. Human error can have damaging effects even when equipment reliability is high. For example, the loaded rifle is highly reliable, but many people have been killed or wounded when cleaning, carrying, or playing with them. Hunting mishaps have been common for hundreds of years. It has been said that the first hunting mishap occurred when an Indian was cleaning his bow and arrow but didn't know it was loaded.

g. Probabilities are predicted on an infinite or large number of trials. Probabilities, for reliability of space and missile systems, are based on small samples that result in low safety confidence levels. This problem occurs with the first pieces of hardware produced for a new system. These pieces are not governed by the constant failure rate criterion on which most reliability calculations are based but on the infant mortality or wear in portions of the curve where most higher failure rates can be expected. Since the development to deployment cycle is compressed, usable data for space systems are sparse. What little data are available for safety analysis purposes are unorganized until analysis results are no longer relevant. At that time, any change to a design can cause delays or loss of launched opportunities.

h. Design deficiencies are rarely quantifiable and can be easily overlooked by a quantitative analysis. For example, on a highly critical system, a relief valve is commanded to the open position. A secondary valve is installed to back up the first in the event of failure. It is essential that the operator knows if the first valve did not open so that backup action can be taken with the second valve. A position indicator light is actuated and the open indicator light illuminates. The valve does not open. The system overpressurizes and fails explosively. Analysis showed that the indicator light circuit was wired to indicate presence of power at the valve. It did not indicate valve position. The indicator showed only that the actuation button had been pushed, not that the valve had operated. An extensive quantitative safety analysis had failed to detect this deficiency because of a low probability of failure for the two relief valves installation. No actual examination of the electrical wiring design was made.

i. Models using probability require some assumptions about such things as the purity of the data forming the population, what the population and its parameters are, and how the various probabilities are modeled. In most applications, these restrictive assumptions are ignored or are not briefed at the onset of the decision-making sessions. The decision-makers are not made aware of the potential problems inherent in what would be otherwise a very straight forward decision input. Quantitative techniques do not lend themselves well to high-value, few-of-a-kind systems. However, occasionally these techniques can be used to advantage for assessment of risk for a specific function.

j. Most calculations for quantitative safety analysis are predicted on use of an exponential function because of the ease with which it can be applied. This method depends totally on knowledge of a supposed constant failure rate. In most cases of failure prediction, the exponential function is not truly representative of actual conditions. A constant failure rate exists when there is a large number of similar components that fail from random causes at approximately equal intervals and are then replaced. In prediction of safety-related failure, the exponential function is applied erroneously to items which do not produce a constant failure rate and, therefore, distort the analysis results.

A quantitative analysis numerically describes the safety phenomena of a system. Mathematical theories are used to assign a numerical value, describe and predict the existing hazard potential in a design. Before such theories can be used, it is necessary to construct mathematical models for the phenomena in question. It is important to recognize that the mathematical theory describes the model and not the item phenomenon itself. Don't ever confuse the mathematical results with reality. If it were, we could achieve fantastic results by sticking pins in a voodoo doll.

A quantitative analysis produces probability of occurrence estimates. Probability estimates can assist significantly in management and design decisions. However, probability figures are not intended to prove the safety or effectiveness of a system. They merely reflect results of the application of mathematical theories to mathematical models that are analogous to real situations. The validity of the analogy depends upon the adequacy of the mathematical model constructed to fit the system under study. Don't ever attempt to apply the results of analyzing one system to the problems of another unless the system and its uses are identical. The testing methods used to obtain reliability and failure data must correspond to the conditions that will be encountered within the system design envelope. The result of a quantitative analysis is of no use in itself but should be used as part of the material that forms the basis of management decisions to change or not change the design approach.

The results of quantitative analyses are used to form decisions concerning the acceptability of the design under study. For example, this type of analysis can be utilized to demonstrate that because of a high mishap probability, design changes are necessary to eliminate hazards and show the rationale for tradeoff decisions.

Figure 7-1

HAZARD ANALYSIS FLOW DIAGRAM

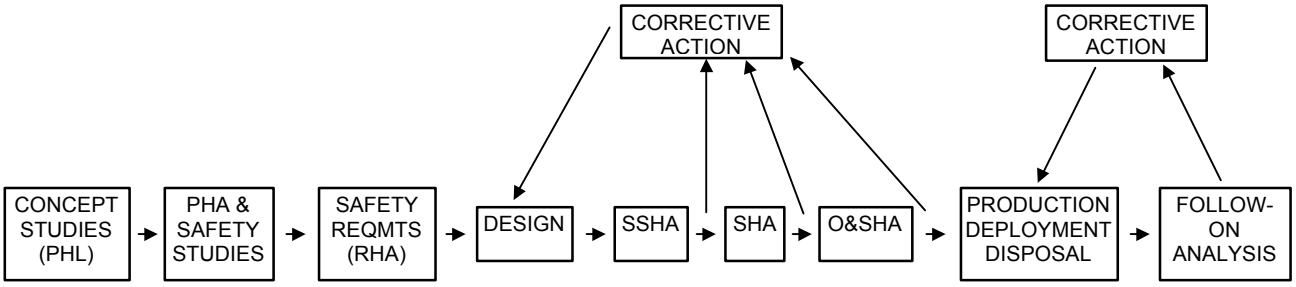
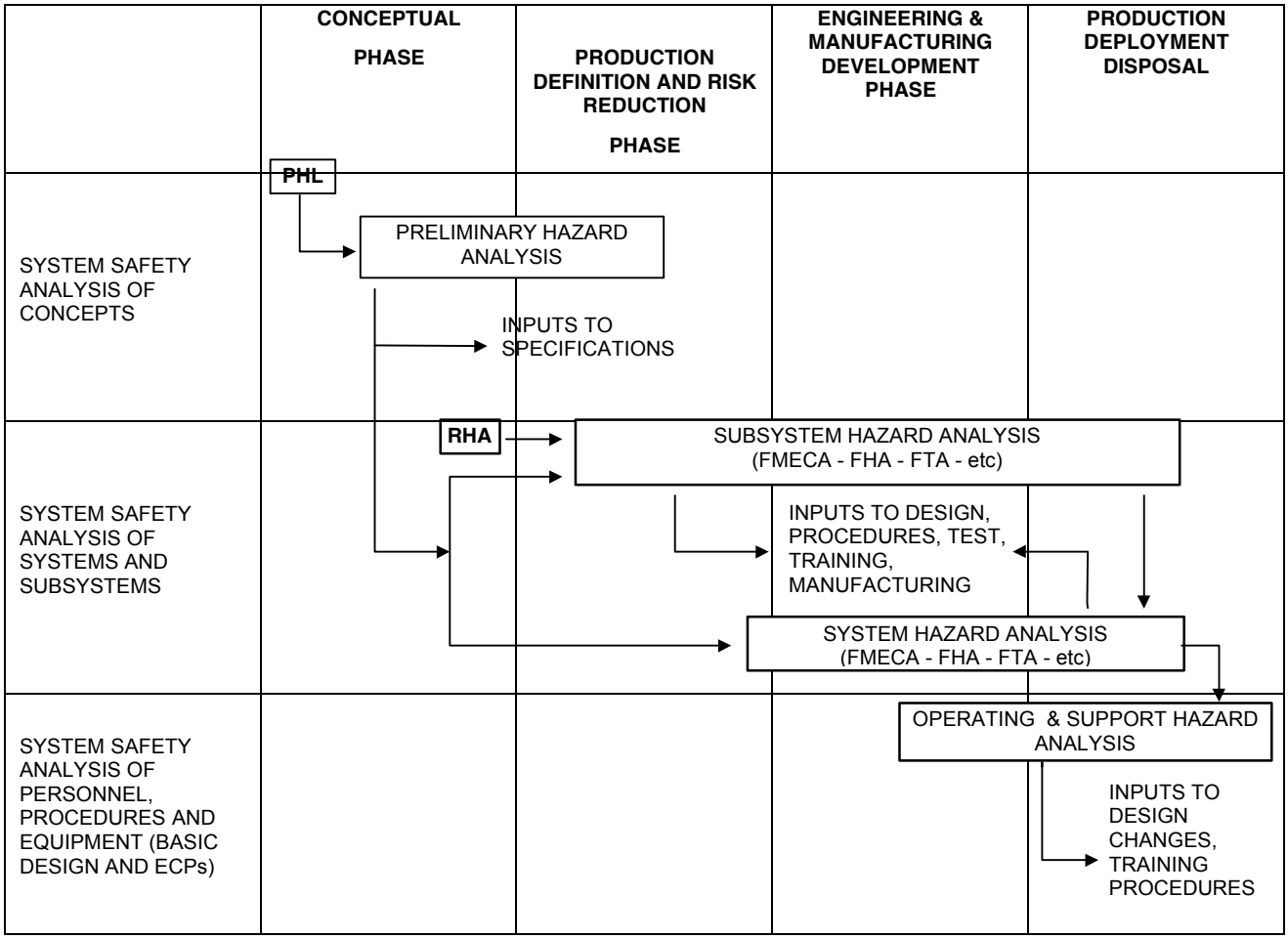


Figure 7-2

HAZARDS ANALYSES INTERRELATIONSHIPS



Quantitative safety analysis can be accomplished most effectively on action-type systems where the operation, interaction, sequencing, or failure can be predicted closely. Hazard classification is applied to monitor the reduction of hazard potential. Quantitative analysis and the application hazard categories distort the analysis results when applied to a nonaction system. The probability of failure normally is applied to action components that tend to wear out from extended use. Probability of failure applied to a nonaction system has little meaning when assigning mishap risk.

For example, as previously mentioned, any structure eventually will fail, but because of the application of fixed-design allowance, the failure rate is not constant or predictable and the probability of occurrence is so remote at any given time that it has little effect on the overall mishap risk. Also, the fixed-design allowance prevents the hazard level from changing. The potential for occurrence can be minimized only by an increase in the fixed-design allowance. The hazard level itself never can be lowered from one category to another.

The contractor's system safety function can make the initial quantitative evaluations to assure that the results of the analysis can be incorporated in program or design change documents, or that the rationale for tradeoff decisions can be documented. Then the program office evaluates a summary of the decisions that resulted from the analyses. Quantitative analysis can provide a useful tool in determining the degree of protection provided the system operator by the system design. It also can provide probability of occurrence data which are useful as management decision tools. However, quantitative analysis should not be regarded as a means to gain an answer to every design problem because it does not lend itself to an in-depth examination of the design. Statistical analysis cannot substitute for the reasoning process. It only can augment the reasoning process by introducing some confidence that the reasoning process is accurate. Used improperly, statistical analysis can add unnecessary cost; used effectively, it can indicate where costs can be avoided through safe design.

7.4 Design and Integration Tasks.

General. The system safety engineering tasks are: (35:26-27)

Task 201--Preliminary Hazard List

Task 202--Preliminary Hazard Analysis

Task 203--Requirements Hazard Analysis

Task 204--Subsystem Hazard Analysis

Task 205--System Hazard Analysis

Task 206--Operations and Support Hazard Analysis

Task 207--Health Hazard Assessment

The logical sequence of hazard analyses is shown in Figure 7-1. The flow is general in nature and can be applied to any phase of the system life cycle or to any evaluation of a design change or retrofit modification. The hazard analyses are interrelated and overlap because of their continuity between the contract phases. A representative relationship to these phases and each other is shown in Figure 7-2.

General Assessment. To ensure that the hazard analyses are thorough and repeatable, it is wise to conduct some sort of assessment of the procedures. This is true for both those monitoring the action and those who are actually performing the analyses. The following is a "checklist" for assessing any type of hazard analysis: (33:40)

1. Is there a 'road map' to show how the analysis was done?
2. Does the bookkeeping make it easy to follow the logic used in performing the analysis?
3. Are all of the primary hazards listed?
4. Do the contributory hazards include all of those that have been identified in mishaps of similar systems?
5. Are the recommended hazard controls and corrective actions detailed?
6. Are the recommended hazard controls and corrective actions realistic?
7. Are the recommended actions fed back into the line management system in a positive way that can be tracked?

7.5 Task 201--Preliminary Hazard List. (Ref 30)

The PHL provides to the MA a list of hazards that may require special safety design emphasis or hazardous areas where in-depth analyses need to be done. The MA may use the results of the PHL to determine the scope of follow-on hazard analyses (PHA, SSHA, etc.). The PHL may be documented using DI-SAFT-80101, System Safety Hazard Analysis Report.

The contractor may examine the system concept shortly after the concept definition effort begins and compile a PHL identifying possible hazards that may be inherent in the design. The contractor shall further investigate selected hazards or hazardous characteristics identified by the PHL as directed by the MA to determine their significance.

Details to be specified include, as applicable:

a. Imposition of Tasks 101 and 201.
b. Identification of special concerns, hazards, or undesired events the MA wants listed and investigated.

7.6 Task 202--Preliminary Hazard Analysis. (Ref 30)

PHA is, as implied by the title, the initial effort in hazard analysis during the system design phase or the programming and requirements development phase for facilities acquisition. It may also be used on an operational system for the initial examination of the state of safety. The purpose of the PHA is not to affect control of all risks but to fully recognize the hazardous states with all of the accompanying system implications.

The PHA effort should be commenced during the initial phases of system concept or, in the case of a fully operational system, at the initiation of a safety evaluation. This will help in the use of PHA results in tradeoff studies which are so important in the early phases of system development or, in the case of an operational system, aid in an early determination of the state of safety. The output of the PHA may be used in developing system safety requirements and in preparing performance and

design specifications. In addition, the PHA is the basic hazard analysis which establishes the framework for other hazard analyses which may be performed.

The PHA should include, but not be limited to, the following activities:

a. A review of pertinent historical safety experience.
b. A categorized listing of basic energy sources.
c. An investigation of the various energy sources to determine the provisions which have been developed for their control.
d. Identification of the safety requirements and other regulations pertaining to personnel safety, environmental hazards, and toxic substances with which the system will have to comply.
e. Recommend corrective actions.

Since the PHA should be initiated very early in the planning phase, the data available to the analyst may be incomplete and informal. Therefore, structure the analysis to permit continual revision and updating as the conceptual approach is modified and refined. As soon as the subsystem design details are complete enough to allow the analyst to begin the subsystem hazard analysis in detail, terminate the PHA. Provide the analyst performing the PHA with the following reference input information:

a. Design sketches, drawings, and data describing the system and subsystem elements for the various conceptual approaches under consideration.
b. Functional flow diagrams and related data describing the proposed sequence of activities, functions, and operations, involving the system elements during the contemplated life span.
c. Background information related to safety requirements associated with the contemplated testing, manufacturing, storage, repair, and use locations and safety-related experiences of similar previous programs or activities.

The techniques used to perform this analysis must be carefully selected to minimize problems in performing follow-on analyses. The PHA may be documented as outlined in DI-SAFT-80101, System Safety Hazard Analysis Report.

The PHA shall consider the following for identification and evaluation of hazards as a minimum:

a. Hazardous components (e.g., fuels, propellants, lasers, explosives, toxic substances, hazardous construction materials, pressure systems, and other energy sources).
b. Safety-related interface considerations among various elements of the system (e.g., material compatibilities, electromagnetic interference, inadvertent activation, fire/explosive initiation and propagation, and hardware and software controls). This shall include consideration of the potential contribution by software (including software developed by other contractors) to subsystem/system mishaps. Safety design criteria to control safety-critical software commands and responses (e.g., inadvertent command, failure to command, untimely command or responses, or MA-designated undesired events) shall be identified and appropriate action taken to incorporate them in the software (and related hardware) specifications.
c. Environmental constraints, including the operating environments (e.g., drop, shock, vibration, extreme temperatures, noise, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, electromagnetic environmental effects, ionizing and nonionizing radiation, including laser radiation).
d. Operating, test, maintenance, and emergency procedures (e.g., human factors engineering, human error analysis of operator functions, tasks, and requirements; effect of factors such as equipment layout, lighting requirements, potential exposures to toxic materials, effects of noise or radiation on human performance; explosive ordnance render safe and emergency disposal procedures; life support requirements and their safety implications in manned systems, crash safety, egress, rescue, survival, and salvage).
e. Facilities, support equipment (e.g., provisions for storage, assembly, checkout, prooftesting of hazardous systems/assemblies which may involve toxic, flammable, explosive, corrosive, or cryogenic materials/wastes; radiation or noise emitters; electrical power sources), and training (e.g., training and certification pertaining to safety operations and maintenance).
f. Safety-related equipment, safeguards, and possible alternate approaches (e.g., interlocks, system redundancy, hardware or software fail-safe design considerations, subsystem protection, fire detection and suppression systems, personal protective equipment, industrial ventilation, and noise or radiation barriers).

Details to be specified include, as applicable:

a. Imposition of Tasks 101 and 202.
b. Minimum hazard probability and severity reporting thresholds.
c. Any selected hazards or hazardous areas to be specifically examined or excluded.

7.7 Task 203--Requirements Hazard Analysis. (Ref 30)

In the early system design phase, the developer may anticipate the system design, including likely software control and monitoring functions, safing systems, etc., to determine the potential relationship between system-level hazards, hardware elements and software control, monitoring and safety functions and develop design requirements, guidelines, and recommendations to eliminate or reduce the risk of those hazards to an acceptable level. The identified hardware and software functions may be designated as safety critical. During the system requirements analysis and functional allocation phases, the developer may analyze the system and software design and requirements documents to refine the identification of potential hazards associated with the control of the system, safety-critical data generated or controlled by the system, safety-critical noncontrol functions performed by the system, and unsafe operating modes for resolution. The requirements hazard analysis is substantially complete by the time the allocated baseline is defined. The requirements are developed to address hazards, both specific and nonspecific, in hardware and software. While the development of requirements is generally

intended to be part of the PHA, often this aspect is not accomplished. In addition, the PHA does not lend itself to the inclusion of design requirements that are not related to an identified hazard.

The requirements hazard analysis uses the preliminary hazard list (Task 201) and the preliminary hazard analysis (Task 202) as a basis, if available. The analysis relates the hazards identified to the system design and identifies or develops design requirements to eliminate or reduce the risk of the identified hazards to an acceptable level. The requirements hazard analysis is also used to incorporate design requirements that are safety related but not tied to a specific hazard. The analysis includes the following efforts:

1. The contractor may determine applicable generic system safety design requirements and guidelines for both hardware and software from military specifications and standards and other documents for the system under development. The contractor may incorporate these requirements and guidelines into the high level system specifications and design documents, as appropriate.
2. The contractor may analyze the system design requirements, system/segment specifications, preliminary hardware configuration item development specification, software requirements specifications, and the interface requirements specifications, as appropriate, to include the following sub-tasks:

    a. The contractor may ensure that the system safety design requirements and guidelines are developed, refined, correctly and completely specified, properly translated into system, hardware, and software requirements and guidelines, where appropriate, and implemented in the design and development of the system hardware and associated software.
    b. The contractor may identify hazards and relate them to the specifications or documents listed above and develop design requirements to reduce the risk of those hazards.
    c. The contractor may analyze the preliminary system design to identify potential hardware/software interfaces at a gross level that may cause or contribute to potential hazards. Interfaces identified shall include control functions, monitoring functions, safety systems, and functions that may have indirect impact on safety. These interfaces and the associated software shall be designated as safety critical.
    d. The contractor may perform a preliminary hazard risk assessment on the identified safety-critical software functions using the hazard risk matrix or software hazard risk matrix of Appendix A or another process as mutually agreed to by the contractor and the MA.
    e. The contractor may ensure that system safety design requirements are properly incorporated into the operator, users, and diagnostic manuals.
    f. The contractor may ensure that the system safety design requirements are properly incorporated into the user, and diagnostic manuals.
3. The contractor may develop safety-related design change recommendations and testing requirements may incorporate them into preliminary design documents and the hardware, software, and system test plans. The following sub-tasks shall be be accomplished:

    a. The contractor may develop safety-related change recommendations to the design and specification documents listed above and shall include a means of verification for each design requirement.
    b. Develop testing requirements. The contractor may develop safety-related test requirements for incorporation into the test documents. Tests shall be developed for hardware, software, and system integration testing.
4. The contractor may support the system requirements review, system design review, and software specification review from a system safety viewpoint. The contractor may address the system safety program, analyzes performed and to be performed, significant hazards identified, hazard resolutions or proposed resolutions, and means of verification.

Details to be specified include, as applicable:

a. Imposition of Tasks 101 and 203 tailored to the developmental program.
b. Definition of acceptable level of risk within the context of the system, subsystem, or component under analysis.
c. Level of contractor support required for design reviews.
d. Specification of the type of risk assessment process.

7.8 Task 204--Subsystem Hazard Analysis. (Ref 30)

This task would be performed if a system under development contained subsystems or components that when integrated functioned together in a system. This analysis looks at each subsystem or component and identifies hazards associated with operating or failure modes and is especially intended to determine how operation or failure of components affects the overall safety of the system. This analysis should identify necessary actions, using the system safety precedence to determine how to eliminate or reduce the risk of identified hazards.

As soon as subsystems are designed in sufficient detail, or well into concept design for facilities acquisition, the SSHA can begin. Design changes to components will also need to be evaluated to determine whether the safety of the system is affected. The techniques used for this analysis must be carefully selected to minimize problems in integrating subsystem hazard analyses into the system hazard analysis. The SSHA may be documented as outlined in DI-SAFT-80101, System Safety Hazard Analysis Report.

The contractor may perform and document a subsystem hazard analysis to identify all components and equipment, including software, whose performance, performance degradation, functional failure, or inadvertent functioning could result in a hazard or whose design does not satisfy contractual safety requirements. The analysis may include a determination:

a. Of the modes of failure, including reasonable human errors as well as single-point failures, and the effects on safety when failures occur in subsystem components.
b. Of potential contribution of software (including that which is developed by other contractors) events, faults, and occurrences (such as improper timing) on the safety of the subsystem.
c. That the safety design criteria in the software specification(s) have been satisfied.
d. That the method of implementation of software design requirements and corrective actions has not impaired or decreased the safety of the subsystem nor has introduced any new hazards.

If no specific analysis techniques are directed, the contractor may obtain MA approval of technique(s) to be used prior to performing the analysis. When software to be used in conjunction with the subsystem is being developed under other development documents, the contractor performing the SSHA shall monitor, obtain, and use the output of each phase of the formal software development process in evaluating the software contribution to the SSHA. Problems identified which require the reaction of the software developer shall be reported to the MA in time to support the ongoing phase of the software development process. The contractor shall update the SSHA when needed as a result of any system design changes, including software changes which affect system safety.

Details to be specified include, as applicable:

a. Imposition of Tasks 101 and 204.
b. Minimum hazard severity and probability reporting thresholds.
c. The specific subsystems to be analyzed.
d. Any selected hazards, hazardous areas, or other items to be examined or excluded.
e. Specification of desired analysis technique(s) and/or format.

7.9 Task 205--System Hazard Analysis. (Ref 30)

An SHA is accomplished in much the same way as the subsystem hazard analysis. However, as the SSHA examines how component operation or failure affects the system, the SHA determines how system operation and failure modes can affect the safety of the system and its subsystems. The SHA should begin as the system design matures, around the preliminary design review or the facilities concept design review milestone, and should be updated until the design is complete. Design changes will need to be evaluated to determine their effects on the safety of the system and its subsystems. This analysis should contain recommended actions, applying the system safety precedence, to eliminate or reduce the risk of identified hazards. The techniques used to perform this analysis must be carefully selected to minimize problems in integrating the SHA with other hazard analyses. The SHA may be documented as outlined in DI-SAFT-80101, System Safety Hazard Analysis Report.

The contractor may perform and document a system hazard analysis to identify hazards and assess the risk of the total system design, including software, and specifically of the subsystem interfaces. This analysis shall include a review of subsystem interrelationships for:

a. Compliance with specified safety criteria.
b. Independent, dependent, and simultaneous hazardous events, including failures of safety devices and common causes that could create a hazard.
c. Degradation in the safety of a subsystem or the total system from normal operation of another subsystem.
d. Design changes that affect subsystems.
e. Effects of reasonable human errors.
f. Determination:

   (1) Of potential contribution of software (including that which is developed by other contractors) events, faults, and occurrences (such as improper timing) on safety of the system.
   (2) That the safety design criteria in the software specification(s) have been satisfied.
   (3) That the method of implementation of the software design requirements and corrective actions has not impaired or degraded the safety of the system nor has introduced any new hazards.

If no specific analysis techniques are directed, the contractor may obtain MA approval of technique(s) to be used prior to performing the analysis. The SHA may be performed using similar techniques to those used for the SSHA. When software to be used in conjunction with the system is being developed under other development documents, the contractor performing the SHA shall monitor, obtain, and use the output of each phase of the formal software development process in evaluating the software contribution to the SHA. Problems identified which require the reaction of the software developer shall be reported to the MA in time to support the ongoing phase of the software development process. The contractor shall update the SHA when needed as a result of any system design changes, including software design changes which affect system safety.

Details to be specified include, as applicable:

a. Imposition of Tasks 101 and 205.
b. Minimum hazard severity and probability reporting thresholds.
c. Any selected hazards, hazardous areas, or other specific items to be examined or excluded.
d. Specification of desired analysis technique(s) and/or format.

7.10 Task 206--Operating and Support Hazard Analysis. (Ref 30)

The O&SHA is performed primarily to identify and evaluate the hazards associated with the environment, personnel, procedures, and equipment involved throughout the operation of a system/element. The O&SHA may be performed on such activities as testing, installation, modification, maintenance, support, transportation, ground servicing, storage, operations, emergency escape, egress, rescue, post-accident responses, and training. The O&SHA may also be selectively applied to facilities acquisition projects to make sure operation and maintenance manuals properly address safety and health requirements.

The O&SHA effort should start early enough to provide inputs to the design and prior to system test and operation. The O&SHA is most effective as a continuing closed-loop iterative process, whereby proposed changes, additions, and formulation of functional activities are evaluated for safety considerations prior to formal acceptance. The analyst performing the O&SHA should have available:

a. Engineering descriptions of the proposed system, support equipment, and facilities.
b. Draft procedures and preliminary operating manuals.
c. PHA, SSHA, and SHA reports.
d. Related and constraint requirements and personnel capabilities.
e. Human factors engineering data and reports.
f. Lessons learned, including a history of mishaps caused by human error.
g. Effects of off-the-shelf hardware and software across the interface with other system components or subsystems.

Timely application of the O&SHA will provide design guidance. The findings and recommendations resulting from the O&SHA may affect the diverse functional responsibilities associated with a given program. Therefore, exercise care in assuring that the analysis results are properly distributed for the effective accomplishment of the O&SHA objectives. The techniques used to perform this analysis must be carefully selected to minimize problems in integrating O&SHAs with other hazard analyses. The O&SHA may be documented using DI-SAFT-80101, System Safety Hazard Analysis Report.

The contractor may perform and document an O&SHA to examine procedurally controlled activities. The O&SHA identifies and evaluates hazards resulting from the implementation of operations or tasks performed by persons, considering: the planned system configuration/state at each phase of activity; the facility interfaces; the planned environments (or ranges thereof); the supporting tools or other equipment, including software-controlled automatic test equipment, specified for use; operational/task sequence, concurrent task effects and limitations; biotechnological factors, regulatory or contractually specified personnel safety and health requirements; and the potential for unplanned events, including hazards introduced by human errors. The O&SHA must identify the safety requirements (or alternatives) needed to eliminate identified hazards, or to reduce the associated risk to a level which is acceptable under either regulatory or contractually specified criteria. The analysis may identify:

a. Activities which occur under hazardous conditions, their time periods, and the actions required to minimize risk during these activities/time periods.
b. Changes needed in functional or design requirements for system hardware/software, facilities, tooling, or support/test equipment to eliminate hazards or reduce associated risks.
c. Requirements for safety devices and equipment, including personnel safety and life support equipment.
d. Warnings, cautions, and special emergency procedures (e.g., egress, rescue, escape, render safe, explosive ordnance disposal, back-out, etc.), including those necessitated by failure of a software-controlled operation to produce the expected and required safe result of indication.
e. Requirements for handling, storage, transportation, maintenance, and disposal of hazardous materials.
f. Requirements for safety training and personnel certification.

The O&SHA documents system safety assessment of procedures involved in: system production, deployment, installation, assembly, test, operation, maintenance, servicing, transportation, storage, modification, demilitarization, and disposal. The contractor shall update the O&SHA when needed as a result of any system design or operational changes. If no specific analysis techniques are directed, the contractor shall obtain MA approval of technique(s) to be used prior to performing the analysis.

Details to be specified include, as applicable:

a. Imposition of Tasks 101 and 206.
b. Minimum hazard probability and severity reporting thresholds.
c. Specification of desired analysis technique(s) and/or format.
d. The specific procedures to be evaluated.

7.11 Task 207--Health Hazard Assessment. (Ref 30)

The purpose of Task 207 is to perform and document an health hazard assessment (HHA) to identify health hazards, evaluate proposed hazardous materials, and propose protective measures to reduce the associated risk to a level acceptable to the MA.

The first step of the HHA is to identify and determine quantities of potentially hazardous materials or physical agents (noise, radiation, heat stress, cold stress) involved with the system and its logistical support. The next step would be to analyze how these materials or physical agents are used in the system and for its logistical support. Based on the use, quantity, and type of substance/agent, estimate where and how personnel exposures may occur and if possible the degree or frequency of exposure involved. The final step would include incorporation into the design of the system and its logistical support equipment/facilities cost-effective controls to reduce exposures to acceptable levels. The life-cycle costs of required controls could be high, and consideration of alternative systems may be appropriate.

An HHA evaluates the hazards and costs due to system component materials, evaluates alternative materials and recommends materials that reduce the associated risks and life cycle costs. Materials are evaluated if (because of their physical, chemical, or biological characteristics; quantity; or concentrations) they cause or contribute to adverse effects in organisms or off-spring, pose a substantial present or future danger to the environment, or result in damage to or loss of equipment or property during the systems life cycle.

Specific health hazards and impacts of an HHA include:

a. Chemical Hazards - Hazardous materials that are flammable, corrosive, toxic, carcinogens or suspected carcinogens, systemic poisons, asphyxiants, respiratory irritants, etc.
b. Physical Hazards - noise, heat, cold, ionizing and non-ionizing radiation, etc.
c. Biological Hazards - bacteria, fungi, etc.
d. Ergonomic Hazards - lifting, task saturation, etc.
e. Other hazardous materials that may be introduced by the system during manufacture, operation, or maintenance.

The assessment addresses:

a. System, facility, and personnel protective equipment requirements (e.g., ventilation, noise attenuation, radiation barriers, etc.) to allow safe operation and maintenance. When feasible engineering designs are not available to reduce hazards to acceptable levels,
alternative protective measures must be specified (e.g., protective clothing, operation or maintenance procedures to reduce risk to an acceptable level).

b. Potential material substitutions and projected disposal issues. The HHA discusses long term effects such as the cost of using alternative materials over the life cycle or the capability and cost of disposing of a substance.

c. Hazardous Material Data. The HHA describes the means for identifying and tracking information for each hazardous material. Specific categories of health hazards and impacts that may be considered are acute health, chronic health, cancer, contact, flammability, reactivity, and environment.

The HHA's hazardous materials evaluation may:

a. Identify the hazardous materials by name(s) and stock numbers; the affected system components and processes; the quantities, characteristics, and concentrations of the materials in the system; and source documents relating to the materials.
b. Determine under which conditions the hazardous materials can release or emit materials in a form that may be inhaled, ingested, absorbed by living beings, or leached into the environment.
c. Characterize material hazards and determine reference quantities and hazard ratings for system materials in question.
d. Estimate the expected usage rate of each hazardous material for each process or component for the system and program-wide impact.
e. Recommend the disposition of each hazardous material identified. If a reference quantity is exceeded by the estimated usage rate, material substitution or altered processes may be considered to reduce risks associated with the material hazards while evaluating the impact on program costs.

Using DI-SAFT-80106A for each proposed and alternative material, the assessment must provide the following data for management review:

a. Material Identification. Includes material identity, common or trade names, chemical name, chemical abstract service (CAS) number, national stock number (NSN), local stock number, physical state, and manufacturers and suppliers.
b. Material Use and Quantity. Includes component name, description, operations details, total system and life cycle quantities to be used, and concentrations of any mixtures.
c. Hazard Identification. Identify the adverse effects of the material on personnel, the system, environment, or facilities.
d. Toxicity Assessment. Describes expected frequency, duration, and amount of exposure. References for the assessment must be provided.
e. Risk Calculations. Includes classification of severity and probability of occurrence, acceptable levels of risk, any missing information, and discussions of uncertainties in the data or calculations.

Details to be specified include:

a. Imposition of tasks 101 and 207.
b. Minimum hazard severity and probability reporting thresholds.
c. Any selected hazards, hazardous areas, hazardous materials or other specific items to be examined or excluded.
d. Specification of desired analysis techniques and/or report formats.

CHAPTER 8

DESIGN EVALUATION, COMPLIANCE, AND VERIFICATION

(30:A19-24, Sections 300 and 400)

8.1 Task 301--Safety Assessment. (MIL-STD-882C and DoD Deskbook task numbers)

The contractor performs and documents a safety assessment to identify all safety features of the hardware, software, and system design and to identify procedural hazards that may be present in the system being acquired, including specific procedural controls and precautions that should be followed. The safety assessment summarizes:

a. The safety criteria and methodology used to classify and rank hazards.
b. Analyses and tests performed to identify system hazards, including:

   (1) Those hazards posing residual risk and actions taken to reduce the risk to a level contractually specified as acceptable.
   (2) Results of tests conducted to validate safety criteria requirements and analyses.

c. The results of the safety program efforts. Include a list of all significant hazards along with specific safety recommendations or precautions required to ensure safety of personnel and property. Categorize the list of hazards as to whether or not they may be expected under normal or abnormal operating conditions.
d. Any hazardous materials generated by or used in the system, including:

   (1) Identification of material type, quantity, and potential hazards.
   (2) Safety precautions and procedures necessary during use, storage, transportation, and disposal (e.g., explosive ordnance disposal).
   (3) After launch safety-related activity of expendable launch vehicles and their payloads, including deployment, operation, reentry, and recovery of launch vehicle/payloads which do not attain orbit (either planned or unplanned).
   (4) Orbital safety hazard awareness associated with space systems such as explosions, electromagnetic interference, radioactive sources, ionizing radiation, chemicals, space debris, safe separation distances between vehicles, and natural phenomena.
   (5) A copy of the Material Safety Data Sheet (OSHA Form 20).

e. Conclude with a signed statement that all identified hazards have been eliminated or their associated risks controlled to levels contractually specified as acceptable and that the system is ready to test or operate or proceed to the next acquisition phase.

In addition, the contractor may make recommendations applicable to hazards at the interface of his system with the other system(s) as contractually required.

Details to be specified include, as applicable:

a. Imposition of Tasks 101 and 301.

b. Define the specific purpose of the requested assessment.

c. Identify at what contractor level (system safety manager, program manager, etc.) the statement (paragraph e) must be signed.

8.2 Task 302--Test and Evaluation.

The purpose of Task 302 is to make sure safety is considered (or safety responsibility assigned) in test and evaluation, to provide existing analysis reports and other safety data, and to respond to all safety requirements necessary for testing in-house, at other contractor facilities, and at government ranges, centers, or laboratories. Planning for test and evaluation safety from the beginning of the contract period may incorporate:

a. Test program milestones requiring completion of hazard analyses, risk assessments, or other safety studies.

b. Schedule for analysis, evaluation, and approval of test plans, procedures, and other documents to make sure safety is covered during all testing.

c. Preparation of or input to safety, operating, and test precedes.

d. That test equipment, installation of test equipment, and instrumentation are considered in hazard analyses prior to test start.

e. Meeting specialized requirements designated by the MA and informing the MA of any identified hazards that are unique to the test environment.

f. Coordination and status reviews with test site safety representatives to ensure test safety requirements

are identified, monitored, and completed as scheduled.

Providing assistance to the safety review teams to the extent necessary to support a system safety certification process and validate, from a safety perspective, that the system is ready to test. Follow-up action to ensure completion of the corrective efforts shall be taken to reduce or correct test and evaluation hazards. Maintaining a repository of test

and evaluation hazard/action status reports are also required.

Details to be specified include, as applicable:

a. Imposition of Tasks 101 and 302.

b. Designation of applicable specialized system safety requirements for testing or use of range facilities.

c. Schedule for meeting requirements.
d. Identification of hazard categories for which organizations will take action.

8.3 Task 303--ECPs, Deviations, and Waivers.

This task may be documented using DI-SAFT-80103, Engineering Change Proposal System Safety Report, and DI-SAFT-80104, Waiver or Deviation System Safety Report. ECPs to the existing design and requests for deviation/waiver from existing requirements must be assessed for any possible safety impacts to the system. Correction of a deficiency can introduce other overlooked deficiencies. This task is designed to prevent that occurrence by requiring contractor system safety engineers to examine each ECP or request for deviation/waiver and investigate all conceivable ways the change or deviation could result in an additional hazard(s). The task specifies that the MA be notified if the ECP or request for deviation/waiver increases the existing level of risk.

Details to be specified include, as applicable:

a. Imposition of Tasks 101 and 303.

b. Specify amount of change in the level of safety requiring MA notification and the method and timing of such notification.

c. Identify class of ECP or type of deviation/waiver to which this task applies.

d. Identify who shall execute review and sign-off authority for each class of ECP or type of deviation/waiver.

8.4 Task 401--Safety Verification

Many safety requirements, as specified in system specifications, requirements documents, etc., will need to be verified by analysis, inspection, demonstration, or test. Also, during design and development, hazard analyses will identify hazards that will be removed through redesign, controls, safety devices, etc. Imposition of these changes will require verification. Task 401 outlines how safety verification should be performed.

The contractor may define and perform tests, demonstrations, or otherwise verify the compliance with safety requirements on safety-critical hardware, software, and procedures (e.g., EOD procedures). Induced or simulated failures shall be considered to demonstrate the failure mode and acceptability of safety-critical equipment and software. Where hazards are identified during the development effort and it cannot be determined by analysis or inspection whether the action taken will adequately reduce the risk, safety tests may be conducted to evaluate the effectiveness of the actions taken. SSPPs and test program plans may be revised to include *these tests. Where costs for

safety testing would be prohibitive; safety characteristics or procedures may be verified by engineering analyses, analogy, laboratory test, functional mockups, or subscale/model simulation, when approved by the MA. Specific safety tests shall be integrated into appropriate system test and demonstration plans to the maximum extent possible. Test plans, test procedures, and results of all tests, including design verification, operational evaluation, technical data validation and verification, production acceptance, and self-life validation shall be reviewed to make sure:

a. Safety of the design is adequately demonstrated, including operating and maintenance procedures and verification of safety devices, warning devices, etc., for all catastrophic hazards not eliminated by design. Critical, marginal, and negligible hazards shall also be addressed, as required by the MA.

b. Results of safety evaluations of the system are included in the test and evaluation reports.

Details to be specified include, as applicable:

a. Imposition of Tasks 101 and 401.

b. Identification of safety-critical equipment and procedures.

c. Identification of hazard categories requiring verification steps.

d. Development of, or inputs to, test plans, procedures, and reports to verify safety requirements.

8.5 Task 402--Safety Compliance Assessment.

A safety compliance assessment is conducted to verify the safe design of a system and to obtain a comprehensive evaluation of the safety risk being assumed prior to test or operation of a system. It can be documented by following DI-SAFT-80102, Safety Assessment Report. It is an operationally oriented analysis, concerned with the safe use of a system, equipment, or facility. A safety compliance assessment is, therefore, broad in scope, covering almost every aspect of the system, but relatively general in nature, delving into detail only to the extent necessary to verify the system's safety or ascertain the risks and precautions necessary for its safe use. A safety compliance assessment may be the only analysis conducted on a program or it may serve as a pretest or preoperational safety review, integrating and summarizing operational safety considerations identified in more detailed hazard analyses.

A safety compliance assessment may be the only analysis conducted on a relatively low safety risk program. The low risk can result from several different factors. The system may be an integration of primarily off-the-shelf equipment involving little or no new design. It may be a system which is low risk by nature of its technology or complexity. Compliance with federal, military, national, and industry specifications, standards, and codes may be sufficient to make sure of the basic safety of the system. A safety compliance assessment may also be conducted on higher safety risk systems, such as research or advanced development projects, where the higher risks must be accepted but for which safe operation is still required and the risks must be recognized and reduced to acceptable levels.

This assessment may be conducted during any phase of system development. It should be started as soon as sufficient information becomes available. For example, evaluation of equipment should begin with the design of equipment components or with the receipt of equipment specifications from a subcontractor or vendor. The analysis can also be tailored in the SOW to meet the particular needs of a program.

A safety compliance assessment should include, but not be limited to:

a. Identification of appropriate safety standards and verification of system compliance. The contractor should also review available historical safety data from similar systems. Verification may be achieved by several methods, including analysis, use of checklists, inspection, test, independent evaluation, or manufacturer's certification.

b. Analysis and resolution of system hazards. The assessment should incorporate the scope and techniques of other hazard analyses to the detail necessary to assure a reasonably safe system.

b. Identification of specialized safety requirements. The contractor should identify all safety precautions necessary to safely operate and support the system. This includes applicable precautions external to the system or outside the contractor's responsibility such as off-the-shelf equipment, emergency lighting, fire protection, or personal safety equipment.

d. Identification of hazardous materials and the precautions and procedures necessary for the safe handling of the material.

Details to be specified include, as applicable:

a. Imposition of Tasks 101 and 402.

b. Identify applicable requirements.

8.6 Task 403--Explosive Hazard Classification and Characteristics Data.

This task requires the contractor to perform those tests and procedures necessary for the development of hazard explosive characteristics data and the classification of new or modified ammunition, explosives (including solid propellants), and devices containing explosives. The contractor may perform tests specified by the PM using DOD Explosive Hazard Classification Procedures (TO 11A-1-47) or by analogy to an item having a valid hazard classification to develop interim or final explosive classifications for program system explosives.

The contractor recommends a category for each item of explosives /ammunition in hazard class, division, storage compatibility group, and DOT class/label areas. Hazard characteristics data should be generated or compiled to reveal hazards involved in handling, shipping, and storage related to the production and procurement of new or modified item of explosives/ammunition. Any changes to an item that had received a final hazard classification must be reported through the Government and Industry Data Exchange Program.

The data should be used to complete the appropriate DI-SAFT-81299A. The data should include identification information, chemical and physical characteristics, item description, functions, assembly drawings, packaging, and storage and shipping limitations. Both an in-process hazard classification (the packaging and handling hazard classification—not the manufacturing hazard) and the shipping/storage hazard classification are required. They may not be the same. The packaging for an item may change the hazard classification. The in-process hazard classification is identified by class or (for liquid propellants) by Group.

Details to be specified include:

a. Imposition of this Task (403).

b. The parts of the DOD EHCP containing the required test methods and procedures.

c. Specific hazard classification data required.

8.7 Task 404--Explosive Ordnance Disposal Source Data.

The purpose of this task is to require the contractor to provide source data, explosives ordnance disposal procedures, recommended render safe procedures, and test data for system explosives. The contractor uses DI-SAFT-80931 for the Naval Explosives Ordnance Disposal Technical Center, Indian Head, MD, to develop, test, validate, and publish joint service non-nuclear explosives ordnance disposal procedures in technical manuals.

The data generated for Task 403 is supplemented with disposal data including: normal/optional use descriptions, differentiating markings and features, operational sequence data, disassembly information, and recommended render safe procedures.

Details to be specified include:

a. Imposition of this Task (404)

b. Hazard classification data for all explosive components.

CHAPTER 9

ANALYSIS TECHNIQUES

9.1 Fault Hazard Analysis. (33:47-49)

Those performing hazard analyses have the option of choosing from amongst several techniques that range from the relatively simple to the complex. This discussion presents the basics of several of these techniques.

A sample fault hazard analysis (FHA) form is shown in Figure XX (Insert figure, using Design handbook 1-6, Sub-Note 3.3.1.1(1))

The fault hazard analysis is an inductive method of analysis that can be used exclusively as a qualitative analysis or, if desired, expanded to a quantitative one. The fault hazard analysis requires a detailed investigation of the subsystems to determine component hazard modes, causes of these hazards, and resultant effects to the subsystem and its operation. This type of analysis is a form of an analysis long used in reliability, called failure mode and effects analysis (FMEA) or failure mode, effects, and criticality analysis (FMECA). The chief difference between the FMEA/FMECA and the fault hazard analysis is a matter of depth. Wherein the FMEA or FMECA looks at ALL failures and their effects, the fault hazard analysis is charged only with consideration of those effects that are safety related.

The fault hazard analysis of a subsystem is an engineering analysis to determine what can fail, how it can fail, how frequently it will fail, what the effects of the failure are, and how important the effects of the failure are.

A fault hazard analysis is used to aid in system design concept selection, to support “functional mechanizing” of hardware, to prompt the designer to “design around” failure modes and effects that involve severe penalties, to assist in operational planning for employment of the system, and to assist management decisions to selectively concentrate limited resources on “highest risk” or “highest criticality” system elements.

Not all modes are considered—only the most important. But here is a Catch 22: How can you tell which are the most important without considering all or nearly all of the modes? The fault hazard analysis must consider both “functional modes” and “out-of-tolerance modes” of failure. For example, a 5-percent, 5K (plus or minus 250 ohm) resistor can have as functional failure modes failing open or failing short, while the out-of-tolerance modes might include too low or too high a resistance.

To conduct a fault hazard analysis, it is necessary to know and understand the mission of the equipment, the constraints under which it must operate, and the limits delineating success and failure. The procedural steps are:

a. The system is divided into subsystems that can be handled effectively.
b. Functional diagrams, schematics, and drawings for the system and each subsystem are then reviewed to determine their interrelationships and the interrelationships of the component subassemblies. This review may be done by the preparation and use of block diagrams.
c. A complete component list with the specific function of each component is prepared for each subsystem as it is to be analyzed.
d. Operational and environmental stresses affecting the system are reviewed for adverse effects on the system or its components.
e. Significant failure mechanisms that could occur and affect components are determined from analysis of the engineering drawings and functional diagrams. Effects of subsystem failures are then considered.
f. The failure modes of individual components that would lead to the various possible failure mechanisms of the subsystem are then identified. Basically, it is the failure of the component that produces the failure of the entire system. However, since some components may have more than one failure mode, each mode must be analyzed for its effect on the assembly and then on the subsystem. This may be accomplished by tabulating all failure modes and listing the effects of each. (The resistor that is open or short, high or low).
g. All conditions that affect a component or assembly should be listed to indicate whether there are special periods of operation, stress, personnel action, or combinations of events that would increase the probabilities of failure or damage.
h. The hazard category from MIL-STD-882 should be assigned.
i. Preventative or corrective measures to eliminate or control the hazards are listed.
j. Initial probability rates may be entered. These are ‘best judgments’ and will be revised as the design process goes on.
k. A preliminary criticality analysis may be done at this time.

A subsystem may have failures that do not result in mishaps and tracking all of these down is a costly process. Even if one desired to track down all the possible failures, all failures may not be found, all failure modes may not be considered, and all failure effects may not be considered. Concentration is usually on hardware failures, and often inadequate attention is given to human factors. For example, a switch with an extremely low failure rate may be dropped from consideration, but the wrong placement of the switch may lead to a mishap. Environmental conditions are usually considered, but the probability of occurrence of these conditions is rarely considered. This may result in ‘over safetying.’ Reliability is considered on the basis of tests, and substandard manufacture and wear are usually not considered.

One of the greatest pitfalls in fault hazard analysis (and in other techniques) is over precision in mathematical analysis.

Too often, analysts try to obtain "exact" numbers from "inexact" data, and too much time may be spent in improving preciseness of the analysis rather than in eliminating the hazards.

9.2 Fault Tree Analysis. (28:42-44)

A fault tree analysis (FTA) (similar to a logic diagram) is a "deductive" analytical tool used to study a specific undesired event. The "deductive" approach begins with a defined undesired event, usually a postulated accident condition, and systematically considers all known events, faults, and occurrences, which could cause or contribute to the occurrence of the undesired event.

A sample FTA is shown in Figure YY (Use DH-16, Sub-Note 3.3.2.1(1))

An FTA is primarily a qualitative technique used to identify those design areas that need further accident prevention attention. However, it can be used quantitatively by applying detailed hazardous event probabilities to calculate the overall probability of the top-level undesired event. The decision as to whether design changes/remedial actions are needed is based upon the outcome of the qualitative or quantitative evaluation of the system. The building of a fault tree normally starts with the identification of an "undesired event" at the top of the "tree." The tree that follows is a graphical logic representation of fault events that may occur to a functional system. This logical analysis must be a functional representation of the system and must include all combinations of system fault events that can cause or contribute to the undesired event. Each contributing fault event should be further analyzed to determine the logical relationships of underlying fault events that may cause them. This tree of fault events is expanded until all "input" fault events are defined in terms of basic, identifiable faults which may then be quantified for computation of probabilities, if desired. When the tree has been completed, it becomes a logic gate network of fault paths, both singular and multiple, containing combinations of events and conditions which include primary, secondary, and upstream inputs that may influence or command the hazardous mode.

Fault trees are logic diagrams showing the relationship of all conditions that will cause an undesired event. It is not an analysis of the system, per se. You must draw fault trees for a specific undesired condition, such as "canopy fails to jettison." The more specific the undesired event, the better the fault tree will accurately reflect the system in the particular mode required to cause the top event. Top events, which are too broad or too general, lead to useless fault trees. The following planning must be done for FTA.

a. Pick an undesired event which can be clearly defined and limited in scope so that the fault tree will accurately represent all the possibilities or conditions necessary to cause them.

b. It's not feasible to investigate all undesired conditions for all systems; thus, decide which ones are more important for each system.

Fault trees will:

a. Analyze selected undesired conditions and determine the faults or combination of faults that cause these conditions.

b. Determine the safety impact of design changes.

c. Provide rational basis for tradeoff studies.

d. Be of continuing value to AFMC during the test and operational phases where the impact of modifications and retrofits must be chosen. The FTA should be updated throughout the life cycle to be of any use to AFMC after transfer of responsibility to logistics.

e. Provide supporting data for accident investigations.

9.3 Common Cause Failure Analysis. (36:21)

Common cause failure analysis (CCFA) is an extension of FTA to identify "coupling factors" which can cause component failures to be potentially interdependent. Examples of coupling factors are:

--redundant relays located in the same vibration environment, making them susceptible to simultaneous failure.

--indicator light bulbs made in the same lot by the same manufacturer and subject to the same manufacturing fault.

Primary events of minimal cut sets from the FTA are examined through the development of matrices to determine if failures are linked to some common cause relating to environment, location, secondary causes, human error, or quality control. Thus, components are identified within the cut sets that are susceptible to the same factor. CCFA provides a better understanding of the interdependent relationship between FTA events and their causes and analyzes safety systems for "real" redundancy. This analysis provides additional insight into system failures after development of a detailed FTA and when data on components, physical layout, operators, inspectors, etc., are available.

9.4 Sneak Circuit Analysis. (18:351-361)

Sneak circuit analysis (SCA) is a unique method of evaluating electrical circuits. SCA employs recognition of topological patterns which are characteristic of all circuits and systems. The purpose of this analysis technique is to uncover latent (sneak) circuits and conditions that inhibit desired functions or cause undesired functions to occur, without a component having failed.

A classic example of a sneak circuit: A car's emergency flasher is wired directly to the car battery. The brake light circuit is wired to the ignition switch, so that the brake lights will only function with the ignition ON. The car radio is also wired to the ignition circuit for the same reason. Now, some of us like to leave on the radio switch and use the ignition switch to turn off the radio. Imagine you've done just that, and decide you need to use the four-way flashers. Turn on the flasher and step on the brakes at the same time, and the radio comes on intermittently with the flashers. ("Man, check out that beat!") OK, a little bit far fetched, but illustrates a sneak circuit...with no component failures.

The latent nature of sneak circuits and the realization that they are found in all types of electrical/electronic systems necessitates the application of SCA to any system that is required to operate with a high reliability. Examples are military aircraft and missile systems that play an important role in the national security.

The SCA of military systems has included manned and unmanned aircraft and missiles. SCA as applied to aerospace systems has encompassed NASA hardware, including manned spacecraft, satellites, aircraft, experimental aircraft systems, launch vehicles, and interplanetary probes. Commercial/nuclear analyses included nuclear plant safety subsystems, aircraft autopilot systems, offshore oil equipment, and rapid transit systems.

The results of the analyses represent the number of undesired conditions discovered during analysis of that system. The primary product of an SCA is the reporting of sneak circuits. Other circuit or system conditions which cannot be classified as sneak circuits, but which should be reconsidered by the designer, are classified as design concern conditions. In the course of each analysis input, data errors are also identified. Using detail (manufacturing) level drawings as a basis for SCA results in the identification of data errors, some of which are translated into hardware. The large number of problems on some projects can be attributed to similar or identical circuits or configurations occurring many times and to the overall size of the system. The depth of detail of SCA and the resultant overview of the system allows the identification of all sneak circuit conditions present.

The fact that the circuits can be broken down into the patterns shown allows a series of clues to be applied for recognition of possible sneak circuit conditions. These clues help to identify combinations of controls and loads that are involved in all types of sneak circuits. Analysis of the node-topographs for sneak circuit conditions is done systematically with the application of sneak circuit clues to one node at a time. When all of the clues that apply to a particular pattern have been considered, it is assured that all possible sneak circuits that could result from that portion of the circuit have been identified. The clues help the analyst to determine the different ways a given circuit pattern can produce a "sneak."

There are four basic categories of sneak circuits that will be found.

a. Sneak Paths--allow current to flow along an unsuspected route.

b. Sneak Timing--causes functions to be inhibited or to occur unexpectedly.

c. Sneak Labels--cause incorrect stimuli to be initiated.

d. Sneak Indicators--cause ambiguous or false displays.

In addition to the identification of sneak circuits, results include disclosure of data errors and areas of design concern. Data errors are identified and reported incrementally on Drawing Error Reports from the time of data receipt through the analysis period. These errors generally consist of lack of agreement between or within input documents. Conditions of design concern are primarily identified during the network tree analysis. Design concern conditions include:

a. Unsuppressed or improperly suppressed inductive loads,

b. Excess or unnecessary components,

c. Lack of redundancy, and

d. Failure points.

The three resultant products of SCA (sneak circuit, design concern, and drawing error conditions) are reported via three separate report formats: reference data, circuit affectivity, and an explanation of the condition found, illustrated as required, and with a recommendation for correction.

9.5 Energy Trace. (9:59-70)

This hazard analysis approach addresses all sources of uncontrolled and controlled energy that have the potential to cause a mishap. Sources of energy-causing mishaps can be associated with the product or process, the resource if different than the product/process, and the items/conditions surrounding the system or resource of concern. A large number of hazardous situations is related to uncontrolled energy associated with the product which is usually the resource being protected. However, some hazards are passive in nature (e.g., sharp edges and corners are a hazard to an astronaut's suit during space walks) or are associated with energy sources external to the resource being protected.

The main purpose of the energy source analysis is to ensure that all hazards and their immediate causes are identified. Once the hazards and their causes are identified, they can be used as top events in a fault tree, be used to verify the completeness of an FMEA, etc. Consequently, the energy source analysis method complements but does not replace other analyses, such as fault trees, sneak circuit analyses, event trees, FMEAs, etc.

Identification of energy sources and energy transfer processes is the key element in the energy source analysis procedure. Once sources of energy have been identified, the analyst considers the ways in which controlled and uncontrolled energy could be dissipated and thus interacts adversely with other components and ultimately with the resource being protected.

These analyses point out potential unwanted conditions that could conceivably happen. Each condition is evaluated further to assess its hazard potential. If it is determined to have hazard potential, then the chance/likelihood of the event is determined in qualitative or quantitative terms. If the hazard is deemed to be credible, safety controls are established to eliminate or control the risk based on classification of the hazard as being catastrophic or critical. This process of hazard identification leads to a balanced design; it minimizes the chance of systems being over or under designed from a safety point of view. Finally, verification procedures are specified to close the hazard analysis process.

Fourteen steps in the energy source hazard analysis procedure are described next. The sequence of steps described below should be viewed as a guideline—certainly the analyst has the prerogative to deviate from the suggested order. An iterative process may also be desirable depending upon the complexity of the system being analyzed.

Energy Source Hazard Analysis Process

Step 1: Identify the resource being protected (personnel or equipment). This item is used to guide the direction of the analysis towards the identification of only those conditions (i.e., hazards) that would be critical or catastrophic from a mission viewpoint.

Step 2: Identify system and subsystems and, if a particular component warrants special emphasis, the component of interest.

Step 3: Identify the operational phase(s), such as prelaunch, launch, in orbit, descent (takeoff, cruise, landing), etc., that each system/subsystem/component will experience. It is often desirable to report results of hazard analyses for each separate operational phase.

Step 4: Identify the operating states for the subsystems/ components. These are the component operating states (e.g., on/off, pressurized/unpressurized) during each operational phase.

Step 5: Identify the energy sources or transfer modes that are associated with each subsystem and each operating state. A list of general energy source types and energy transfer mechanisms is presented in Figure 9-1.

Step 6: Identify the energy release mechanism for each energy source (released or transferred in an uncontrolled/unplanned manner). It is possible that a normal (i.e., as designed) energy release could interact adversely with other components in a manner not previously or adequately considered.

Figure 9-1

ENERGY SOURCES AND TRANSFER MODES

SOURCES	
KINETIC	ROTATIONAL
	TRANSLATIONAL
POTENTIAL	GRAVITATIONAL
INTERNAL	STATE EQUATION
HEAT TRANSFER	CONDUCTION
	CONVECTION
	RADIATION

	WORK
TRANSFER MODES	HYDROSTATIC (flow energy)
	BOUNDARY TWISTING (shaft)
	BODY FORCE (gravitational)
	BOUNDARY STRETCHING (surface tension)
	TANGENTIAL MOTION (shear)
	ELECTRICAL (charge)
	MAGNETIZATION (magnetic field)
	POLARIZATION (electric field)
	CHEMICAL (electrochemical potential)

Step 7: For each component and energy source or transfer mode, review a generic threat checklist. Experience has shown that certain threats are associated with specific energy sources and components.

Step 8: Identify causal factors associated with each energy release mechanism. A hazard causal factor may have subordinate or underlying causal factors associated with it. For instance, excessive stress may be a “top level” factor. The excessive stress may, in turn, be caused by secondary factors such as inadequate design, material flaws, poor quality welds, excessive loads due to pressure or structural bending, etc. By systematically evaluating such causal factors, an analyst may identify potential design or operating deficiencies that could lead o hazardous conditions. Causal factors are identifiedindependent of the probability of occurrence of the factor; the main question to be answered is: Can the causal factor occur or exist?

Step 9: Identify the potential mishap that could result from energy released by a particular release mechanism.

Step 10: Define the hazardous consequences that could result given the mishap specified in the previous step.

Step 11: Evaluate the hazard category (i.e., critical, catastrophic, or other) associated with the potential mishap.

Step 12: Identify the specific hazard associated with the component and the energy source or transfer mode relative to the resource being protected.

Step 13: Recommend actions to control the hazardous conditions.

Step 14: Specify verification procedures to assure that the controls have been implemented adequately.

As an accident avoidance measure, one develops strategies for energy control similar to those listed below.

a. Prevent the accumulation by setting limits on noise, temperature, pressure, speed, voltage, loads, quantities of chemicals, amount of light, storage of combustibles, height of ladders, etc.
b. Prevent the release through engineering design, containment vessels, gas inerting, insulation, safety belts, lockouts, etc.
c. Modify the release of energy by using shock absorbers, safety valves, rupture discs, blowout panels, less incline on the ramps, etc.
d. Separate assets from energy (in either time or space) by moving people away from hot furnace, limiting the exposure time, picking up with tongs, etc.
e. Provide blocking or attenuation barriers, such as eye protection, gloves, respiratory protection, sound absorption, ear protectors, welding shields, fire

doors, sunglasses, machine guards, tiger cages, etc.

f. Raise the damage or injury threshold by improving the design (strength, size), immunizing against disease, warming up by exercise, getting calluses on your hands, etc.

g. And by establishing contingency response such as early detection of energy release, first aid, emergency showers, general disaster plans, recovery of system operation procedures, etc. (49:55)

9.6 Evaluation of Analyses (General)

The information in Chapter 9, sections 9.6 - 9.12 was taken from the Guide for Evaluating Hazard Analyses by Harvey "Chuck" Dorney, Chief of System Safety at Air Force Materiel Command. Paragraph numbers have been changed to "Point" numbers to simplify the numbering in this handbook. The superb guidance is otherwise unchanged.

Point 1. This guide provides methods for evaluating hazard analyses (also called system safety analyses). The guide is structured around the classic MIL-STD-882 hazard analyses, but includes other analyses and analytical techniques.

Point 2. This guide is intended for a varying audience that includes:

a. The individual(s) who actually performs the analysis being evaluated. Thus, the guide serves as a self-evaluation tool.

b. Engineering and management personnel in the organization responsible for the item(s) being analyzed. They can evaluate hazard analyses to further examine their own product and they can evaluate the analyses prior to releasing the analyses outside the organization.

c. System safety personnel outside the organization who have expertise in hazard analyses, but not necessarily familiar with the details of the item being analyzed.

Figure 9-2

METHODS OF RESOLVING HAZARDS

(example: failure to extend landing gear prior to landing)

RESOLUTION METHOD (IN ORDER OF PREFERENCE)	EXAMPLE
Change the design to eliminate the hazard	Use fixed (non- retractable) landing gear. usually unacceptable due to aircraft performance considerations
Use safety devices	Have landing gear automatically extend when certain parameters (air speed, altitude, power setting) are met. Difficult to establish parameters. May need to override system for certain flight characteristics.
Use warning devices	Provide a warning light, horn, or voice if the landing gear is not down and locked when certain aircraft parameters are met.
Use special training and procedures	Instruct pilot to extend gear prior to landing. Place a step "**Landing Gear - Down**" in the aircraft procedures.

d. This guide could also be an information source for individuals outside the responsible organization who are intimately familiar with the item(s) being analyzed, but are not familiar with system safety analyses.

Point 3. When evaluating any hazard analysis, the user of this guide must keep in mind the main purpose of the analysis:

a. To identify actual and potential hazards, including those that may occur from either simultaneous or sequential failures and from "outside" influences, such as environmental factors or operator errors.

b. To assess each identified hazard. A realistic assessment considers the hazard severity (i.e., what is the worst that can happen?) and the potential frequency of occurrence (i.e., how often can the mishap occur?). Risk as a function of expected loss is determined by the severity of loss and how often the loss occurs. Loss rate or frequency is a function of hazard frequency and the probability of the loss, given hazard occurrence. Some hazards are present all the time, or most of the time, but do not cause losses.

c. To recommend methods of resolving the hazard, i.e., what should we do about it? Possible solutions are shown in Figure 9-1.

Point 4. Timeliness is an important consideration for evaluating a hazard analysis. Only system safety documents specify the appropriate times for completing and submitting hazard analyses.

For example, a preliminary hazard analysis (PHA) should typically be completed in time to ensure that safety requirements are included in specifications and interface documents, and submitted sometime prior to the preliminary design review. For a program being bided on, bidders should be instructed to submit a draft PHA with the proposal. This initial PHA would provide a basis for evaluating the bidder 's system safety program. As more design specifications and details emerge, the PHA should be revised. System and subsystem hazard analyses are typically submitted prior to the critical design review. However, these analyses cannot be "really" complete until the design is finalized, and that occurs after the critical design review (CDR). Finally, operating (and support) hazard analyses are typically submitted after operating, servicing, maintenance and overhaul procedures are written prior to initial system operation. Whatever the schedule, the most important evaluation criteria is:

THE ANALYSIS MUST BE DONE IN TIME TO REALLY DO SOME GOOD.

If a system hazard analysis is done late, what good will it do, particularly if the design has already been established and fabrication has begun? Look at the timeliness of the analysis and determine whether or not it was done to "fill a contractual square" or to satisfy some other program requirements. Even though the report of the analysis was submitted in time, evaluation must consider if it was a "last minute" job.

Remember, the submitted document is a report of analysis, which may have been started many months before the report, was submitted. Some of the giveaways are:

a. Overly good-appearing binder, title page, etc., which may be making up for a not-so-complete report.

b. Lack of detail in the reports. Be careful though, this lack of detail may also be due to insufficient experience or knowledge on the analyst's part, or due to lack of detailed design information at the time.

c. Hazards are corrected by procedure changes, rather than designed out. This indicates that hazards were detected too late to impact the design.

d. Verification tests for corrective actions are not defined or scheduled. This indicates poor integration between design, safety, and test personnel or an inadequate understanding of system safety impact on the test program.

e. Lack of specific recommendations. Some incomplete or late hazard reports may have vague recommendations such as: "needs further evaluation" or "will be corrected by procedures". Also, look for recommendations which could have/should have been acted on by the contractor and closed out before the report was submitted. You should not see recommendations to make the design comply with contractual specifications and interface requirements.

Point 5. Let's look some more at actions on identified hazards. If MIL-STD-882 Task 105 is on contract, this should be very specific and show positive means of tracking the actions. Ideally, the final corrective actions should be stated in the analysis. However, in most cases, this is not possible because the design may not be finalized, or procedures have not been written. In either case, identify actions that control risk to acceptable levels. For example, if a hazard requires procedural corrective action, the report should state where the procedure will be found, even if it will be in a document not yet written. If the corrective action is a planned design change, the report should state that, and how the design change will be tracked (i.e., who will do what and when). In any case, look for specific risk control actions. Identified hazards should be listed into a hazard tracking and resolution system.

Point 6. If specific risk control actions are not yet known (as can happen in some cases), there are two main options:

a. Leave the analysis continually on going and periodically revise the report as risk control actions are implemented. (This will require a contract change proposal if outside the scope of the original statement of work (SOW). For example, a subsystem hazard analysis might recommend incorporating an automatic wing flap extension system for low speed flight. After alternatives have been evaluated and a decision has been made, the report should be revised to include "Flaps will be automatically extended below 200 knots."

b. Close the analysis, but indicate how to track the recommendation. (Provisions for tracking such recommendations must be within the scope of the contract.) This is usually done for a preliminary hazard analysis (PHA) which is rarely revised. For example, a PHA may recommend a backup emergency hydraulic pump. The analysis should state something like "...recommend emergency hydraulic pump that will be tracked under Section L of the hydraulic subsystem hazard analysis." This method works fine so long as the contract requires the analyst to develop a tracking system to keep hazards from getting lost between one analysis and the next. The presence of a centralized hazard tracking system is a good indictor of a quality system safety program.

Point 7. Who did the analysis being evaluated? This is an important consideration because there can be some pitfalls:

a. The analysis may be done by an experienced system safety person who is not familiar with the system being analyzed. The system safety engineer should not only be familiar with the subsystem being analyzed, but he should also have some prior experience with the subject. Otherwise, he may lack the understanding that is needed to perform an analysis that would have sufficient detail to identify all the hazards.

b. The analysis may be done by an experienced engineer (for the system involved) but lacks system safety experience. He would have difficulty starting out the analysis, particularly a fault tree.

c. Obviously, the best solution is to have the system safety engineer and subsystem engineer work together on each analysis. They will need to establish a good working relationship in order to complement each other. Most organizations have a separate system safety staff, but a few will hale system safety engineers located within each subsystem area (i.e., fuel, hydraulic, etc.). This is the best working relationship, but generally requires more overall manpower.

d. The system safety program plan should specify which individual has the authority to close each hazard.

Point 8. A few system safety analyses get their start from failure modes and effects analyses (FMEAs) prepared by reliability engineers. The FMEAs get modified into system safety analyses by adding a hazard category or other appropriate entries. This technique will save manpower and funds, but has some disadvantages:

a. Hazards may be left dangling with no specified corrective action.

b. Upstream and downstream effects may not always be identified.

c. Sequential or multiple hazards may not be identified.

d. Obvious hazards may be missing.

e. Many hazards are not a result of component failures (e.g., human errors, sneak circuits).

f. If all reliability data is used, time will be wasted on adding safety entries on non-safety critical systems.

g. Human error hazards might not be identified.

Point 9. Require the analyst to include the sources of design data used in the analysis. The obvious sources are system layout and schematic diagrams, and physical inspections. Did the analyst also use generic sources such as AFSC Design Handbook 1-6 (System Safety) and 1-X (System Safety

Checklists)? There are others, such as the Air Force lessons learned data bank at Wright-Patterson AFB, Ohio. These generic sources will help to "trigger" the analyst to consider hazards that otherwise would go uncovered. Finally, the analyst should obtain experience and mishap data for systems that are related to the ones being evaluated.

Point 10. Hazard analyses will be written in one of three basic formats:

a. The matrix format is the most widely used. This method lists the component parts of a subsystem on a preprinted form that includes several columns, the number of which can vary according to the analysis being done. As a minimum, there should be columns for each of the following:

1) Name of the item(s).
2) Function of the item(s).
3) Type of hazards.
4) Category (severity) of the hazards.
5) Probability of the hazards.
6) Recommended corrective action

b. Logic diagrams, particularly fault trees, are used to focus on certain hazards. These are deductive analyses which begin with a defined undesired event (usually a mishap condition) then branch out to organize all faults, subverts, or conditions that can lead to the original undesired event. A separate chapter will cover these analyses in greater detail.

b. The narrative format will suffice for a few cases, such as focusing on a few easily identified hazards associated with simple systems. This format is the easiest to apply (for the analyst), but is the most difficult to evaluate.

c. There is no way to determine if a narrative report covers all potential hazards, so the evaluator is relying totally on the analyst's judgment.

Point 11. Some analyses will employ quantitative (numerical) techniques mainly to highlight or prioritize the greater hazards. quantitative techniques will be covered in a later section.

Point 12. Which hazard analyses should be done? MIL-STD-882 prescribes several analyses, each of which will be treated in separate sections of this guide. The choice, however, is left up to individual managers and engineers. Some large-scale programs may require several hazard analyses, while smaller scale programs may require only one or two analyses. The selection of the types of hazard analyses to be accomplished is the most important aspect when preparing the SOW and negotiating the system safety portion of the contract. If insufficient hazard analyses are designated, the system will not be analyzed properly and many hazards may not be identified. Conversely, if too many or the wrong types of analyses are selected, the system safety effort will be an overkill and will expend valuable monetary and manpower resources needlessly. One rule of thumb: a PHA should always be done for each separate program or project. The PHA provides an initial assessment of the overall program risk and it is used as a baseline for follow-on analyses, such as subsystem, and operating and support hazard analyses. It

also identifies the need for safety tests and is used to establish safety requirements for inclusion in the system's specifications. Therefore, when evaluating any hazard analysis, look for a PHA and see how it was used as a baseline for future system safety efforts.

The next choice is whether or not to do either a subsystem hazard analyses (SSHA) or system hazard analyses (SHA). This choice should be based upon two factors:

a. The nature and use of the system being evaluated.

b. The results of the PHA. If the subject being analyzed has no unresolved safety concerns, then further analyses may not be necessary.

b. If the hazards appear to be based upon training or procedural problems, then an operating and support hazard analysis (O&SHA) may be the next step. Again, the results of the PHA will dictate the need.

c. The complexity of the system being analyzed. A major system, such as an aircraft or battle tank would need separate analyses for different subsystems, then an overall system analysis to integrate, or find the hazards resulting from the interfaces between the different subsystems. On the other hand, an aircraft refueling nozzle should only need one single hazard analysis.

e. For major programs, the choices will have already been made; the contract will require several analyses.

f. The available funding.

The next choice is whether or not to perform an O&SHA. If there is a man/machine interface (almost always the case) an O&SHA should be performed. The sources of information (to help decide) should be the PHA, and consultations with human factors personnel, who should be able to advise of problems associated with operating the equipment. Do not forget tests. The addition of test equipment to a system can greatly change the system, adding severe hazards. Test procedures, especially those concerning safety critical systems can also contribute mishap potential.

Point 13. Formats for analyses will be covered in subsequent chapters. If more than one contractor or organization will be performing analyses, or if one is subcontracted to another, be sure all of them use the same formats, techniques, and definitions or mismatching will occur, and it will be difficult, if not impossible, to correlate the analyses. In addition, the analyses should use compatible computer data formats so that interface analyses can be expedited by direct data transfer.

9.7 Preliminary Hazard Analysis Evaluation

Point 1. The first analysis to be evaluated is the Preliminary Hazard Analysis (PHA), which is an initial assessment of the anticipated safety problems within a system. The PHA's is not a detailed analysis; it covers the broad areas of a system, but leaves the details for future analyses. The results of the PHA will dictate which analyses need to be performed as the system design develops, what safety tests need to be performed, and helps define safety design requirements for inclusion in the system's specifications and interface control documents.

Point 2. Was a PHA accomplished? If not, look carefully at the management of the particular system safety program in mind. A PHA should always be done. Without an initial analysis, how can an effective system safety program be planned? Before evaluating any type of system safety

analysis, look for, and evaluate the PHA. Given that a PHA has been performed, there are three main areas of evaluation: The format of the PHA, the level of detail, and the proposed resolution of identified hazards.

Point 3. The PHA format should be carefully chosen after considering the objectives of the analysis.

a. The tabular, or matrix, format is the most widely used format for a PHA, primarily because it provides a convenient assessment of the overall hazards to a system. The basic tabular format may have entries for potential hazard sources, such as energy sources (i.e., electrical, pneumatic, mechanical, etc.). This PHA would list all known electrical energy sources with their initial hazard assessments, and then recommended corrective action. The PHA would then list other energy sources and continue on. When evaluating an "energy source" PHA, be sure it includes special energy sources, such as nuclear, laser, RF,
etc. Some of these may be skipped and need to be added later (usually too late to do much good).

b. Another type of tabular format PHA would list key hazards (such as fire, explosion, etc.) and identify the known potential causes for these events. Again, the evaluator must be assured that the analyst considered an adequate number of potential hazards for the proposed system.

c. In some cases, a tabular PHA may resemble a Failure Modes and Effects Analysis (FMEA). This is rare, but may be appropriate for some systems. This PHA is usually simplified with no numerical data, such as failure rates. These are generally added on later in subsequent analyses. The evaluator should look at the level of detail. Some analysts may attempt to get too detailed when the design details are not yet finalized.

d. Some PHAs will be in the form of a logic diagram or fault tree analysis. These are usually done to identify the major causes of a top undesired event, and are generally not done to a detailed level. Instead, the details are added during subsequent analyses.

e. A few PHAs will be done in a narrative format. Typically, each paragraph will cover an individual hazard, its impact, and proposed resolution. Narrative analyses are preferred for covering a potential hazard in detail, but have the drawback of not having a good tracking system unless tracking numbers are assigned. Narrative PHAs can have provisions for tracking hazards, by limiting each single hazard and by using the paragraph numbers for tracking.

Point 4. A PHA should be open-ended to keep track of identified hazardous areas. For most programs, a PHA is done once and not updated. Future analyses (subsystem and system hazard analyses) take up the effort to identify new hazards as the design progresses. When a PHA is completed, there will be hazards that have not yet been resolve. Some sort of tracking system will be necessary to assure these hazards are not dropped until resolved. Each unresolved hazard should be tracked (usually by a numbering system) to carry over to future analyses. This "tracking system" is probably the easiest area of a PHA to evaluate. Because a PHA is just that, i.e., preliminary, it is difficult to tell whether or not it is really complete or accurate. However, if several obvious potential hazards are not included or if some of the identified hazards are not relevant, the PHA should be suspect. The evaluator should ask these questions:

a. Does the PHA cover all anticipated hazardous areas?

b. Does it establish a baseline for defining future system safety tasks and analyses?

c. Does it allow for adequate tracking of hazards?

d. Are the proposed hazard control actions realistic/implementable?

If the answer to any of the questions is "no", then revising or reaccomplishing the PHA may be necessary. One pitfall may be tuning; by the time a PHA is completed and submitted, there may be insufficient time to do much with it before the program continues on towards future milestones.

9.8 Subsystem Hazard Analysis Evaluation

Point 1. The subsystem hazard analyses (SSHA) are the central parts of any system safety program. These are the detailed analyses that identify hazards and recommend solutions. The design details are known and the analyses cover all details that are necessary to identify all possible hazards. When evaluating an SSHA, keep the following main points in mind:

a. Who did the analysis?
b. Was the format appropriate?
c. What level of detail did the analysis cover?
d. What actions were taken on identified hazards?
e. Is the analysis limited to evaluation of failures or does it consider faults?

Point 2. Who did the analysis? Typically, the system safety organization does the analysis using design data furnished by engineering organizations. Another method is to have the engineering organizations do the hazard analyses using formats and guidance provided by system safety; then to have system safety review, verify, and finalize the analysis. A third method is to have full-time system safety engineers collocated in different engineering organizations to perform the safety analysis. This last approach would result in very comprehensive hazard analyses, but management of resources could be a major problem. Consider interpersonal relationships. For example, would a hydraulics engineer feel "crowded out" by a full-time system safety engineer collocated in his shop? Each approach to be selected will depend on the strength of the organization and resources. We do not know of any experience data that makes an approach, universally better or worse than the others. Each will need to be judged individually. In any case, the analyst must be skilled in system safety analytical techniques and be most intimately familiar with the subsystem being analyzed. Details of the management structure used during the system safety program should be outlined in the system safety program plan. If there is something unusual about the management structure, or if it is different than that specified in the SSPP, the capabilities of the system personnel should be questioned.

Point 3. Was the format used for analysis documentation appropriate for the job? Most SSHAs are documented in the matrix format, while some are fault trees or other forms of logic diagrams. Fault trees, by themselves, are incomplete and do

not directly provide useful information. The utility of fault trees come from the cut and path sets they generate and the analysis of the cut and path sets for common cause failures and independence of failures/faults. Narrative SSHAs are rare; most narrative analyses are PHAs. Fault trees are good for analyzing a specific undesired event, (e.g., rupture of pressure tank) and can find sequential and simultaneous failures, but are time consuming and expensive. The SSHAs must be more detailed than the PHA, and hopefully will show that the subsystem design meets the safety requirements in the subsystem specifications(s). Remember, this is the central part of the system safety program - if hazards are not identified and corrected now, they might not be later on when the subsystem designs are frozen and the cost of making a change is significantly increased.

Point 3.1. Should a reliability analysis be used for an SSHA? Not entirely. Most reliability analyses use the failure modes and effects analysis (FMEA) technique, a matrix type of analysis. This format is partially suitable for an SSHA, because it lists each component, the component function, types of failure, and the effects of the failures. Most FMEAs also include component failure rate information. An FMEA can be used as a basis for an SSHA, but several factors must be considered.

a. Many FMEAs do not list hazard categories (Category I - catastrophic, etc.) which are necessary in the system safety world.

b. Hazards may be left dangling in a reliability analysis. These analyses emphasize failure effects and rates, but not always corrective action.

c. Upstream or downstream effects may not be identified.

d. Failure rate data used by reliability may not be meaningful for safety analyses. Failure rates which meet reliability requirements (normally in the .9 or .99 range) may not be adequate to meet safety requirements (often in the .999999 range). In addition, many reliability failures (leaking actuator) may not be safety failures (ruptured actuator).

e. Sequential or multiple hazards might not be addressed.

f. FMEAs address only failures. They do not include faults.

g. Human factors related to hazards will not be addressed.

In spite of shortcomings, it is normally more cost effective to expand a reliability analysis to include Hazard Category, Hazard Resolution, and other columns, and to modify reliability data which is appropriate for safety to be useful as an SSHA.

Point 3.2. A fault tree analysis (FTA) is ideal for focusing on a single undesired event (e.g., inadvertent rocket motor ignition) but is time consuming and can be expensive. Nevertheless, the FTA should be used for any serious hazard whose causes are not immediately obvious ("0" ring failure) and that needs to be examined in detail because of the concern over the effects of multiple failures and common cause failures. List the undesired events, then perform fault trees for each one. Fault tree analyses are covered in detail in section 9-11.

Point 3.3. Narrative analyses are generally not recommended for an SSHA unless the subsystem under evaluation is relatively small. Narrative analyses do not specify much detail; try to imagine a narrative SSHA on the anti-skid braking system on a Boeing 747.

Point 3.4. Matrix formats are the most common formats for SSHAs. There are many variations, but virtually all of them list key items in tabular form. As a minimum, there should be columns for:

a. The subsystem, item, or component being analyzed.

b. Its function.

c. The potential hazard.

d. The hazard severity.

e. The likelihood of the hazard causing a mishap. Is this likelihood before or after the corrective action?

f. Controls (design, safety device, warning device, procedure and personnel equipment). Reduction of risk (hazard severity and mishap probability), if known.

g. Risk control verification method(s).

h. Corrective action. Recommended corrective actions should include changes which are considered "out-of-scope" of the contract. Corrective changes to bring the subsystem into compliance with contractual requirements should already have been made. Although exceptions are possible (system safety recommendations to change the design can be beat down by other disciplines). When these exceptions occur, documentation in the SSHA report which is delivered just prior to CDR is often too late to react. In addition, the same forces which beat down the original safety recommendation are probably in a position to eliminate the recommendation from the SSHA.

i. Status (open or closed).

Point 4. What level of detail did the analysis cover? The best answer is something like "...whatever detail is necessary to identify all hazards." Sounds nice, but easier said than done. One of the most important aspects of conducting any analysis knows when to stop. It is not always practical to analyze all the way to the individual nut-and-bolt or resistor- and-capacitor level, which seems like an obvious answer. Therefore, judgment must be used, depending on the individual case. To illustrate, let us go to an airliner fuel system:

a. A fuel crossed valve fails partially open. This results in some uncommanded fuel crossfeed (from one tank to another) and usually is not a safety hazard. Therefore, further analysis will not be necessary.

b. A fuel jettison (dump) valve fails partially open. This will result in loss of fuel during flight, so a serious hazard is present. Therefore, it is definitely worthwhile to analyze this valve's failure modes in detail (i.e., operating mechanism, power sources, indicator lights, etc.).

Secondary (undeveloped) and environmental failures requires judgment too. During most fault tree analyses, these failures usually are not developed (i.e., pursued further) as they may be beyond the scope of the analyses. These failures are labeled by diamond symbols in a fault tree.

Point 5. What actions were taken on identified hazards? This is where an analysis can really be worthwhile. We have been talking not only about recommended actions, but also actions already taken and planned follow-up actions. For a matrix

type analysis, it is easy to recommend changing a design or adding a procedural step to control a hazard. It is also easy to close the item based upon a recommended change. Do not let that happen. Keep the item open until the hazard is positively controlled or until someone documents accepting the hazard. Because of contractual requirements (e.g., delivery of final SSHA 90 days prior to CDR), it may be impossible to keep the SSHA open. The options would be to write the CONTRACT so that the " final" SSHA is delivered when the production baseline design is really established or require the hazard to be tracked through TASK 106 of MIL-STD-882 until it is really closed out. For matrix type analyses, tracking can usually be done by printing "open" or "closed" in the column telling the status. It is even easier if the analysis is done on a computer. There are many ways to track hazards, but be sure someone has a good method to keep items open until positive action is taken. MIL-STD-882 can be interpreted to intend that hazard tracking and hazard analysis are two different activities. This can lead to contractual confusion when a contractor plans to stop supporting (with man-hours) the analysis shortly after the required report is delivered.

9.9 System Hazard Analysis Evaluation.

Point 1. This is a short chapter. For the most part, the comments in the previous chapter on SSHA apply also to the system hazard analysis (SHA). Those comments don't need repeating. However, we do need to look at a unique aspect of an SHA. That is, it analyzes the whole system and integrates SSHAs.

Point 2. Ideally, the SHA identifies hazards that apply to more than a single subsystem and were not identified in the SSHAs. Most hazards of this type result from interfaces between subsystems. For example, your new high-tech car might have separate subsystems hazard analyses on the anti-skid braking system and the four-wheel steering system. Let's assume that these subsystem hazard analyses controlled all known critical and catastrophic hazards. Now, we perform a system hazard analysis that identifies a previously undiscovered hazard: rapidly turning the steering wheel at high vehicle speed causes intermittent anti-skid drop-off. That's the idea - look at interfaces between subsystems. In addition, the SHA looks for ways in which safety-critical system level functions can be lost. Going back to the aircraft anti-skid braking subsystem hazard analysis, it is likely that it was performed using information gained from the landing gear design group. But there are many other subsystems, which interface with the anti-skid subsystem. For instance, the cockpit will contain a control panel which turns the anti-skid system on and off and notifies the crew of an anti-skid system failure. This control panel may well be outside the design authority of the landing gear design group and could be left out of the subsystem hazard analysis. Since interface hazards could also exist within hydraulic and electrical power supply interfaces. By looking for all the ways a system level safety critical function can be degraded or lost, the SHA is designed to cut across all interfaces.

Point 3. When evaluating an SHA, look at the system and subsystem definitions. If the overall system (and its subsystems) is not adequately defined, it is pretty tough to perform a good SHA. In most cases, system definition is simple. In one previous example, the car was the system. In an aircraft "system" there are many subsystems, such as flight controls and landing gear.

Point 4. The next hurdle is defining the interfaces between the subsystems. This can be a two-fold problem:

a. Are all the proper interfaces considered? We all know that aircraft flight control subsystems interface with hydraulic power subsystems, but they also interface with electrical, structural, and (sometimes) the weapons delivery subsystems. The evaluator will need to be familiar with the system being analyzed; if not, he can't determine whether or not all interfaces were covered.

b. How were the interfaces considered? For example did the analysis consider both mechanical and electrical connections between two subsystems? Structural? Hydraulic? Again, the evaluator must have a good familiarity with the system being analyzed.

9.10 Operating and Support Hazard Analysis Evaluation.

Point 1. The operating and support hazard analysis (O&SHA) identifies hazards during use of the system. It encompasses operating the system (primarily procedural aspects) and the support functions (maintenance, servicing, overhaul, facilities, equipment, training, etc.) that go along with operating the system. Its purpose is to evaluate the effectiveness of procedures in controlling those hazards, which were identified as being controlled, by procedures, instead of by design, and to ensure that procedures do not introduce new hazards.

Point 2. When evaluating the O&SHA, look at its timing. Generally, an OSHA's output (i.e., hazard control) is safety's blessing on "procedures". In most cases, procedures aren't available for analyses in the O&SHA until the system begins initial use or initial test and evaluation. As a result, the O&SHA is typically the last formal analysis to be completed. However, don't let an analyst think that the O&SHA is the last analysis to begin. Actually, the sooner the better. Even before the system is designed, an O&SHA can be started to identify hazards with the anticipated operation of the system. Ideally, the O&SHA should begin with the formulation of the system and not be completed until sometime after initial test of the system (which may identify additional hazards). This is critical because design and construction of support facilities must begin far before the system is ready for fielding and all special safety features (e.g., fire suppression systems) must be identified early or the costs to modify the facilities may force program managers and users to accept unnecessary risks.

Point 3. When evaluating an O&SHA, it's important to keep in mind the definition of operating the "system". We' re not only talking about normal operation of the system, but abnormal, emergency operation, system installation, maintenance, servicing, storage, and other operations. We must also consider misuse and emergency operations. In other words, if anyone will be doing anything with the system, planned or unplanned, the O&SHA should cover it.

Point 4. It's also important to consider the support aspects of an O&SHA. Be sure the analysis includes:

a. Auxiliary equipment (loading handling, servicing, tools, etc.) that are planned to be used with the system.

b. Training programs. Who will do the training, when, and how? What training aids will be used? Mock-ups and simulators may definitely be needed for complex systems.

c. Procedures, manuals, etc. These must be reviewed and revised as needed to eliminate or control hazards. For this effort, it's important to assure that the analyst has a good working relationship with the organization developing the procedures. If procedures are revised for any reason, the analyst needs to be in the loop.

d. Handling, use, storage, and disposal procedures for hazardous materials.

Point 5. How much human factors consideration was put into the analysis? There had better be plenty: The O&SHA should be done in concert with the human factors organization. There is a pressing need to set system safety and human factors functions more closely entwined. This has been evidenced by many mishaps or accidents that were caused by operator error. We need to goof-proof the equipment, and the O&SHA is the method. Ideally, the O&SHA should be done and signed by system safety and human factors organizations. But, if a dual signature requirement is not in the contract, don't expect it on the O&SHA.

Point 6. O&SHAs are normally completed and submitted as a single package done in a matrix format. For a complex system, look for an analysis that is comprised of several separate analyses, such as for maintaining and servicing the system (sometimes called maintenance hazard analysis). This should go into the hazards of disconnecting and re-applying power, using access doors and panels, hardstands, etc. Past systems have had enough maintenance mishaps, that a separate analysis is definitely justified.

Point 7. The O&SHA should also include expanded operations, i.e., anticipate using the system for additional operations not specified in the original design. For example, an O&SHA should normally cover the hazards of aircraft refueling and separate weapons loading. However, few O&SHAs have covered the hazards of simultaneous refueling and weapons loading (as in a combat scenario). There could be many new hazards identified the hard way (by mishaps) instead of during the design stages (knowing these hazards ahead of time). For example, an aircraft fuel vent outlet could be relocated to remove fuel vapors away from weapons loading equipment with hot engines. The way to get these "expanded operations" O&SHAs is to ensure that such a requirement is included and defined in the contract.

9.11 Fault Tree Analysis Evaluation.

Point 1. Fault tree analysis (FTA) is a technique that can be used for any formal program analysis (PHA, SSHA, O&SHA). It, therefore, makes more sense to cover the FTA in a separate section instead of in the previous chapters. A complete description of FTA can be found in the U.S. Nuclear Regulatory Commission's NUREG - 0492 "Fault Tree Handbook". (Jan 1981)

Point 2. The FTA is one of several deductive logic model techniques, and is by far the most common. The FTA begins with a stated top-level hazardous/undesired event and uses logic diagrams to identify single and combinations of events that could cause the top event. The logic diagram can then be analyzed to identify single and multiple events, which can cause the top event. When properly done, it shows all the problem areas and makes the critical areas stand out. The FTA has two drawbacks:

a. Depending on the complexity of the system being analyzed, it can be time consuming, and therefore very expensive.

b. It does not identify all system failures; it only identifies failures associated with the top event being analyzed. For example, an FTA will not list all failures in a home water heater, but will show all failures that lead to an event such as "catastrophic water heater rupture".

Point 3. The first area of evaluation (and probably the most difficult) is the top event. This top event should be very carefully defined and stated. If it is too broad (e.g., aircraft crashes), the resulting FTA will be overly large. On the other hand, if the top event is too narrow (e.g., aircraft crashes due to pitch-down caused by broken bellcrank pin), then the time and expense for the FTA may not yield significant results. The top event should specify the exact hazard and define the limits of the FTA. In this example, a good top event would be "uncommanded aircraft pitch-down" which would center the fault tree around the aircraft flight control system, but would draw in other factors, such as pilot inputs, engine failures, etc.

In some cases, a broad top event may be useful to organize and tie together several fault trees. In our example, the top event would be "aircraft crash"; this event would be connected to an OR-gate having several detailed top events as shown in Figure 9-3. However, these fault trees do not lend themselves to quantification because the factors which tie the occurrence of a 2nd level event to the top event are normally outside the control/influence of the operator (e.g., an aircraft which experiences loss of engine power may or may not crash depending on altitude at which the loss occurs).

Point 4. A Quick evaluation of a fault tree may be possible by looking at the logic gates. Most fault trees will have a substantial majority of OR-gates. If fault trees, have too many OR-gates every fault of event may lead to the top event. This may not be the case, but a huge majority of OR-gates will certainly indicate this.

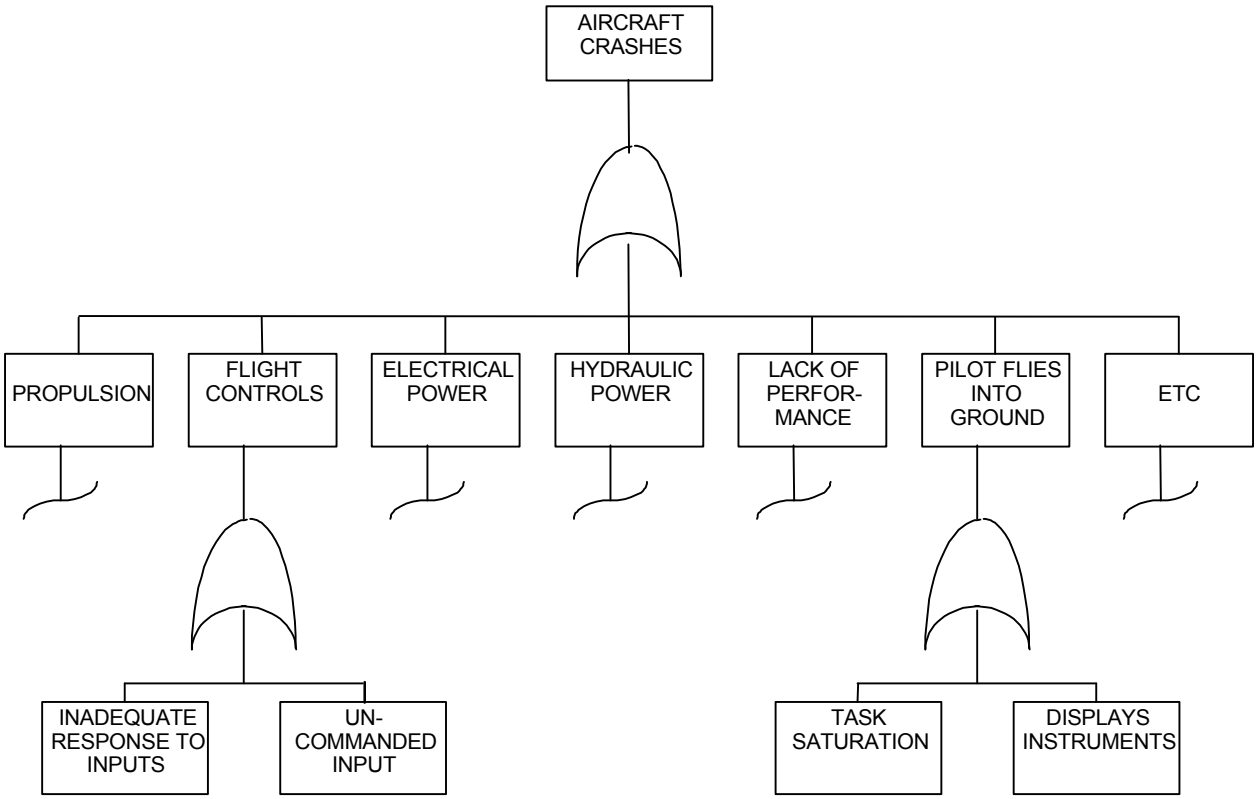
Point 5. While we are talking about gates and logic symbols, an evaluator needs to be sure that logic symbols are well defined and understood. If nonstandard symbols are used, be sure they do not get mixed with other symbols or get misunderstood.

Point 6. Check for proper control of transfers. Occasionally, a transfer number may be changed during fault tree construction. If the corresponding subtree does not have the same transfer number, then improper logic will result and cut sets may be lost.

Point 7. Cut sets (minimum combinations of events that lead to the top event) need to be evaluated for completeness and accuracy. One way to check is to see if the fault tree is reduced to minimum cut sets, so that faults or subevents are not needlessly repeated elsewhere in the tree. For example, the fault tree in Figure 9-4, can be reconstructed to have fewer events and gates. The only drawback to reconstructing a fault tree is that the original logic might be lost. Events C and D, and their affected design features, would no longer be traceable.

Point 8. Each fault tree should include a list of minimum cut sets. Without this list, it is pretty tough to identify critical faults or combinations of events. For large or complicated fault trees, a computer will be necessary to catch all the cut sets; it is nearly impossible for a single individual to find all the cut sets.

Figure 9-3



Point 9. For a large fault tree, it may be difficult to determine whether or not the failure paths were completely developed. If the evaluator is not totally familiar with the system, he may need to rely upon other means. A good clue is the shape of the symbols at the branch bottom. If the symbols are primarily circles (primary failures), the tree is likely to be complete. On the other hand, if many symbols are diamonds (secondary failures or areas needing development), then it is likely the fault tree needs expansion.

Point 10. Faulty (pun?) logic is probably the most difficult area to evaluate, unless the faults lie within the gates, which are relatively easy to spot. A gate-to-gate connection shows that the analyst might not completely understand the workings of the system being evaluated. Each gate must lead to a clearly defined specific event, i.e., what is the event and when does it occur. If the event consists of any component failures that can directly cause that event, an OR-gate is needed to define the event. If the event does not consist of any component failures, look for an AND- or INHIBIT-gate.

Point 11. Be critical of any large fault tree that was not done with the aid of a computer of some sort. Granted, a large fault tree can be done manually, but a good computerized fault tree can make a number to tasks simpler:

a. Logic errors and event (or branch) duplications can be quickly spotted.

b. Cut sets (showing minimum combinations leading to the top event) can be listed.

c. Numerical calculations (e.g., event probabilities, etc.) can be quickly done.

d. A neat, readable, fault tree can be drawn.

Point 12. If one event in a quantitative fault tree has the majority of the probability, but it is not identified in the summary as a primary cause factor, the fault tree could be suspect.

9.12 Quantitative Techniques Evaluations

Point 1. This chapter discusses evaluation of analyses that use quantitative techniques, or using numbers for various purposes including:

a. Establishing overall risk levels (usually specified in terms of hazard severity and hazard probability).
b. Determining areas that need particular attention due to their higher probabilities of a failure or hazard.
c. Fine-tuning or revising the analysis to include more detailed information or analysis as needed.

Point 2. Overall risk is expressed by looking at the combination of hazard severity (i.e., what's the worst that can happen) and hazard probability (i.e., how often will it happen?). This is a realistic and widely accepted approach. A high-level hazard can have a low risk. For example, an aircraft wing separation in-flight is definitely a catastrophic hazard, but under normal flight conditions, it's not likely to occur, so the risk is relatively low. At the other end of the spectrum, many jet engines spill a small amount of fuel on the ground during

shutdown. This is a relatively small hazard with a high probability of occurrence, but again, the overall risk is low.

Point 3. Judgment is needed for preparing an analysis and for evaluating it. First, look at the hazard levels. An analyst mightjudge a flight control bellcrank failure as a Category II or III hazard because its failure still gives the aircraft “get home” capability with reduced control response. On the other hand, if the bellcrank fails during a 4G pull-up, the aircraft might hit the ground. Now it ‘s a Category I hazard. Judgment is also needed for hazard probabilities.

Point 4. The most accurate method for determining hazard probabilities is to use component failure rates (e.g., valve xxx will fail to close 6 x 10-5/hr.). However, here are some pitfalls that need to be considered during evaluation:

a. Where did the failure rates come from? Industry data sources? Government data sources? Others? What is their accuracy?

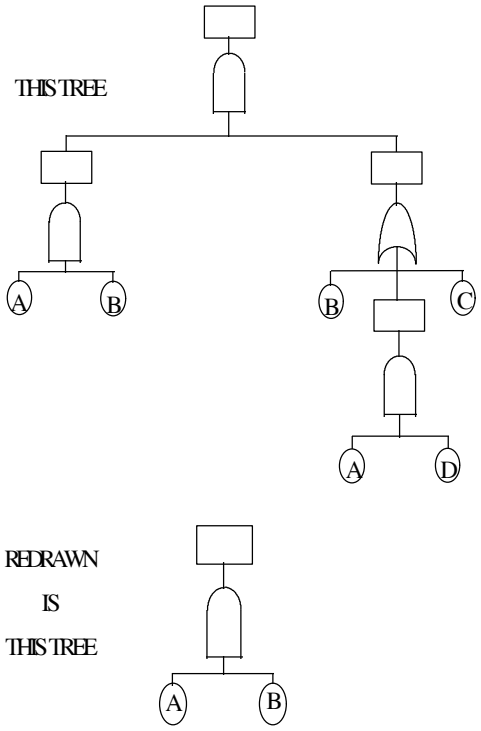
b. If the component has a usage history on a prior system, its failure rate on the new system might be the same. However, the newer system might subject the component to a different use cycle or environment, and significantly affect the failure rate.

c. For newly developed components, how was the failure rate determined?

Point 5. Any of the above techniques can be used successfully. If more than one contractor or organization will be performing analyses, or if one is subcontracted to another, try to get all of them to use the same definitions of probability levels, or some mismatching will result.

Figure 9-4

FAULT TREE SIMPLIFICATION



CHAPTER 10

SYSTEM SAFETY LIFE-CYCLE ACTIVITIES

10.1 Concept Exploration Phase Activities.

General life cycle activities of defense systems have been discussed. Now consider the life cycle processes, this time looking specifically at the role of system safety, keeping in mind the roles of other participants in the entire cycle.

Because of the possibility that some new system may prove to be so valuable that it goes directly from the exploratory development to production-deployment with but a quick pass through the earlier life cycle phases, it would be wrong to wait until a formal life cycle process is commenced to undertake any system safety activity.

During the development of a new technology, system safety concerns should be documented. The documentation will provide the system safety background data necessary should a decision be made to implement technology within a system development program. This is particularly true of exotic and/or radically new systems that may go almost directly from research to full-scale production.

The system safety activities in the concept exploration phase might be divided into two primary functions: one for the system, and one for the program. The safety activities for the system involve the determination of the state of the safety and the requirements for safety for the various alternatives that are under consideration. This determination is used—along with many other determinations—to make a decision as to which of the alternatives will be accepted as the program system.

The safety activities for the program involve getting the program started in such a manner that it can continue throughout the life cycle. The earlier that system safety can be inserted into the program, the easier its functions will be. (33:23)

System safety tasks include the following: (30:B-1 to B-2)

a. Prepare an SSPP to describe the proposed integrated system safety effort for the concept exploration phase.

b. Evaluate all considered materials, design features, maintenance servicing, operational concepts, and environments that will affect safety throughout the life cycle. Consider hazards which may be encountered in the ultimate disposition of the entire system, or components thereof, or of dedicated support equipment, which encompasses hazardous materials and substances.

c. Perform a PHA to identify hazards associated with each alternative concept.

d. Identify possible safety interface problems, including problems associated with software-controlled system functions.

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

f. Review safe and successful designs of similar systems for consideration in alternative concepts.

g. Define the system safety requirements based on past experience with similar systems.

h. Identify safety requirements that may require a waiver during the system life cycle.

i. Identify any safety design analysis, test, demonstration, and validation requirements.

j. Document the system safety analyses, results, and recommendations for each promising alternative system concept.

k. Prepare a summary report of the results of the system safety tasks conducted during the program initiation phase to support the decision-making process.

l. Tailor the system safety program for the subsequent phases of the life cycle and include detailed requirements in the appropriate demonstration and validation phase contractual documents.

10.2 Production Definition and Risk Reduction (PDRR) Activities.

The system safety tasks in this phase describe the proposed integrated system safety effort planned for demonstration and validation. The design process is a continuous series of tradeoffs, and the system safety personnel must ensure that risks are considered during these tradeoffs.

System safety requirements for system design and criteria for verifying that these requirements have been met must be established, the preliminary hazard analyses are updated, and detailed hazard analyses are performed to determine the risk involved in system hardware and system software. (49:24)

Tasks during the PDRR phase will be tailored to programs ranging from extensive study and analyses through hardware development to prototype testing, demonstration, and validation. System safety tasks will include the following: (30:B-3 to B-4)

a. Prepare or update the SSPP to describe the proposed system safety effort planned for the demonstration and validation/concept design phase.

b. Participate in tradeoff studies to reflect the impact on system safety requirements and risk. Recommend system design changes based on these studies to make sure the optimum degree of safety is achieved consistent with performance and system requirements. For munitions or systems involving explosive items, this will include explosive ordnance disposal design considerations.

c. Perform or update the PHA done during the concept exploration phase to evaluate the configuration to be tested. Prepare an SHA report of the test configuration considering the planned test environment and test methods.

d. Establish system safety requirements for system design and criteria for verifying that these requirements have been met. Identify the requirements for inclusion in the appropriate specifications.

e. Perform detailed hazard analyses (SSHA or SHA) of the design to assess the risk involved in test operation of the system hardware and software. Obtain and include risk assessment of other contractor's furnished equipment, or GFE, and all interfacing and ancillary equipment to be used during system demonstration tests. Identify the need for special tests to demonstrate/evaluate safety functions.

f. Identify critical parts and assemblies, production techniques, assembly procedures, facilities, testing, and inspection requirements which may affect safety and will make sure:

(1) Adequate safety provisions are included in the planning and layout of the production line to establish safety control of the demonstration system within the production processes and operations.
(2) Adequate safety provisions are included in inspections, tests, procedures, and checklists for quality control of the equipment being manufactured so that safety achieved in design is maintained during production.
(3) Production and manufacturing control data contain required warnings, cautions, and special safety procedures.
(4) Testing and evaluation are performed on early production hardware to detect and correct safety deficiencies at the earliest opportunity.
(5) Minimum risk is involved in accepting and using new design, materials, and production and test techniques.

g. Establish analysis, inspection, and test requirements for GFE or other contractor-furnished equipment (hardware, software, and facilities) to verify prior use that applicable system safety requirements are satisfied.

h. Perform operating and support hazard analyses of each test and review all test plans and procedures. Evaluate the interfaces between the test system configuration and personnel, support equipment, special test equipment, test facilities, and the test environment during assembly, checkout, operation, foreseeable emergencies, disassembly, and/or teardown of the test configuration. Make sure hazards identified by analyses and tests are eliminated or the associated risk is minimized. Identify the need for special tests to demonstrate or evaluate safety-of-test functions.

i. Review training plans and programs for adequate safety considerations.

j. Review system operation and maintenance publications for adequate safety considerations and ensure the inclusion of applicable Occupational Safety and Health Administration (OSHA) requirements.

k. Review logistic support publications for adequate safety considerations and ensure the inclusion of applicable US Department of Transportation (DOT), US Environmental Protection Agency (EPA), and OSHA requirements.

l. Evaluate results of safety tests, failure analyses, and mishap investigations performed during the demonstration and validation phase. Recommend redesign or other corrective action (this subparagraph does not apply to the facility concept design phase).

m. Make sure system safety requirements are incorporated into the system specification document based on updated safety studies, analyses, and tests.

n. Prepare a summary report of the results of the system safety tasks conducted so far to support the decision-making process.

o. Continue to tailor the system safety program. Prepare or update the SSPP for the engineering and manufacturing development phase and production phase.

10.3 Engineering and Manufacturing Development (EMD) Activities.

The requirements for this phase include the preparation or updating of the SSPP, the review of preliminary engineering designs to make certain that safety requirements are incorporated and that the hazards identified during earlier phases are eliminated or the associated risks reduced to an acceptable level.

The subsystem hazard analyses (SSHA), the system hazard analyses (SHA), and the operating and support hazard analyses (O&SHA) are performed and any necessary design changes are recommended. Here may be the first chance to analyze actual, specific hardware items. This may also be the first opportunity to see all of the systems so as to make full system interface analyses as well as the operating and support interfaces. (33:25)

To support the system engineering program, the system safety tasks during the EMD/final design phase will include the following: (30:B-5 to B-6)

a. Prepare or update as applicable the SSPP for the EMD phase. Continue effective and timely implementation of the SSPP during facility final design phase.

b. Review preliminary engineering designs to make sure safety design requirements are incorporated and hazards identified during the earlier phases are eliminated or the associated risks reduced to an acceptable level.

c. Update system safety requirements in specification/design documents.

d. Perform or update the SSHA, SHA, and O&SHA and safety studies concurrent with the design/test

effort to identify design and/or operating and support hazards. Recommend any required design changes and control procedures.

e. Perform an O&SHA for each test, and review all test plans and procedures. Evaluate the interfaces between the test system configuration and personnel, support equipment, special test equipment, test facilities, and the test environment during assembly, checkout, operations, foreseeable emergencies disassembly, and/or teardown of the test configuration. Make sure hazards identified by analyses and tests are eliminated or their associated risks controlled. Identify the need for special tests to demonstrate or verify system safety functions. Establish analyses, inspection, and test requirements for other contractors' or GFE/GFP (hardware, software, and facilities) to verify prior to use that applicable system safety requirements are satisfied.

f. Participate in technical design and program reviews and present results of the SSHA, SHA, and/or O&SHA.

g. Identify and evaluate the effects of storage, shelf life, packaging, transportation, handling, test, operation, and maintenance on the safety of the system and its components.

h. Evaluate results of safety testing, other system tests, failure analyses, and mishap investigations. Recommend corrective action.

i. Identify and evaluate safety considerations for tradeoff studies.

j. Review appropriate engineering documentation (drawings, specifications, etc.) to make sure safety considerations have been incorporated.

k. Review logistic support publications for adequate safety considerations, and ensure the inclusion of applicable DOT, EPA, and OSHA requirements.

l. Verify the adequacy of safety and warning devices, life support equipment, and personal protective equipment.

m. Identify the need for safety training and provide safety inputs to training courses.

n. Provide system safety surveillance and support of test unit production and of planning for production and deployment. Identify critical parts and assemblies, production techniques, assembly procedures, facilities, testing, and inspection requirements which may affect safety and will ensure:

(1) Adequate safety provisions are included in the planning and layout of the production line to establish safety control of the demonstration system within the production process and operations.
(2) Adequate safety provisions are included in inspections, tests, procedures, and checklists for quality control of the equipment being manufactured so that safety achieved in design is maintained during production.
(3) Production and manufacturing control data contain required warnings, cautions, and special safety procedures.

(4) Testing and evaluation are performed on early production hardware to detect and correct safety deficiencies at the earliest opportunity.

(5) Minimum risk is involved in accepting and using new designs, materials, and production and test techniques.

o. Make sure procedures developed for system test, maintenance, operation, and servicing provide for safe disposal of expendable hazardous materials. Consider any material or manufactured component (whether or not an identifiable spare part or replenishable component) when access to hazardous material will be required by personnel during planned servicing, teardown, or maintenance activities, or in reasonably foreseeable unplanned events resulting from workplace operations. Safety data developed in SSHA, SHAs, and O&SHAs and summarized in safety assessment reports must also identify any hazards which must be considered when the system, or components thereof, are eventually demilitarized and subject to disposal. This should include EOD requirements to render safe and dispose of explosive ordnance.

p. Prepare a summary report of the results of the system safety tasks conducted during the EMD phase to support the decision-making process.

q. Tailor system safety program requirements for the production and deployment phase.

10.4 Production and Deployment Activities.

The final life cycle phase at the contractor's facility begins with the production of the system and includes 'roll out' and the deployment of the system to the operating forces. The system safety activity during this phase includes the identification of critical parts and assemblies, production techniques, assembly procedures, facilities, testing, and inspection requirements which may affect safety; the assurance that adequate safety provisions are included in the planning and layout of the production line; and that adequate safety provisions are included in the inspections, tests, procedures, and checklists for quality control of the equipment being manufactured so that safety achieved in design is maintained during production. Quality control needs some hints from system safety as where to look! (33:26)

System safety tasks for this phase are: (30:B-6 to B-7)

a. Prepare or update the SSPP to reflect the system safety program requirements for the production and deployment phase.

b. Identify critical parts and assemblies, production techniques, assembly procedures, facilities, testing, and inspection requirements which may affect safety and will make sure:

(1) Adequate safety provisions are included in the planning and layout of the production line to establish safety control of the system within the production process and operations.

(2) Adequate safety provisions are included in inspections, tests, procedures, and checklists for quality control of the equipment being manufactured so that safety achieved in design is maintained during production.
(3) Production technical manuals or manufacturing procedures contain required warnings, cautions, and special procedures.

d. Verify that testing and evaluation is performed on early production hardware to detect and correct safety deficiencies at the earliest opportunity.

e. Perform O&SHAs of each test, and review all test plans and procedures. Evaluate the interfaces between the test system configuration and personnel, support equipment, special test equipment, test facilities, and the test environment during assembly, checkout, operation, foreseeable emergencies, disassembly, and/or teardown of the test configuration. Make sure hazards identified by analyses and tests are eliminated or their associated risk reduced to an acceptable level.

e. Review technical data for warnings, cautions, and special procedures identified as requirements in the O&SHA for safe operation, maintenance, servicing, storage, packaging, handling, transportation, and disposal.

f. Perform O&SHAs of deployment operations, and review all deployment plans and procedures. Evaluate the interfaces between the system being deployed with personnel, support equipment, packaging, facilities, and the deployment environment, during transportation, storage, handling, assembly, installation, checkout, and demonstration/ test operations. Make sure hazards identified by analyses are eliminated or their associated risk is reduced.

g. Review procedures and monitor results of periodic field inspections or tests (including recall-for-tests) to make sure acceptable levels of safety are kept. Identify major or critical characteristics of safety-significant items that deteriorate with age, environmental conditions, or other factors.

h. Perform or update hazard analyses to identify any new hazards that may result from design changes. Make sure the safety implications of the changes are considered in all configuration control actions.

i. Evaluate results of failure analyses and mishap investigations. Recommend corrective action.

j. Monitor the system throughout the life cycle to determine the adequacy of the design, and operating, maintenance, and emergency procedures.

k. Conduct a safety review of proposed new operating and maintenance procedures, or changes, to make sure the procedures, warnings, and cautions are adequate and inherent safety is not degraded. These reviews shall be documented as updates to the O&SHAs.

l. Document hazardous conditions and system deficiencies for development of follow-on requirements for modified or new systems.

l. Update safety documentation, such as design handbooks, military standards and specifications, to reflect safety “lessons learned.”

m. Evaluate the adequacy of safety and warning devices, life support equipment, and personnel protective equipment.

10.5 Operations and Support Activities.

The operations and support phase is the final phase and extends throughout the useful life of the system. It ends with the disposal of the system. During this phase, the system safety organization assigned the safety responsibility for Air Force Material Command provides safety related liaison to other commands having an interest in the system. This is accomplished at the air logistic center’s depot operations. When the depots or users discover system inadequacies that require correction, they take action to improve the reliability, performance, and/or safety of the system. The deficiencies are reported and subsequently corrected by retrofit is necessary. The retrofit actions have to be reviewed and evaluated to ensure that they have not introduced an new hazards to the system.

Using the accumulated safety data from operational experience, the SSG assists the program manager at the depot by continuing to be a safety focal point of advise and expertise. Specific phase activities are:

a. Evaluate results of failure analyses and mishap investigations. Recommend corrective action.

b. Update hazard analyses to reflect changes in risk assessments, and to identify any new hazards, based on actual experience with the system or facility. Make sure the safety implications of the changes are considered in all configuration control actions.

c. Update safety documentation, such as design handbooks, military standards and specifications, to reflect safety “lessons learned.”

d. Review procedures and monitor results of periodic field inspections or tests (including recall-for-tests) to make sure acceptable levels of risk are kept. Identify major or critical characteristics of safety significant items that determine with age, environmental conditions, and other factors.

e. Monitor the system throughout the life cycle to determine the adequacy of the design, and operating, maintenance, and emergency procedures.

f. Document hazardous conditions and system deficiencies for development of follow-on requirements for modified or new systems.

g. Review and update disposal plans and analyses.

h. Conduct a safety review of proposed new operating and maintenance procedures, or changes, to make sure the procedures, warnings, and cautions are adequate and inherent safety is not degraded. These reviews shall be documented as updates to the O&SHAs.

i. Ensure that the system is operated in accordance with prescribed procedures—observance of warnings and cautions—to preserve system integrity.

j. Ensure that user and AFMC effectively us the channels of communication for reporting material deficiencies, safety problems, or mishaps.

k. Ensure that safety reviews are conducted periodically or in response to the user's current safety problems to identify the scope and frequency of the problem and possible solutions.

10.6 Major Modifications.

During the operations and support phase, many systems will undergo major modification. The system changes may be needed to improve safety or could be for a host of nonsafety mission or performance related reasons. When missions change or nonsafety modifications are proposed, the system safety activities must accomplish a review of the new hazards and changes in the risk levels of previously identified hazards. For safety modifications, which are usually the result of mishaps or other experiential evidence, not only must the modification proposal be examined but also the hazards and risk assumptions that led to the system failure. System safety activities must see if these same assumptions affect other system components that have not yet but may soon fail.

Specific system safety related activities associated with major modifications are:

a. Review design proposals

b. Perform risk analyses

c. Coordinate modification category determinations

d. Participate in various meetings, such as SSGs, material safety test groups, and configuration control board meetings.

e. Coordinate safety status and modification prioritization.

f. Prepare formal risk assessments for safety modifications (see paragraph 18.3)

10.7 Demilitarization and Disposal.

When systems are no longer needed and phase-out is contemplated, system safety activities shift to concerns of demilitarization, de-arming, and disposal risks. Analysis of hazardous materials and environmental issues begins with a close look at hazards already identified in system safety analyses during the development and production of the system. Initial termination concepts must then be updated with current applicable laws and policy. SSG meetings provide a focal point for bringing together diverse expertise to address these issues.

If the system is to be demilitarized or salvaged, safety and the avoidance of environmental pollution are important considerations. Systems containing explosives, chemicals, or radioactive materials compose special environmental as well as safety problems . Mechanical systems, such as springs and pressurized containers, also present safety hazards for

disposal. Combat vehicles released for nonmilitary use must be carefully reviewed to ensure explosives have been removed. Disposal actions involving destruction require a plan that implements protection schemes for personnel and the environment. Specific end of life system safety activities are:

a. Establish the limits of damage or injury capability of a system or subsystem.

b. Identify the special procedures and equipment needed for handling and disposal. Prepare instructions for implementing the plan.

c. Determine whether or not the material or its construction can be safely reused.

d. Identify the characteristics and amounts of hazardous materials present in the system.

e. Determine the current service requirements for destruction.

f. Determine whether societal impacts will occur during disposal, such as transportation through civilian areas.

g. Determine the availability of disposal sites for hazardous materials.

h. Ensure that current local, state, and federal laws are applied to disposal and demilitarization efforts.

10.8 Facilities Construction Activities. (30:B-8)

As part of the continuing system safety program for facilities, the system safety tasks for this phase will include the following:

a. Ensure the application of all relevant building safety codes, including OSHA, National Fire Protection Association, and US Army Corps of Engineers safety requirements.

b. Conduct hazard analyses to determine safety requirements at all interfaces between the facility and those systems planned for installation.

c. Review equipment installation, operation, and maintenance plans to make sure all design and procedural safety requirements have been met.

d. Continue the udpating of the hazard correction tracking begun during the design phases.

e. Evaluate mishaps or other losses to determine if they were the result of safety deficiencies or oversight.

f. Update hazard analyses to identify any new hazards that may result from change orders.

CHAPTER 11

PROGRAM OFFICE SYSTEM SAFETY

11.1 Program Office Description.

A key concept of system management is the designation of a single manager to be responsible for all of the technical and business aspects of a program. That manager must then assemble a team to assist in accomplishing the program objectives. The management team, or integrated product team (IPT), is formed by drawing personnel from all of the appropriate functional areas and placing them under the control of the program manager. The program manager is given the authority required to carry out his responsibilities and is held accountable for the accomplishment of the total management task. A yearly budget must be prepared, defended, and managed; schedules must be developed and adhered to (or deviations must be justified); mission hardware must be design, developed, tested, and produced; a capable logistic support system must be assured; contractors must be selected, and contracts negotiated and administered. The team operates through a program office. (34:1-5)

Contracting. (34:6-3 to 6-4) Contracting is the service function designated to actually effect the acquisition process. That is, it provides the legal interface between the buying agency, for example the Air Force, and the selling organization, usually a civilian contractor. All the terms of the agreement between the buyer and seller must be reduced to writing and structured according to law and regulation so as to protect the rights of both parties. The resulting document is a contract, which binds both parties.

Contracting officers, acting within the scope of their properly delegated authority, are the only people authorized to commit the government to a contractual obligation. To evidence this authority, and to specify any bounds on it, a document called a warrant is issued to contracting officers, establishing their legal capacity to act for the government. In large organizations, contracting officers may be asked to specialize in certain areas of contracting. One who is appointed primarily to create and enter into new contracts is referred to as a PCO (for Principal Contracting Officer). One whose main task is to administer previously awarded contracts, making certain that the contract provisions are carried out in performance, is called an ACO (for Administrative Contracting Officer).

Some of the contracting functions are:

Review Contract Proposals	Inspection/acceptance
Quality assurance	Cost assistance
Subcontract management	Facilities
Field pricing support	Cost/schedule control
GFP/GFE	Make or buy decisions
Payment	Administrative mods
Approved purchasing system	Allowability of costs
Deliveries	Post-award orientation
Insurance	Waivers
Small business plan	Manufacturing
Contract closet	Program management

Engineering. Engineering involves not only initial system design but also areas such as maintainability, reliability, survivability, and quality assurance. Satisfying system performance requirements and meeting validation criteria are the main focus. System safety is closely associated with this area of the program office as this is where the problems of design safety are solved. In many cases, it may be advantageous to locate System safety within the engineering organization. This will allow better communications with engineers, but might reduce communications with top management or the program manager. Some of the functions include: (37:12-3)

- Provide safety criteria and requirements to designers.
- Review and provide input into system and component specifications.
- Review interface specifications and control drawings.
- Review design and functional concepts and participate in trade studies.
- Support design reviews and technical interchange meetings.
- Review schematic diagrams and engineering drawings to verify incorporation of safety controls.
- Perform safety hazard analyses.
- Utilize human engineering design criteria in designing hazard controls.
- Utilize human reliability data.
- Support human engineering analyses.
- Identify and control human error hazard causes.
- Review maintainability plans and analyses for safety impacts.
- Utilize failure mode analyses and reliability models to assist in the identification of failure points.
- Identify safety-critical components for reliability analysis.
- Review reliability plans and analyses.
- Review corrective action requirements with safety impact.
- Review customer deficiency reports with safety impact.
- Identify potential hazards and control requirements.
- Serve on certification boards.
- Inspection of safety-critical components.
- Manage the operational safety, suitability, and effectiveness (OSS&E) program.

Integrated Logistics Support (ILS). (34:10-3 to 10-9) The program manager, who is responsible for ILS planning and management, will usually assign ILS responsibility to the Deputy Program Manager for Logistics and, in some cases, to the Integrated Logistics Support Manager.

In order to understand ILS, it is necessary to familiarize yourself with the definition of acquisition logistics. It is the process of systematically identifying and assessing logistics alternatives, analyzing and resolve ILS deficiencies, and managing ILS throughout the acquisition process. Acquisition logistics, then, is a generic term identifying and describing the overall logistics function within which ILS is the predominant

activity. ILS program is a disciplined, unified, and iterative approach to the management and technical activities necessary to:

a. Integrate support considerations into system equipment design.
b. Develop support requirements that are related consistently to readiness objectives, to design, and to each other.
c. Acquire the required support.
d. Provide the support during the operational phase at minimum cost.

ILS elements subdivide the ILS program into the manageable functional areas below.

a. Maintenance Planning. This is the process conducted to evolve and establish maintenance concepts and requirements for the life of the system.
b. Manpower and Personnel. This element involves the identification and acquisition of military and civilian personnel with the skills and grades required to operate, maintain, and support systems over the systems lifetime.
c. Supply Support. This element consists of all management actions, procedures, and techniques to determine requirements to acquire, catalog, receive, store, transfer, issues, and dispose of spares, parts, and supplies.
d. Support Equipment. This element is made up of all equipment (mobile of fixed) required to support the operation and maintenance of a system.
e. Technical Data. This element represents recorded information, regardless of form or character (such as manuals and drawings), or scientific or technical nature. Computer programs and related software are not technical data; documentation of computer programs and related software are. Technical orders and engineering drawings are the most expensive and, probably, the most important data acquisitions.
f. Training and Training Support. This element consists of the processes, procedures, techniques, training devices, and equipment used to train civilian and military personnel to operate and support a system.
g. Computer Resources Support. This element encompasses the facilities, hardware, software, documentation, manpower, and personnel needed to operate and support mission-critical computer hardware/software systems.
h. Facilities. This element consists of the permanent and semi-permanent real property assets required to support a system, including studies to define types of facilities or facility improvements, location, space needs, environmental requirements, and equipment.
i. Packaging, Handling, Storage, and Transportation. This element is the combination of resources, processes, procedures, design considerations, and methods to ensure that all system, equipment, and support items are preserved, packaged, handled, and transported properly.
j. Design Interface. This is the relationship of logistics-related design parameters to readiness and support resource requirements. The logistics-related design parameters include system safety, human factors, engineering, hazardous materials, etc.

Program Control/Financial Management. (34:5-4 to 5-5) Organization which serves the program manager, attempts to facilitate the goal of producing systems within schedule and acceptable cost constraints while meeting performance and logistic supportability requirements. Program control personnel frequently develop key contacts in and out of the government to carry out their responsibilities. They essentially become filter devices to the program manager so that issues and challenges are elevated and answered quickly and thoroughly.

Functionally, program control is typically divided into three unique divisions depending on the type of work involved. The program evaluation division deals with the contractor while monitoring the costs of the program; the financial management division focuses on identifying and monitoring funds to keep the program moving; and the plans and integration division deals with nonfinancial aspects of the system program office like planning, scheduling, and forecasting. Some program offices may not be organized this way, but the type of work done in each division is typical of any program control directorate.

Program evaluation is really program analysis of costs in support of the financial manager. By interfacing with the financial managers, program evaluation identifies the cost requirements and the cost performance of the contractor. Some activities one normally finds in program evaluation are cost/schedule control systems criteria and cost analysis.

Financial management, on the other hand, deals with the management of program funds and the process of budget requests. Some feel this is the heart of any program since if you did not have funds to run your program, you would not have a program. Typical financial management functions are budgeting, financial analysis, fund administration, fiscal integrity and accountability, appropriation integrity, and support of the program manager.

Configuration Management. (34:11-4 to 11-6) Configuration management is comprised of a set of engineering management practices and procedures that are applied in four basic areas of emphasis:

a. Configuration Identification: the documentation of the functional and physical characteristics of the system and its component hardware and software.
b. Configuration Audits: the review of the results of the contractor's development effort to assure that design requirements have been fulfilled and accurately documented.
c. Configuration Control: the communication/decision-making process used to completely document and control changes to the contractually binding configuration identification.
d. Configuration Status Accounting: the information system used to provide traceability of the documentation and delivered units and of the changes to both.

The basic unit of configuration management is the configuration item. Essentially, all of the configuration management functions are performed at the configuration item level. Specifications are written to document the characteristics of each configuration item, the design reviews and audits are performed for each configuration item, engineering change proposals are written separately for each configuration item affected by the change, and status accounting tracks the implementation of changes to each configuration item. The exception is that a system specification will be written for each major system to define the required performance.

Data Management. (34:12-5 to 12-6) The program manager is responsible for acquiring the contract data necessary to manage all aspects of the program/project. A data

management officer (DMO) is usually appointed to assist the program manager in this task. The process of identifying and acquiring the required data begins in the concept exploration phase and continues throughout the entire system life cycle. For each contract to be issued (usually for each phase of the program), the formal process begins when the DMO issues a data call. This data call is usually a letter which describes the planned program and asks functional managers to identify and justify their data requirements for that contract.

After contract award, the DMO is responsible to track, for timely deliver, all of the CDRL data on the contract. If the contractor is late on delivery or if the data delivered is deficient (including having restrictive markings not authorized by the contract), the DMO, through the contracting officer, can use the FAR clause entitled, Technical Data—Withholding of Payment, to withhold from the contractor up to 10 percent of the contract price in order to press for the late/deficient data.

Test and Evaluation. (1:14-4) Within a program office, a typical test and evaluation directorate is not a simple thing to define. Depending on the number of programs involved, and their size and complexity, the organization can vary from a deputy director for large programs, chief of a division for other small programs, to possibly only one or two individuals for small or one-of-a-kind programs. In any case, while the complexity, schedules, and resource planning may change, the mission of the organization does not. Regardless of type organization, the "testers" must plan, coordinate, and manage the program test activities within policies set by the program manager. The larger programs usually require more schedule and test disciplines due to more test articles and, possibly, more complex operations. However, testing small programs should receive the same emphasis within the program office as the large programs.

Test and evaluation commences as early as possible in the acquisition process and continues throughout the entire system life cycle. Moreover, sufficient test and evaluation must be accomplished successfully before decisions will be made to commit significant additional resources to a program or to advance it from one acquisition phase to another. While conducting test and evaluation, quantitative data must be used to the maximum extent possible, thereby minimizing subjective judgments. Well, what are the main purposes of test and evaluation? Essentially, they encompass (1) the assessment and reduction of risks, (2) the evaluation of the system's operational effectiveness and suitability, and (3) the identification of system deficiencies.

Manufacturing. (34:13-4) Management of the manufacturing process is a subset of the larger function of program management and represents the techniques of economically planning, organizing, directing, and controlling the resources needed for production. A primary goal of manufacturing management is to assist program managers in assuring that defense contractors deliver goods and services, of specified quality, on time, and within agreed cost constraints. To accomplish this goal, manufacturing managers must become involved EARLY in the acquisition life cycle of a program.

The feasibility analysis involves the evaluation of:

a. Producibility of the potential design concepts.
b. Critical manufacturing processes and special tooling development which will be required.
c. Test and demonstration required for new materials.
d. Alternate design approaches within the individual concepts.
e. Anticipated manufacturing risks, costs, and schedule impacts.

Manufacturing activities include production feasibility, production risks, manufacturing technology needs, manufacturing strategy, producibility planning, production surveillance, and implementing product improvements.

11.2 System Safety Manager's Role. (37:1-3 to 1-5)

Similarly, the system safety managers do not directly control any program activities. They function only with the program managers' or the commander's authority. They are effective only to the degree that the program managers are willing to accept guidance and advice, and only to the degree that the commander supports them. Fundamental to the mishap risk management concept is the requirement that competent and responsible safety management be assigned with centralized authority and totally capable of maintaining a continuous safety overview of the technical and management planning aspects of the entire program. The responsibility for preventing a mishap belongs to the program manager. It cannot be delegated. When the program manager makes the decision to initiate testing or commence operations, all risk inherent in the system has been accepted.

It is the task of the system safety manager to be sure that, when the decision is made, the decision maker is fully aware of the mishap risks that are accepted by that decision. If the program manager is allowed to make a decision without full knowledge of the inherent risks in the system, that manager, along with the taxpayers and the country, is being cheated. They are being cheated in that a critical decision, which could result in millions of dollars lost, is required to be made with incomplete information. There is no reason for this to happen. The tools and talent are available to provide this information. Properly used, this information can significantly reduce the risk of losing valuable equipment, personnel, and time. Program managers are not always aware of this or willing to use the resources which are available through the system safety process.

The program manager should begin establishing his system safety activity in a position of authority. The program is made effective by assuring an awareness of risk and the importance of reducing risk within all program elements down to the lowest organizational level. Each program element manager must periodically be held directly accountable to implement safety policies and decisions at the lowest organizational level possessing such authority. Most important, the program manager must assign a capable and knowledgeable watchdog to act as eyes and ears throughout the organization to ensure that the tasks are accomplished. The system safety manager is that watchdog, and to be effective, he must be assigned the authority to act directly as the safety agent of the program manager. In this capacity, the system safety manager assures that proper engineering and management expertise is brought to bear on a specific problem to identify and effect a solution. The task is to tie together, to monitor, and to influence activities for developing safe systems. To be effective, continuous efforts from the large perspective of the total program, with an understanding of the various interrelationships among its organizational elements, are required. The system safety manager is a major motivating force for guiding system development safety through the evolutionary process and, as the program manager's agent, the system safety manager focuses the program manager's authority and responsibility on the program's safety aspects. The program manager, in turn, should require frequent progress reports to keep his fingers on the pulse of the system safety activity.

The mishap risk management concept evolved because the accepted approach of eliminating hazardous conditions through good engineering practice alone was not necessarily adequate to assure safe operation of complex military systems. Military development programs are traditionally success oriented. Program managers are not necessarily receptive to a function which tries to find out ways it can fail. Throughout the entire life cycle, program-oriented safety management is necessary if all of the safety-critical aspects of a system are to be controlled cost effectively. In planning and managing the reduction of risk, the system safety manager must be free, within the program structure, to exercise professional judgment and organizational flexibility with the authority of the program manager.

11.3 System Safety Manager's Responsibilities. (37:6-1 to 6-3; 31:7-9)

a. Maintain an overview of the technical and planning aspects of all program efforts through attendance at appropriate meetings and review of program documents. It doesn't take long to lose touch with the world if you isolate yourself from it. The only way to get in touch and stay there is to maintain a constant working interface with as many individuals and groups as possible. The system safety manager should attend as many program office meetings as possible to have a good working knowledge of what is happening. There are some meetings that are specified as mandatory for the system safety manager, such as the configuration control board and system safety group meetings, but, generally, it is up to the system safety manager to determine which meetings are important.
b. Ensure the application of system safety design principles to developing programs through contract tailoring and continual program oversight. This requirement is met by assuring the application of MIL-STD-882 to the contract to provide for a strong management approach and by applying all necessary technical requirements documents in the specifications.
c. Serve as advisor to both Air Force and contractor program management. In this way, you can be sure that the same advice and direction is being passed to all involved parties.
d. Initiate programs to ensure unacceptable accident/mishap risks are identified and acceptably controlled. Each program will, for analysis purposes, define unacceptable damage that will impact the mission or its objectives. Damage includes breakage, mangling, mutilation, or ruin of items which causes obstruction of functions generated across system or component interface by internal or external action, including human error.
e. Review all program documents to ensure they contain appropriate system safety tasks. This includes SOWs, plans, and operating procedures.
f. Ensure that the requirements of interfacing agencies and disciplines are addressed and properly implemented.
g. Ensure that system safety concepts are incorporated into planning documentation.
h. Ensure that the program manager receives regular reports and briefings on the status and progress of the above tasks.
i. Request staff assistance whenever problems or questions arise and the solution is beyond the scope of his knowledge and experience.
j. Provide a single point of contact for the purchasing office, all contractor internal program elements, and other program associate or subcontractors for safety-related matters.
k. Participate in all test, flight, or operational readiness reviews and arrange for presentation of required safety data.
l. Provide for technical support to program engineering activities on a daily basis. Such technical support will include consultation on safety-related problems, research on new product development, and research/interpretation of safety requirements, specifications, and standards.
m. Participate in configuration control activities to review and concur with safety significant system configuration and changes.
n. Review all trade studies and identify those that involve or affect safety. Provide participation in all safety-related trade studies to assure that system safety trade criteria is developed and the final decision is made with proper consideration of accident risk.
o. Provide participation in program-level status meetings where safety should be a topic of discussion. Provide the program manager the status of the system safety program and open action items.
p. Provide for safety certification of safety-critical program documentation and all safety data items contained in the CDRL.
q. Provide internal approval and technical coordination on deviations to the contractually imposed system safety requirements.
r. Conduct or arrange for internal audits of safety program activities. Support purchasing office safety audits and inspections as required.
s. Coordinate system safety, industrial safety, facility safety, product safety, and other safety activities on the program to ensure total coverage.
t. Support the local operational safety, suitability, and effectiveness (OSS&E) program (refs AFPD 63-12 and AFI 63-1201) (Refs need to be placed in bibliography)

11.4 Implementation. (37:6-4 to 6-7)

There are some problems in implementing a system safety program. They fall into four general categories:

a. Insufficient time to provide adequate surveillance of either program office or contractor activities.
b. Insufficient knowledge to do an adequate job.
c. Obtaining sufficient authority or direction to do the job.
d. Not using the system safety manager as intended by the regulations.

Time Management. The average program office system safety manager may be assigned this task full time or as an additional duty. Normally, this assignment includes reliability, quality assurance, and other related functions. This presents somewhat of a dilemma since all of these functions are important and require time-consuming attention. Each of these tasks, at one time or another, during a typical program, require full-time attention. Often, they will peak at the same time.

So, first, lay out the tasks required of the system safety manager. These tasks are specified generically in regulations. From these documents, prepare a list of primary tasks.

Once the details of these tasks are laid out, they can be compared with the program milestones and sequence of events to determine how your time should be allotted. Armed with this information, it is easier to budget your time with that required for other additional duties. If there is less time than you need available, inform your program manager that the task cannot be performed effectively. You may be able to get the help you need by assigning other additional duty people to help.

Knowledge. All assigned system safety managers and engineers are required to receive formal training. General system safety concepts are covered by Air Force Safety Center-sponsored courses in management and analysis areas. Product centers and air logistics centers provide courses that give specific detailed system safety guidance for daily system safety operation. Handbooks, continuation courses, seminars, conferences, and other training opportunities should also be used.

Authority and Direction. The authority and direction for conducting a system safety program is a matter of Air Force policy. It requires an organizational structure and sufficient resources to perform the task. The regulations establishing SSM authority are also there. Make sure your program manager understands that. Whatever the reporting channels, when the SSM performing system safety functions, he works for the PM and is responsible only to the PM.

Each Air Force program office should have an operating instruction which states this. However, since the SSM may be newly assigned, he may find that regulations and OIs need reinforcing. Write a letter for the program manager or deputy's signature. Address it to all program office element managers. In this letter, establish the SSM's authority under the regulations. State that in all system safety matters, the SSM is the spokesman and agent for the program manager. Camp on his door step until you get a signature. Arrange for regular system safety program status briefings. Then implement your program.

Some SSMs may have a boss that won't allow you to do this. That is the time to ask for assistance from the product center or air logistics center headquarters safety staff. Assistance will be provided to make sure he knows what needs to be done.

Program Managers/System Safety Manager Interfaces. This problem normally results from a lack of knowledge of what the regulations intend. Be sure that in your initial contact with the program manager, you brief him on the tasks that you are assigned and the objective of the program. In your periodic status briefings, always make sure that the mishap risks involved with each decision option are clear. Be sure the program manager participates in establishing the acceptability parameters. Do not accept lack of funding or manpower as an excuse for not paying attention to the regulations. If this becomes a problem, again, let the base or center safety staff help. Do not let problems build up until they are unsolvable; you have got the job, go do it!

Assistance. These requirements represent only a part of the system safety task. As an acquisition manager, you cannot be expected to know all there is to know about the application of these and other documents which are required for use. There are several places you can go for expert help. They are listed below in the general order normally used, but there is no set precedence. Most safety acquisition managers soon learn where to go for specific assistance.

a. HQ Product Division or Air Logistics Center Safety Office: Focal point for program-specific safety policy and guidance. System safety personnel from this office ensure, by assistance and surveillance, that the system program manager has implemented an adequate system safety program. In the acquisition area, all program statements of work and other program documents are reviewed by this office for adequacy of system safety content.
b. MAJCOM Safety Office: Sets and reviews policy and guidance that applies to all product division and air logistics centers. Career development, training, regulations, specifications, and major program reviews are some of the AFMC concerns.
c. Air Force Safety Center: Broad system safety policy and education are key concerns addressed by the AF Safety Agency. Multiservice and non-DOD government agency cooperation are also concerns. The effectiveness of AF system safety programs and issues addressing the entire spectrum of system safety education and professional assistance are action areas as well.

11.5 Interfacing.

a. Introduction. (10:8-10)

An interface is the necessary work relationship of two persons. It is suggested that this is synonymous with an interrelationship, but this interrelationship should be understood as a professional and ethical sharing of information while working to achieve a common goal. Integration is understood as a prime contractor or program manager's efforts to bring together and meld the separate work interfaces into a project. That successful or unsuccessful melding results in fusion or confusion and will have a major influence on the success of the project.

Roland and Moriarty highlighted the importance of the interface. They wrote: "Lines of authority for the system safety management organization must be easily identifiable by all interfacing organizations within and outside the project. Since system safety interfaces with almost every aspect of management organization, it must have the ability to influence design, provide concise identification of hazards, and have the full cooperation of company management. The importance of interfaces cannot be stressed enough; they are the breakpoint for the success of the safety effort...."

How does the system safety manager establish an effective interface? To properly interface system safety with the other disciplines, the system safety manager must fully understand: (1) the safety requirements of the system, (2) the tasks necessary to satisfy the requirements, and (3) the data requirements of the system safety program. He/she must also get familiar with the system to understand and be effective with steps 1-3. It is imperative that the terminology of the designers with whom you are working is understood.

b. General. (28:53) The system safety program is intended to encompass or provide awareness of the entire accident prevention effort for a specific system. However, system safety alone cannot assure that every effort has been employed to minimize, eliminate, or control the hazards involved. This task must be done in conjunction with engineering, reliability, quality control, human

factors, etc. The internal relationship within the various disciplines and organizations involved becomes an essential link in achieving necessary direction and feedback. Contractor and program management must understand and appreciate the system safety discipline. Without proper management support and emphasis, the effective application of system safety techniques becomes more difficult, if not impossible. Although MIL-STD-882 and other related specifications are included in the contract, working relationships between system safety and other common disciplines must be identified and established. Specific system safety-oriented tasks, such as stipulation of program requirements, participation in preliminary and critical design reviews, and performance of systems and operations hazard analyses, should interface with other disciplines. One of the most important tasks of the system safety manager is to ensure that system safety objectives, criteria, and goals are established in meaningful terms. This is necessary so that the safety direction contained in the contract results in actions and allocation of resources for system safety during the validation phase. To accomplish this task, and to ensure an acceptable system safety effort throughout the life cycle of the system, close and continuous interfaces with all system engineering support activities, whether within the program office or outside it, are of primary importance.

c. Interfacing Within the Program Office. (28:53-57)

Data Management.

1. The system safety manager should be familiar with DOD Acquisition Management System and Data requirements Control List (AMSDL) which contains all the data item descriptions (DID), some of which are pertinent to system safety. The system safety manager should consult this document to aid him/her in selecting appropriate DIDs such as DI-SAFT-80101, etc.
2. It will be necessary for the system safety manager to tailor the DIDs to satisfy specific program requirements.
3. Early in the program, the system safety manager should attend in-process reviews of technical publications, especially in the operations and maintenance areas. Both systems and subsystems should be reviewed to ensure that safety requirements are incorporated in the manuals, TOs, etc.
4. The system safety manager should actively participate in the validation and verification of technical data pertaining to his/her system.

Configuration Management.

1. Configuration management is the formal management process which is applied to system and equipment programs for the identification, controls, and accounting of the configuration of the system and equipment.
2. Identification is accomplished by means of specifications, drawings, and other engineering documentation. Format and content of system and configuration item specifications is established in accordance with MIL-STD-961. In particular, safety requirements to preclude or limit hazards to personnel and equipment will be specified in Section 3, Requirements, of the applicable performance specification.
3. Changes in the configuration of systems and equipment will usually be accomplished by means of engineering change proposals.. The system safety manager should ensure that all changes have been assessed for safety impact. Each change should be evaluated by determining the outcome when the change is inserted in the same analysis that were performed during original design work. Accurate, timely, and complete evaluation of proposed ECPs should be an essential task of the system safety manager. The system safety manager should also be a member of the configuration control board.

Program Control/Financial Management. The system safety manager will have important contacts with the program control and financial management personnel and will be involved in the areas of plans and documentation and financial management. These are:

1. The personnel responsible for plans and documentation will interface with the system safety manager to:
   (a) Ensure that the safety portion of the program is properly described in the documentation. This description is to include definite statements regarding the responsibilities assigned to each organization involved in system safety during the acquisition process.
   (b) Revise program documentation as necessary whenever changes to the system safety portion of the program are generated.
   (c) Establish meaningful, clearly defined milestones for the accomplishment of the safety aspects of the program.
   (d) Establish schedules for system safety in consonance with overall system guidelines and constraints.
   (e) Assess, on a continuing basis, progress toward timely accomplishment of program schedules.
   (f) Establish impact on total system program when schedules are not accomplished in a timely manner.
2. The personnel responsible for financial management will interface with system safety to:
   (a) Ensure that system safety budget estimates are established and included in all financial information. When full funding for system safety is not provided, works with system safety manager and plans and documentation personnel to revise the system safety aspects of the program in terms of what can be accomplished with the funds available.
   (b) Revise cost estimates and assess impact whenever changes are made in the system safety effort.
   (c) Continuously assess expenditure of funds to determine if rate is in accordance with plan and progress toward meeting established goals. Included will be an assessment of the cost outlook for completion of the program. When outlook is at variance with planned funding

arrangements, an assessment of the impact on the total system must be accomplished.

Contracting. The system safety manager should be familiar with cost information/reporting procedures. This system will provide information in support of program change request estimates and also information for weapon system cost effectiveness studies. The system safety manager should be aware that the cost of tasks reflected in the system safety plan can be called for on an exception basis if the requirement for a system safety plan is included in the work breakdown structure (WBS). It is important that the system safety manager ensure that the requirement for a system safety plan is reflected in the WBS. It is also important that the system safety manager ensure that the WBS index contains the necessary subject titles to delineate the system safety tasks to be performed by the contractor and that the tasks are backed by the WBS dictionary to adequately describe them. The system safety manager should make sure that the WBS description of the system safety tasks agrees with the requirement in the SOW. Work statement preparation is covered in WBS in MIL-HDBK-881. Also, see Chapter 12 of this handbook.

Engineering.

1. Reliability.

   (a) The system safety manager should be familiar with the reliability efforts. This technique is parallel to and complements safety modeling. The system safety manager should also collaborate with reliability efforts in design to avoid duplication and to assure optimum system evaluation.
   (b) The procedures for accomplishing a reliability analysis are: The creation of a system functional model, the execution of a failure mode and effects analysis, and the identification of critical items. Critical items are defined as those items, the failure of which, or the inability to achieve a required function, would significantly affect the capability, reliability, or safety of a system.
   (c) The procedures for accomplishing a subsystem hazard analysis also require the creation of a system functional model and the execution of a fault hazard analysis in which the first portion is similar to a reliability failure mode and effects analysis.

2. Maintainability. The system safety manager should interface as early as possible with maintainability requirements to perform preventive, corrective, servicing, and configuration management. Accessibility to perform certain maintenance functions on particular equipment or components may introduce unwarranted hazardous conditions resulting from proximity of hazardous energy sources and a limited working environment. Therefore, in order to impact design, hazards associated with maintainability must be considered as early as possible and, in any case, must be examined in the O&SHA.

3. Quality Assurance.

   (a) In each program office, there should be a designated quality assurance monitor. The system safety manager should work closely with quality assurance personnel as they are knowledgeable of details of acceptance and qualification procedures, as well as other program aspects which could directly affect safety.
   (b) The system safety manager should be familiar with AFI 63-501.

4. Human Factors.

   (a) Human factors is a management concept and procedure which provides an organized approach to and close integration of various disciplines which consider man-in-weapon system development.
   (b) Several of the disciplines involved in the personnel subsystem are concerned with safety. Human factors engineers provide design criteria for hardware which consider man's safety. Biomedical support personnel have specific responsibility for man's psychological and physiological safety.
   (c) A human factors team is normally formed shortly after the establishment of weapon system requirements. Their purpose is to evaluate and enhance the man/system interface. This team is composed of human factors engineers, training equipment engineers, training specialists, and biomedical personnel, as well as using command specialists.
   (d) It is highly desirable that the system safety manager work with the human factors team to coordinate their effort with other disciplines. This relationship should continue throughout the life cycle of the system.

5. Armament Integration. For program offices requiring armament integration, there will be an engineer assigned to monitor the compatibility for both nuclear and nonnuclear stores. Total armament integration includes the evaluation of aircraft stores (rockets, missiles, bombs), their suspension system release mechanisms, separation characteristics, loading/handling procedures, and associated checkout equipment. The system safety manager should work closely with the armament integration engineer and be familiar with the direction outlined in Chapters 16 and 17 (Nuclear and Explosive Safety).

6. Survivability/Vulnerability.

   (a) In each of the major system program offices, there will be an engineer responsible for implementing AFI 62-201. The integration of proven design criteria and techniques will reduce aircraft vulnerability, thereby enhancing aircraft survivability.

   Survivability must be incorporated in the basic design of an aerospace weapon system. Survivability is a function of the hardness of the system's basic designs, the conditions and methods of its employment, and the threat environment. It warrants positive attention at each echelon of management throughout the system life cycle. Special emphasis is warranted during initial design. Survivability requirements must be carefully considered with respect to their impact on cost, performance, safety, reliability, maintainability, and other

system requirements to assure maximum operational effectiveness. It is not intended that every system that is developed or acquired for Air Force use should meet the same set of survivability criteria. Instead, specific criteria must be established on a system-by-system basis for each system that is expected to function in a hostile environment. A comparison of peacetime accident and combat losses indicates a strong tie between design deficiencies, unsafe aircraft, and vulnerable aircraft.

7. Operational safety, suitability, and effectiveness (OSS&E). The program manager has the overall responsibility for assuring to the user that the system or product will be safe to use, and will be suitable for its intended mission, and will be effective in doing so. AFI 63-1201 outlines the necessary efforts to achieve OSS&E assurance. The program chief engineer has the bulk of the efforts to support OSS&E by incorporating a robust systems engineering program, including configuration management. Safety will generally be measured by hazard analyses, risk indices and mishap rates. Suitability will be measured by such factors as availability, reliability, maintainability, human factors, etc. Effectiveness will generally be measured by performance: range, payload, vulnerability, etc. It is important to understand that the role of the system safety engineer/manager will not change appreciably. If anything, OSS&E will boost the system safety effort, as it will be required to support OSS&E assurance to the user.

Test. The system safety manager should work closely with the program test manager and contractor system safety manager in reviewing test plans and the responsible testing organization's operating practices and procedures. This safety review should identify those tests that are potentially hazardous and examine the procedures or techniques being used by the responsible testing organization to minimize those hazards. Test data requirements should be challenged if test risks are too high for the data point being sought. However, in all cases, high-risk testing must be clearly identified and brought to the attention of the program manager.

The program office has a responsibility to ensure safe operation of government aircraft and equipment used by contractors. Therefore, the system safety manager should become familiar with the requirements of AFI's 99-101 and -102. In addition, the system safety manager should review the requirements of AFJI 10-220.

11.6 System Safety Groups. (28:47-51)

System safety groups (SSG) are advisory groups organized to advise the program manager in implementing the system safety program. SSG meetings should be held during each phase of the acquisition cycle. The earlier phases are the most important to the system safety manager. The frequency and content of the meetings will depend on the number and severity of safety concerns. Usually, the earlier phases require more meetings.

The SSGs provide many useful and productive functions. They bring together people and organizations which have talent, expertise, and experience not available within the program manager's organization. Using command participation in the safety group activities is particularly meaningful. Personnel from these commands can readily find subtle deficiencies and hazards in new equipment designs by recalling the many lessons learned through operating and maintaining similar equipment. The safety group is a tool to be used by the program manager. Although many organizations attend SSG meetings, care should be taken to limit the number of attendees from each organization so that a reasonable discussion can be conducted. The SSG should be formed with the following representatives:

a. Program manager (chairperson)
b. System safety manager
c. SPO personnel (as required by the meeting)
d. Contractor personnel (as required by the meeting)
e. Using command representatives
f. Production division/air logistics center safety representatives
g. AFMC safety representatives
h. AF Safety Center representative
i. Test personnel (as required by the meeting)
j. Other services (as required by the meeting)

Concept Exploration Phase. Since the system specification is normally completed by the end of the conceptual phase, an SSG meeting should be hosted towards the middle of the concept exploration phase. The object is to incorporate system safety engineering requirements, criteria, analyses, and constraints into contractual documentation. If safety requirements are not specified in the ORD, this is the time to incorporate the safety requirements. An ideal source of information for these requirements is AFSC Design Handbook 1-6. Another source of information is lessons learned. Not all SSG desires can be incorporated into contractual documentation for the validation phase. Validation phase contracts are purposely written with minimum government guidance to encourage contractor ingenuity. Nevertheless, an aggressive SSG will be able to include sufficient safety guidance in contractual documentation to provide initial directions to the contractor. Specifically conceptual phase SSG activities should include but are not limited to:

a. Prepare an SSG charter.
b. Establish procedures at the first meeting, if possible.
c. Validate safety criteria in the ORD document. If safety criteria are lacking, the SSG should suggest safety criteria for the system specification and other documentation intended for use during the validation phase.
d. Identify additional safety criteria.
e. Determine scope of contractor system safety effort and draft an input for the validation phase statement of work.
f. Determine safety criteria for inclusion in the system specification.
g. Draft an input for the single acquisition management plan (SAMP).

Production definition and Risk Reduction (PDRR) Phase. The PDRR phase SSG should have a high degree of success in influencing the design. Instead of only monitoring the status of the design and existing hazards, the group should obtain necessary substantiating data from similar systems and, finally, make recommendations to influence the design. Specific validation phase SSG activities should include:

a. Participate in design and other types of reviews.
b. Identify safety deficiencies in the prototypes and provide recommendations to the program manager.
c. Compile a list of safety criteria for use in the EMD phase.
d. Determine scope of contractor system safety effort and draft inputs for the EMD statement of work and specifications.
e. Draft an input for follow-on management plans.

f. Assist the contractors in making tradeoff decisions by providing mishap occurrence rates, repair costs, maintenance data, etc.
g. Participate in test planning and preparation of test documentation.
h. Evaluate effectiveness of contractor's system safety programs and make recommendations to the program manager.
i. Assist in preparing source selection criteria and participate in the source selection for EMD phase.

Engineering and Manufacturing Development Phase. Great system safety strides should be made in the EMD phase. The greatest SSG effort should be towards improving systems design so as to prevent retrofits in the production phase. The EMD phase contractors are usually required to perform preliminary, subsystem/system, fault, and operating hazard analyses. They are also tasked to actively take part in SSG activities and to identify and eliminate or control identified hazards. The SSG should meet just before the preliminary and critical design reviews to establish safety positions on system designs which are unsatisfactory to the SSG. The SSG should also meet before production decisions. Specific EMD phase SSG activities should include:

a. Review and evaluate the contractor's system safety program plan.
b. Identify the safety-critical systems, operations, facilities, and events to be included in design review proceedings.
c. Evaluate the contractor's periodic system safety reports.
d. Evaluate all the hazard analyses for adequacy. Ensure that the proposed corrective action for each identified hazard is appropriate; that is, ensure warnings proposed for technical manuals are actually included.
e. Participate in program and design reviews to observe hardware firsthand and detect overlooked or ignored hazards.
f. Conduct independent hazard analyses.
g. Recommend appropriate additional analyses after the design is firm.
h. Obtain and review data from AFSC mishap files. Use the AFSC representative to provide accident/incident data on "similar" systems, if possible.
i. Review SPO instructions and procedures for requesting investigations, changes, reports, clarifying requirements, reevaluations, etc., from the contractors.
j. Assist the contractor in making tradeoff decisions by providing mishap occurrence rate, repair costs, maintenance data, etc.
k. Document SSG safety concerns and recommendations and forward them to the program manager.
l. Participate in formulation of EMD phase test plans and preparation of test documentation.
m. Evaluate selected engineering change proposals.
n. Draft an input to the production phase program management plan.
o. Determine scope of contractor system safety effort and draft inputs for the production phase statement of work.
p. Review lessons learned activities.

Production/Deployment Phase. During the production/deployment phase, the SSG's primary tasks are to review safety deficiencies identified by the using command during operational use of the system and advising the program manager on evaluating these deficiencies and taking corrective action. Specific production phase SSG activities should include the following:

a. Ensure that safety-critical production techniques and procedures have been identified and that quality control within the contractor's organization has established corresponding production controls; that is, test and inspection requirements.
b. Evaluate selected ECPs for safety impact and provide recommendations to the program manager. Usually, this task is accomplished by the system program office system safety manager.
c. Ensure that safety analyses and other documentation are included in the transfer package from the product center to the Air Logistics center.
d. Review lessons learned activities.

Other Suggestions. The program manager shall chair the SSG meetings. The manager's presence adds emphasis to the safety program. It also allows him/her to understand safety concerns firsthand. The system safety manager will handle the administrative details and act as official recorder.

Program Office Business. The system safety manager should provide the members with some basic information and reference material and advise members on the required operational need for the system and the current conception of its operational use.

The members and their organizations should try to ensure continuity of attendance. They should expect to take part in activities of the group. Stable membership will improve the products of the SSG.

Individual members should accept the responsibility to prepare themselves before each meeting. The following publications are recommended for reading as basic preparation for the initial SSG meeting: AFI 91-202 and supplements, AFMCP 91-2,MIL-STD-882D, AFSC Design Handbooks 1-3, 1-6, and 1-X, and the SSG charter. Members should try to familiarize themselves with historical information concerning similar systems fielded in the past. Using command members should examine the problems their command has experienced in operations, maintenance, and support areas. They should research traditional high-cause factors for accidents, types of accidents, high-hazard operations, system tests, and features historically noted. Members are entitled to technical briefings and handouts describing the system technical aspects. The ultimate purpose of the SSG is to improve the effectiveness of the system by providing protection from mishap loss.

Members should be authorized to represent their command, organization, or agency and state its official position. Members must be authorized to accept action items assigned by the SSG. This responsibility should be stated in the SSG charter and members should be prepared to support it. If conflicts arise beyond the member's authority to resolve, then the member is responsible for requesting a staffed response from his agency to resolve the conflict.

System Safety Working Groups (SSWG). SSWGs are informal organizations consisting mainly of program office personnel but may include additional expertise to discuss, develop, and present solutions for unresolved safety problems to the program manager. Additionally, they investigate engineering problem areas assigned by the SSG and propose recommended solutions.

No formal minutes or charter are required. It is intended for this group to meet as needed and provide continuity throughout the SPO concerning safety.

The system safety manager will maintain a logbook of meetings outlining areas discussed, personnel present, date, time, and place of meetings.

The SSWG should be used by a SSG or program manager to solve specific safety problems.

SPOs managing many small programs can use the SSWG for individual programs and specific safety problems. A formal SSG could then establish general safety guidelines and policies for all programs in the SPO.

11.7 Key System Safety Personnel Qualifications.

The program manager can require that key system safety personnel meet minimum qualifications. Key system safety personnel are usually limited to the person who has supervisory responsibility/technical approval authority for the system safety work. A guide is provided in Figure 11-1 for these qualifications. The PM must specify the minimum qualifications of key personnel in the SOW. Some programs will require that the key system safety personnel possess special qualifications in addition to the ones shown below. The special qualifications must also be specified in the SOW.

Figure 11-1

MINIMUM QUALIFICATIONS FOR KEY SYSTEM SAFETY PERSONNEL

PROGRAM COMPLEXITY	EDUCATION	EXPERIENCE	CERTIFICATIONS
HIGH	BS IN ENGINEERING, PHYSICAL SCIENCE OR OTHER*	FOUR YEARS IN SYSTEM SAFETY OR RELATED DISCIPLINE	REQUIRED CSP IN SYSTEM SAFETY, PE IN SAFETY OR OTHER*
MODERATE	BACHELOR'S DEGREE PLUS TRAINING IN SYSTEM SAFETY	TWO YEARS IN SYSTEM SAFETY OR RELATED DISCIPLINE	DESIRED CSP IN SYSTEM SAFETY, PE IN SAFETY OR OTHER*
LOW	HIGH SCHOOL DIPLOMA PLUS TRAINING IN SYSTEM SAFETY	FOUR YEARS IN SYSTEM SAFETY	NONE

CHAPTER 12

CONTRACTING FOR SYSTEM SAFETY

12.1 Contracting Principles. (34:6-5 to 6-7)

Contracting is the service function designated to actually effect the acquisition process. That is, it provides the legal interface between the buying agency, for example the Air Force, and the selling organization, usually a civilian contractor. All the terms of the agreement between the buyer and seller must be reduced to writing and structured according to law and regulation so as to protect the rights of both parties. The resulting document is a contract which binds both parties to its provisions.

Government contracts must conform to the principles of law which have governed the formation of contractual relationships for centuries. The basic elements required to be present in order to have a valid contract can be presented very simply, although legal cases on any part of an element can be very complex. Basically, there must be at least two parties to the contract, each of whom has the legal capacity to act for its organization. An offer must be formulated and communicated, and an acceptance must be made and manifested. When an offer or counteroffer is accepted, an agreement is created. An agreement, although basic to a contract, is not in and of itself a contract, as other ingredients must also be present. Consideration must be present, meaning that each party gives to the other something of value to guarantee its promise to perform. The terms of the agreement must be clear and certain, and the objective of the contract must be some legal act. Finally, the contract must be in the form required by law.

Contracting officers, acting within the scope of their properly delegated authority, are the only people authorized to commit the government to a contractual obligation. To evidence this authority, and to specify any bounds on it, a document called a warrant is issued to contracting officers, establishing their legal capacity to act for the government.

Historically, there have been two methods of contracting available to the contracting officer. These methods, which had evolved over 200 years of government contracting, were called (until recently) Formal Advertising and Negotiation. In 1984, Congress passed Public Law 98-369 called "The Competition in Contracting Act." This piece of legislation made sweeping changes in many areas of contracting, emphasizing competition as a key ingredient of the process. In the area of methods of contracting, Formal Advertising was renamed the Sealed Bidding process and Negotiation was renamed the Competitive Proposals process, and both were acknowledged as equally legal and effective methods, given the circumstances of the acquisition. The Sealed Bid method has relatively little application in the systems contracting arena; it is used primarily in base-level contracting and in some centralized spare parts acquisitions. In systems contracting, the Competitive Proposals method (still referred to as Negotiation) is used almost exclusively.

12.2 Contracting Process. (34:6-7 to 6-9)

There is a definite contracting process, or series of activities, which must be accomplished in order to effect an acquisition. These activities include acquisition planning, communicating the requirement to industry, evaluation of the resulting proposals or bids, negotiation or other selection of the source to perform the contract, and management of the awarded contract to assure delivery of the supplies or services required. The following paragraphs will look at these activities within the contracting process.

Acquisition Planning. Much work has already been accomplished before the contracting function officially becomes involved in the acquisition. Technical personnel have selected and tailored an existing specification for the items required or may have had to create a new one if none existed. Decisions concerning the quantity of items, the required level of quality, the type of logistics concerns, the delivery schedule, the performance parameters the items must meet, the testing and evaluation process, the data required to document the performance of the items, and the estimated cost of all the above have already been coordinated and approved. All of the paperwork documenting these decisions, along with evidence of the availability of funds for the acquisition, are forwarded to the contracting office as part of a purchase request.

The contracting officer must accomplish a great deal of planning for the acquisition before potential sources are even notified of the requirement. An acquisition plan is written (or if one already exists, it is updated), addressing such topics as the intended method of procurement; the amount of competition expected or rationale for no competition; the intended contract type; the timeline of milestones which will result in contract award; the applicability of various logistics, quality assurance, and financial management systems; the method of source selection to be used; the criteria to be used to select the winning contractor; and any special contract clauses which might apply.

Development and Distribution of a Solicitation. When the required decisions have been made and documented, the contracting officer turns his/her attention toward preparing the document which will communicate the requirement to industry. This documented, called an Invitation for Bids if the Sealed Bidding method is used or a Request for Proposals (RFP) if Competitive Proposals (Negotiation) is used, transmits the specification or other description of the requirement, data requirements, proposed final contract format, criteria for award, and any directions necessary for filling out the forms correctly in order to submit an offer. It also establishes a common cutoff date by which offers must be returned.

If an RFP was used, proposals will be evaluated against the award criteria in the RFP and negotiations will take place with each contractor still in contention after initial review. This action may take place within the formalized procedures of Formal Source Selection, in which panels of government personnel review in detail all segments of each contractor's proposal and make recommendations to a formally appointed Source Selection Authority or, in the less formal program office procedures where the contracting officer determines the winning offerer, with assistance from technical personnel. In either case, extensive cost and price analysis of the

contractors' proposals must be accomplished so that the contracting officer can make a determination that the final price is "fair and reasonable" to the government and to the contractor.

Negotiation allows the fact finding, the discussion, and the bargaining necessary to come to a full understanding of the requirement, the approach the contractor plans to take, the basis for his costs, and any tradeoffs that may be necessary along performance, schedule, logistics support, and costs. For these reasons, virtually all of the weapon systems requirements are converted to contract via the Competitive Proposals method of contracting.

Award of Contract. Once the low bidder or the selected source has been confirmed as responsive and responsible, the final contract is prepared reflecting all of the agreements between the two parties. The contract is reviewed by the contracting officer and his supervisor, by the legal office, and if its amount meets certain dollar thresholds, by higher headquarters' contracting and legal staffs. Once correct and legally sufficient, it is sent to the contractor for signature by the appropriate official and, when returned, it is signed by the contracting officer for the government. The official announcement of contract award can now be made, and multiple copies of the contract are made and mailed to participating or affected organizations. This completes the "buy cycle," but now the actual work must be carried out.

Contract Management. It must be realized that, up to this point, there has been only an exchange of promises about the coming work effort and no real work accomplished. The winning contractor has promised to do the job the government has defined, and the government has promised to give him a certain amount of money and perhaps facilities, equipment, or other support in return. But now, these promises on both sides must be converted to action, and this conversion ushers in the longest phase of the acquisition process, the contract management phase.

While the contractor has the primary responsibility for accomplishing the objectives of the contract, the government is still vitally interested in the contractor's progress and so "looks over his shoulder" while he carries out the contract requirements. Such activities as quality assurance, inspection, and acceptance of finished items; monitoring of financial status and schedule adherence; oversight of the subcontracted portions; and in general, contract compliance are carried out by various government organizations established for this exact purpose. Many of the largest defense contractors have contract administration offices located at their plants, while those who do not are monitored by other offices having responsibility for all contractors in a given geographic area.

12.3 Contracting for Safety. (37:2-1 to 2-3)

To understand effective application of the system safety concept in the acquisition process, it is necessary to be familiar with several axioms regarding contractor reactions to safety requirements. They apply to any contracted activity from aerospace to ditch digging. These axioms were first presented to the Space Division at a system safety seminar in 1973 by Mr. Willie Hammer of Hughes Aircraft Company. They are not intended to be derogatory but just basic facts that must be understood before effective dialogue can be established in a contractor/customer relationship. They are as follows:

a. A contractor will not include any uncalled for effort in a proposal which will increase cost to a level which might not be competitive.
b. A contractor will not accomplish a task unless specifically and contractually required to do so.
c. A contractor will pay more attention to a requirement when the penalties for noncompliance are clear.

Basically, these can all be summed up by a single axiom. Any contractor will respond better to a clearly stated, properly scoped task, with tangible, usable results rather than to a vague generality. In any contractor proposal effort, the emphasis is on submitting the best possible response to the stated task with the lowest possible bid. In preparing a competitive proposal, a contractor cannot afford to elaborate on an implied requirement when such elaboration might increase cost above that of a competitor. At best, they include details of a poorly stated requirement. The possibility always exists, from the bidders' point of view, that a competitor, with inferior knowledge and capability, may win because that lack of knowledge presents a simpler program and thus a lower cost estimate. In preparing a proposal, anything not considered by the bidder as essential to winning the contract is admissible. It is absolutely essential that all the tasks of system safety are clearly and concisely spelled out. First, so that the bidder can prepare a reasonable proposal; second, so that the bidder's proposal can be evaluated; and third, so that the entire process can be tracked closely by both contractor and customer. Once this is understood, we have established the baseline for effective contractor/customer communication.

Inclusion of system safety in the acquisition process requires a functional expertise like the many other activities which contribute to mission success. Military acquisition programs generally obtain their system safety expertise by contract. If mistakes are made in the initial communications regarding application of the system safety requirement, they are longer lasting and less amenable to simple correction than mistakes in other functional areas because of the complex interface in all program phases. If it is to be done right, contracting for effective assessment of mishap risk is particularly dependent on fully defined program safety requirements and a complete understanding of their impact on the overall program. For an effective expression of risk acceptability, the procuring activity needs to communicate the desired risk level to the contractor during the earliest contact. This is preferred before the proposal preparation phase. This communication must express the desires of the procuring activity in a manner that cannot be interpreted wrongly. This is done normally with the RFP.

There are four elements involved in achieving the system safety objectives:

a. The statement of work must clearly define the required tasks.
b. The contract data requirements list (CDRL) must define the data required as a result of those tasks.
c. The bidders' instructions, which accompany the RFP, must specifically define the response that is expected. This is necessary so that the procuring activity can properly evaluate each bidders' responses from the same baseline and assure proper understanding of the task by all participating bidders.
d. The specifications must include all necessary requirements documents to define safety design requirements.

12.4 Statement of Objectives (SOO)

A SOO is attached to an RFP to specific overall top-level objectives for the contractor to accomplish. It is usually not more than two or three pages long. The system safety portion of a SOO is typically very short without much detail; it basically tells the contractor that one of the program's objective is to acquire a safer product and that the contractor should have a program for achieving this objective. The contractor will typically 'answer' the SOO with a statement of work (SOW) and a system safety program plan (SSP).

12.5 Statement of Work (SOW).

A SOW is the part of the contract that defines the work necessary to complete the contractual task. The SOW was formerly prepared by the government, but, under the principles of acquisition reform, is now prepared by the contractor in response to an RFP and a SOO. The SOW is the only means the procuring activity has available to contractually communicate the scope of the system safety task. For this reason, it is essential that the system safety tasks are clearly and concisely defined in a manner which is priceable. The tasks must be stated to provide a realistic balance among other program elements (e.g., tasks, controls, data). The system safety tasks must be stated so that results are produced commensurate with the program phase under contract. The SOW task can consist of a detailed statement of the task or contain only a list of mandatory paragraphs from compliance documents. Elaborate task descriptions are not required; however, a simple statement in the body of the SOO such as, "The contractor shall conduct a system safety program to identify and control mishap risk" will define the task adequately enough so that the contractor will be driven to the tasks defined by the compliance document. (37:2-3)

System Safety Section. (27:10) This section of the SOW must be detailed enough to tell the contractor exactly what kind of system safety program to develop. The contractor has to have enough information to price the system safety program and write an SSPP. Most contractors will propose and do exactly what is written in the SOW. A lack of appropriate detail will probably result in a deficient system safety program. Some of the tasks that should be detailed in the SOW are:

a. Planning and implementing a system safety program meeting the requirements of the latest version of MIL-STD-882..
b. Specifying special relationships among the prime contractor and associate contractors, integrating contractors, and subcontractors.
c. Contractor support of safety meetings such as SSG meetings. If extensive travel is anticipated, estimate the number of trips and locations.
d. Number and schedule of safety reviews, with a statement of what should be covered at the reviews. Safety reviews are best scheduled for major design reviews, such as the system design review, preliminary design review, and critical design review.
e. Contractor participation in special certification activities, such as for nuclear and nonnuclear munitions.
f. Procedures for reporting hazards. The contract data requirements list will specify the format and delivery schedule of hazard reports.
g. Analyses to perform, such as the preliminary hazards list, preliminary hazard analysis, and system hazard analysis. The contract data requirements list will specify the format and delivery schedule of required analyses.
h. Safety testing.
i. Basic risk management criteria. Specify a set of conditions that state when the risk of the hazard is acceptable and that require the contractor to specify alternate methods for satisfying the acceptable risk requirement.
j. Special safety training or certification that might be needed for safe operation of critical systems.
k. Reviews of engineering change proposals and deviations and waivers to make sure design changes do not degrade the safety level of the system.
l. Techniques for doing analyses, such as the fault hazard analysis and fault tree analysis. If included, specify on which system and subsystems the contractor should do these analyses. Specify the candidate top events for fault tree analyses, such as flight control system power loss or failure of solar array to deploy.

12.6 Contract Data Requirements List (CDRL).

Contractual data to be delivered falls into two general categories:

a. Financial, administrative, or management data. The procuring activity requires these data to monitor contractor activities and to control the direction contractor activities are taking.
b. Technical data required to define, design, produce, support, test, deploy, operate, and maintain the delivered product.

Contractor-produced data can be expensive and can represent a major portion of the contractor activities. The system safety data requirements listed on the CDRL, therefore, should represent only the absolute minimum required to manage or support the safety review and approval process. The contractor prepares the data in a format specified by a data item description (DID).

The contractor does not get paid for any data not covered by the CDRL/DID. He is not obligated to deliver anything that you request that is not required by a CDRL. Only certain DIDs are authorized for use. These are indexed in the Acquisition Management System Data List (AMSDL). It is very advantageous to effectively utilize the DIDs which are available. Each DID should be examined carefully, sentence by sentence, to assure complete compatibility with the SOW task. The application of the DID requirement without consideration of the SOW task output can cause the contractor to exert considerable effort and money with little significant gain. (37:2-3)

Based on the data that you require you must prepare an AF Form 585, Contractor Data Requirement Substantiation, for each data item you want the contractor to deliver. Use this form to describe the required data, formats, submittal requirements, distribution, approval requirements, and so on. The SSPP, hazard analysis reports, progress reports, and so on must be included in the CDRL if you want them delivered. Your configuration or data management office incorporates your AF Form 585 inputs into the CDRL by using DD Form 1423, Contract Data Requirements List, or the local equivalent. You can use data items as formats for deliverable safety documentation, but you should tailor them by listing the applicable paragraphs of the latest version of each data item (DI): (27:10-11)

12.7 Bidders' Instructions.

The bidder's instructions convey a message to the bidder that indicates how the proposal will be evaluated. It should, therefore, not surprise anyone to hear that the bidders' proposal responds mainly to what is contained in these instructions, not necessarily what is in the SOO or RFP. That response comes after the contract is let and normally is included in the system safety program plan (SSPP). The management and technical sections of the bidders' instructions should contain system safety response instructions. The bidders' response should be keyed to specific requirements or tasks.. From an evaluation standpoint, the most significant element of the bidders' proposal is the SSPP. This plan must be included in the first program phase that requires significant system safety effort, usually the late concept or early dem/val phase. However, it could be any phase where significant engineering activity is planned and where significant or unusual mishap risk is involved. If these factors are not present, then preparation of an SSPP is not worth the additional cost and should not be required. When an SSPP is included, the following type of statement tailored to specific program needs should be contained in the management section of the bidders' instructions: (37:2-4 to 2-5)

"The offerer shall submit an initial SSPP as part of the proposal."

NOTE: This is not to imply that page limitations on system safety plans are not appropriate. A well-prepared plan can cover the subject in less than 50 pages.

The companion technical system safety tasks, required in the proposal, cover preliminary hazard analysis results, identification of specific safety criteria, implementation of lessons learned, and the description of basic system safety design concepts, etc. These should be examined closely on a case—by-case basis.

Improperly stated bidders' instructions could result in a simple restatement of the SOW task. For proper evaluation, the bidder must convey an understanding of how the tasks will be conducted. If this understanding is not evident, the proposal will be judged unacceptable. The bidders' instructions in the technical area vary considerably with the magnitude of the RFP task.

In the initial phases, a statement such as the following should be included in the bidders' instructions. "The offerer shall submit a summary of system safety considerations involved in initial trade studies." In later phases, it may be advantageous to require the offerer to "submit a preliminary assessment of mishap risk." The validation phase may require the bidder to describe system safety design approaches that are planned for particularly high-risk areas (i.e., common bulkhead between propellant tanks, use of liquid fluorine to toxic propellants, use of lithium batteries, etc.) During this program phase, the following statement should be included. (37:2-5)

"The offerer shall submit a description of the planned system safety design and operational approach for identification and control of safety-critical, high-risk system design characteristics."

You cannot formally request any data items, such as the SSPP or PHL, before contract award. However, you can instruct the bidders to discuss their proposed system safety program in detail, including typical hazards and design solutions for them or candidate hazards for analysis. Careful wording can provide almost the same results as a draft data item. Key areas of interest, such as personnel qualifications or analysis capabilities, can be cited from data items as guides for the bidders' discussions. ." The ITO also includes the criteria, preferably prepared by you, for fairly and impartially evaluating each proposed system safety program during source selection. These criteria also inform bidders what areas they must include in their proposals. Sample criteria could include the following:

a. Describe in detail the system safety organization, showing organizational and functional relationships and lines of communication.
b. Describe in detail the analysis technique and format to be used to identify and resolve hazards.
c. Justify in detail any deviations from the RFP. (27:12)

12.8 Specifications.

Specifications are the instructions to the designer dictating the way the system will perform. It is here that specific safety design parameters are presented to the designer. Documents which contain specific design parameters affecting the safety of operation are made applicable here, not in the compliance section of the SOW. Designers normally do not stray so far from their work that they are interested in any more than what they are specifically tasked to do. Documents such as MIL-STD-1522 which contains specific instruction for pressure vessels, placement of relief valves, gauges, and high-pressure flex hose containment; MIL-STD-1576 which contains specific design parameters for electric explosive devices; MIL-HDBK-454 which specifies design controls for electrical hazards; and control of static discharge. If they are not called for specifically in the specifications, you cannot be sure that the completed design will be acceptable. Mistakes here are very costly. If the approving authority will not accept your design, you must go back and make a change. Waivers to a requirement are obtainable, but they normally are granted for a specific limit. Eventually, the problem must be fixed. Whether these specifications are contractor prepared or supplied by the managing activity, it is important that proper instructions are given directly to the designer who controls the final safety configuration of the system. (37:2-6)

The various types of specifications are:

Type A - System/Segment Specification

Type B - Development Specifications

B1 - Prime Item
B2 - Critical Item
B3 - Noncomplex Item
B4 - Facility or Ship
B5 - Software

Type C - Product Specifications

C1a - Prime Item Function
C1b - Prime Item Fabrication
C2a - Critical Item Function
C2b - Critical Item Fabrication
C3 - Noncomplex Item Fabrication
C4 - Inventory Item
C5 - Software

Type D - Process Specifications

Type E - Material Specifications

Type A System Specification defines the system-level functional requirements of the system. Usually developed during the concept phase and updated during the demonstration/validation phase, this type specification forms the baseline for performance of the whole system. (See Figure 12-1)

Type B Development Specifications developed during the latter portion of the demonstration/validation phase, define functional requirements of various major subsystems; i.e., configuration items. They provide general guidance for preliminary and, later, detailed design work. (See Figure 12-2)

Type C Product Specifications are formulated during the late full-scale development stage and provide initial production guidance by defining functional performance requirements and detail design fabrication requirements. The product performance specification defines the requirements of the system as it is intended for use under operational conditions. Fabrication specifications detail the parts and assemblies, as well as the production tests and inspections.

Type D Process Specifications outline requirements for treatment of the system, subsystem, or materials used in the system. They cover manufacturing areas (such as heat or chemical treatments, welding, plating, markings, shipping and handling, etc.) that require specific processes to be performed.

Type E Material Specifications define the detailed requirements in the production process of materials used, such as chemicals, raw materials, various paints and coatings, cables, and tubing.

MIL-STD-961 gives the format for preparing the standard types of specifications. Appendix I of MIL-STD-961 identifies the title and contents of each paragraph of the system specification. Other appendices describe other types of specifications, such as prime item development, product, and so on. Several paragraphs in the system specification are safety related. You should carefully write parts of or all of the following paragraphs:

a. Health and Safety Criteria. This paragraph concerns the health of operations personnel. It should include firm requirements for radiation levels (such as X-rays from high-power amplifiers and antenna radiation patterns), toxic gases, high noise environment, potable water, nuclear radiation, non-nuclear explosive requirements, and so on. Each system has its unique operating environment, and you must anticipate all possible associated health problems and put firm requirements for solving those problems in this section. Those problems missed may be identified by the contractor's system safety program. The advantage of identifying actual or anticipated health problems in this section of the system specification is that their solution will be included in the contract price and be a design requirement.
b. Nuclear Control Requirements. This paragraph should include known nuclear safety rules with which the contractor must comply.
c. Safety Requirements. This paragraph should contain general system-level safety requirements. Some examples of these requirements can be found in MIL-HDBK-454 and paragraph 5.13 of MIL-STD-1472. You should not cite an entire document or design handbook and expect the contractor to comply with every design criteria in it. You may also identify the acceptable probability numbers for Category I and II hazards, if such numbers have been determined. This gives them greater visibility.
d. Functional Area Characteristics. This paragraph has subparagraphs that address more specific lower-level safety requirements, such as safety equipment. Under paragraph 3.7, identify all emergency-use hardware, such as fire extinguishers, smoke detection systems, and overheat sensors, that the system operating environment requires as necessary for sensible precautions.
e. Quality Conformance Inspections. This paragraph requires the contractor to verify by inspection, analysis, or actual test each requirement in section 3 of the system specification. System safety engineering requirements should also be verified. The requirement for verification is often included in the contractor's human engineering program. Therefore, in paragraph 4.2, you should task the contractor to verify the corrective actions taken to manage the risk of all Category I and II hazards. The corrective measures would be verified by inspection, analysis, or demonstration.

12.9 Proposal Evaluation. (27:11)

After the RFP is released to industry, several potential contractors will prepare and submit proposals. You will probably be required to participate in part of this process.

Bidders' Briefing. For large, high-interest programs, bidders may prepare summary briefings on their interpretation of the RFP and on key points of their proposals. If possible, you should attend. Observe how and where safety is addressed but do not be surprised if it is missing. Make mental notes on any areas you may wish to verify against the RFP and bidders' proposals.

Source Selection. This is the culmination of all your RFP activity. Now you evaluate the response to each bidder's proposal to your RFP system safety requirements. You will attend a source selection in-brief that will tell you what you should and should not do. Evaluate each proposal against only the RFP and its criteria and requirements. Do not discuss anything about the source selection outside the source selection area. Use the source selection criteria you included in the ITO for your evaluation. You may also be required to prepare descriptions and standards for system safety factors or items that will be part of your evaluation. (These descriptions and standards for system safety factors are part of the source selection process and are not part of the RFP or anything given to the bidder.) Bidders' proposals must be evaluated in terms of source selection criteria—how well bidders respond, exceptions taken, and so on. It is important to evaluate each proposal for the bidder's knowledge of implementing a system safety program, adequate resources and qualified personnel, and the system safety role in their management structure. Your evaluations will be given to the source selection authority. The source selection authority is the final authority and will make a selection decision based on all the evaluations from source selection participants.

Negotiations. In some cases, you may be invited to take part in negotiations in which face-to-face questions are asked before a selection decision is made. This is a rare but extremely beneficial opportunity to make sure the bidders understand exactly what you require for your system safety program. Remember the following:

a. The USAF contracting officer is in charge. Do only what you are told to do.
b. Restrict everything you say to only that bidder's proposal and the RFP.

12.10 Evaluation Standards. (37:2-6 to 2-7)

Now that we have clearly established with the bidder the type of response that is expected, it is essential that we determine how that response will be evaluated. First, the specific item/element/factor evaluation standards that are prepared by the source selection team must be consistent with the bidders' instructions. They must be in sufficient detail to allow objective evaluation by any member of the team. In the preceding section, the bidders' instructions were keyed to paragraphs in the DID for a SSP; therefore, the evaluation factors should be keyed to the same data item paragraphs as listed in the management area of the bidders' instructions.

Examples of evaluation standards are:

a. Does the organization chart define organizational and functional relationships?

b. Are the responsibilities and authority of system safety personnel and other program organization elements described?

c. Is the organizational unit responsible for executing each task identified?

d. Is the authority for hazard resolution identified?

To be minimally acceptable, a contractor proposal must have the following:

a. A representative organization.
b. Clear responsibilities/authority.
c. A qualified manager.
d. Adequate resources.

From this base, if the contractor misses on a few counts, you can correct any problems after contract award. Without it, you will find the contractor playing catch-up, struggling for routine task effort, etc. This situation is a significant safety risk in itself. Your program will fail!

Figure 12-1

Type A--System/Segment Specification Format

Section 1. SCOPE

Section 2. APPLICABLE DOCUMENTS

Section 3. SYSTEM REQUIREMENTS

- 3.1 Definition
- 3.2 Characteristics
  - 3.2.1 Performance Characteristics
  - 3.2.2 System Capability Requirements
  - 3.2.3 External Interface Requirements
  - 3.2.4 Physical Characteristics (including safety)
  - 3.2.5 System Quality Factors
    - 3.2.5.1 Reliability
    - 3.2.5.2 Maintainability
    - 3.2.5.3 Availability
    - 3.2.5.4 Additional Quality Factors
  - 3.2.6 Environmental Conditions
  - 3.2.7 Transportability
  - 3.2.8 Flexibility and Expansion
  - 3.2.9 Portability
- 3.3 Design and Construction
  - 3.3.1 Materials
    - 3.3.1.1 Toxic Products and Formulations
  - 3.3.2 Electromagnetic Radiation
  - 3.3.3 Nameplates and Product Markings
  - 3.3.4 Workmanship
  - 3.3.5 Interchangeability
  - 3.3.6 Safety
  - 3.3.7 Human Engineering
  - 3.3.8 Nuclear Control (including nuclear safety rules)
  - 3.3.9 System Security
  - 3.3.10 Government-Furnished Property Usage
- 3.4 Documentation
- 3.5 Logistics
- 3.6 Personnel and Training
- 3.7 Characteristics of Subordinate Elements
- 3.8 Precedence
- 3.9 Qualification
- 3.10 Standard Sample
- 3.11 Preproduction Sample, Periodic Production Sample, Pilot or Pilot Lot

Section 4. QUALITY ASSURANCE

- 4.1 General
  - 4.1.1 Responsibility for Inspection
  - 4.1.2 Special Tests and Examinations (safety verifications)
  - 4.1.3 Requirements Cross Reference Section

Section 5. PREPARATION FOR DELIVERY

Section 6. NOTES

- 6.1 Missions
- 6.2 Threat

APPENDICES

Figure 12-2

Type B--Development Specification Format

Section 1. SCOPE

Section 2. APPLICABLE DOCUMENTS

Section 3. REQUIREMENTS

- 3.1 Prime Item Definition
  - 3.1.1 Prime Item Diagrams
  - 3.1.2 Interface Definition
  - 3.1.3 Major Components List
  - 3.1.4 Government-Furnished Property List
  - 3.1.5 Government-Loaned Property List
- 3.2 Characteristics
  - 3.2.1 Performance
  - 3.2.2 Physical Characteristics
    - e. Health and safety criteria
  - 3.2.3 Reliability
  - 3.2.4 Maintainability
  - 3.2.5 Environmental Conditions
  - 3.2.6 Transportability
- 3.3 Design and Construction
  - 3.3.1 Materials, Processes and Parts
  - 3.3.2 Electromagnetic Radiation
  - 3.3.3 Nameplates and Product Marking
  - 3.3.4 Workmanship
  - 3.3.5 Interchangeability
  - 3.3.6 Safety
  - 3.3.7 Human Performance/Human Engineering
- 3.4 Documentation
- 3.5 Logistics
  - 3.5.1 Maintenance
  - 3.5.2 Supply
  - 3.5.3 Facility and Facility Equipment
- 3.6 Personnel and Training
  - 3.6.1 Personnel
  - 3.6.2 Training
- 3.7 Major Component Characteristics
- 3.8 Precedence

Section 4. QUALITY ASSURANCE PROVISIONS

- 4.1 General
  - 4.1.1 Responsibility for Tests
  - 4.1.2 Special Tests and Examinations
- 4.2 Quality Conformation Inspections

Section 5. PREPARATION FOR DELIVERY

Section 6. NOTES

Section 10. Appendix I

CHAPTER 13

EVALUATING CONTRACTOR SYSTEM SAFETY

13.1 Process.

In this chapter, we consider the different ways that we evaluate the effectiveness of a system safety program, both at the program office and the contractor level. First, in appraising the management effort, we determine the safety level that we are assessing; then, to establish an evaluation scale, we use other indicators, such as job descriptions, personnel qualifications, and managerial authority and control. This is judged in two ways: first, by reviewing documents such as the system safety program plan, trade studies, preliminary hazards analysis report, and the operating hazards analysis; second, by participating in contractor/customer technical interchange meetings and formal design reviews. Remember, rarely are we faced with strictly a good or bad program. Each program has varying degrees of effectiveness which may be acceptable in a given situation. Also, based upon the organizational performance level, system safety programs differ.

13.2 Six Levels of System Safety.

The following six generic system safety levels provide a general idea of the variations in tasks and the way these tasks are evaluated.

Level One--Corporate or Headquarters. At this level, the system safety manager establishes policies and develops implementation tools such as standards and techniques. Generally, these individuals are responsible for overseeing multiple independent programs or cost centers. Qualifications should include a working knowledge of the other levels and experience in management and engineering principles.

Level Two--Procurement Activity. This level is predominant at the procurement activity where contracts are written, policies and implementation tools are turned into contractual direction. Contractors have some activity in this area when they write specifications for subcontractors or vendors. Professional safety expertise, coupled with an understanding of the procurement process and effective contractor communications, is required for effective performance.

Level Three--Contractor's Management System Safety Program. At the contractor's facility, the system safety manager uses contractual direction to develop, manage, and control the program and its resources. To perform effectively, this individual must not only know company policies, procedures, and practices but also he or she must understand the requirements, activities, and functions of level four, Contracting Engineering System Safety Program, and level five, Specifications and Requirements, incorporated into the design. Also, a good grasp of operational concepts, level six, is an asset.

Level Four--Contractor's Engineering System Safety Program. The system safety engineer should possess in-depth knowledge of engineering concepts, the system, and associated mishap risk to implement the system safety program. The engineer develops design checklists, defines specific requirements, and performs analyses.

Level Five--Specifications and Requirements. At this level, engineers and designers, possessing minimal safety knowledge, incorporate safety criteria, specifications, and requirements into the system or product design. It is essential that they know how to convert these requirements and criteria into a safe design.

Level Six--Operational Location. The activities, at this level, usually occur at an operational location where the end product is used. The system users and operators take the system analysis and operational data, prepared at level four, Contractor's Engineering System Safety Program, and level five, Specifications and Requirements incorporated into the design, and manage the operations. In-depth knowledge of the system's operational concepts and characteristics is essential. To function effectively, individuals should be qualified at the contractor's system safety program level—level three; at the program implementation level—level four; and at the specifications and requirements incorporation level—level five. Also, one should be knowledgeable of the principles at the second level, the procurement activity, and at the first level, corporate or headquarters.

Generally, the contractor's system safety program effectiveness is evaluated on achievement in establishing and implementing the system safety program—levels three and four, respectively. Also, program effectiveness is measured by how well the specifications and requirements are incorporated into the design—level five and the success of the operational activities—level six. Operational success is influenced considerably by the quality of the system safety program at level three. Needless to say, dynamic interest at the corporate or headquarters level considerably enhances the overall system safety program's effectiveness.

13.3 Management and Planning of a System Safety Program.

Four essential factors or primary drivers of an effective system safety program that must be considered separately from other criteria are personnel qualifications and experience, managerial authority and control, effective program planning, and sufficient resources. If one of these is missing or insufficient, the program will fail.

Personnel Qualifications and Experience. To provide decision makers with adequate mishap risk assessments, the government program manager must insist that the contractor have fully qualified, responsive system safety management personnel. This is not an unreasonable requirement since the contractor's system safety manager is the one who certifies, for his employer, that all safety requirements have been met. Qualifications desired are listed in Chapter 11.

To evaluate an individual's qualifications, first one determines which one of the six system safety levels, mentioned in paragraph 13.2, applies to the job. Usually, contractor activities encompass levels three through six; however, other levels sometimes are covered. Using a "Job Analysis Worksheet," Figure 13.1, one assesses the job requirements for the specific level. You determine the major job requirements and the knowledge, skills, and abilities (KSA) necessary to implement the program successfully. The government system safety manager requests the contractor to submit a position description that addresses the job functions and supports major job requirements, and the candidate's resume. The position description is reviewed against the job requirements; then, reviewed against each KSA to determine if the candidate is really qualified to perform the job. Sample position descriptions are in Attachment I of this chapter. Normally, when a waiver is granted, it will be valid only for the specific program requested.

Management Authority and Control. The system safety manager's authority and control may be evaluated at various stages in the program. First, by reviewing the contractor's proposal, which usually contains a preliminary system safety program plan, one ascertains the type of system safety program being established. The acquisition manager should review the proposal for the following points:

- What is the reporting level of the safety manager?
- What is the relationship between safety and the other disciplines?
- Can the safety manager effectively do the job in the proposed organization?
- Does the contractor recognize and understand the requirements?
- Does the contractor visualize his job at the right level and focus on the end events and products?

Later, by evaluating the updated system safety program plan, the government system safety manager is able to assess if the proposed program is a reality. Questions to aid in evaluating the contractor system safety manager's authority and control are given in Attachment II of this chapter.

System Safety Program Planning. An effective system safety program results primarily because both government and contractor program management recognize the importance of the planning task. The contractor's system safety tasks and activities will be implemented. To a major extent, the contractor's approach determines the program effectiveness in terms of cost and technical value. Since warning signs of an ineffective program may arise during the plan preparation, the government system safety manager may prevent an ill-conceived safety program by conducting early evaluations and discussions with the contractor. The contractor's problems in system safety planning phases are complex and not always obvious to either the preparer or the evaluator.

Effective planning includes a systematic, detailed overall program analysis and the application of system safety requirements. One way to achieve this is to break down the entire program into tasks and subtasks as the basic elements relate to each program organizational element. Attachment III, Example of Contractor Work Breakdown Structure, provides an excellent sample of how a work breakdown structure is accomplished. The system safety manager must determine the resources necessary to complete each task element and the organizational element responsible for task completion. These organizations have funds for system safety tasks allocated in their budgets. If possible, the system safety manager should control both manning and monetary resources. Effectiveness evaluation includes how well the planning phase was accomplished. Again, the System Safety Checklist, Attachment II, will provide appropriate questions that the government system safety manager should ask in assessing the effectiveness of program planning.

Resources. An excellent proposal and plan are nothing more than beautiful prose without adequate resources to accomplish the job. The right level of effort for each task and sufficient funds to obtain necessary engineering assistance must be allocated and applied appropriately. In evaluating a system safety program's resources, manning is a prime consideration. As a general rule of thumb, the following scale was developed to assist in considering the adequacy of manning resources depending on system complexity:

Level One. One and a half to two qualified system safety managers for each major subordinate organization.

Level Two. One to two dedicated system safety managers for each three major program segments or one dedicated person for each segment of $5,000,000 or more.

Level Three. One qualified manager for each program segment of $5,000,000 or more. For programs less than $5,000,000, it is acceptable to consider attestment from an outside consultant to the effect that all requirements have been met.

Level Four. Five percent of engineering manning for each major program segment.

Level Five. At least one dedicated engineer for each major subsystem or for each system segment.

Level Six. The manning requirements at this level vary considerably with system and operational complexity, number of facilities or areas involved. System safety manning should never be less than one qualified engineer/manager for each major operational segment.

13.4 Engineering Effectiveness of a System Safety Program.

Having covered various areas to consider and questions to ask in evaluating the system safety program's management effectiveness, now we concentrate on the other half—the system safety program's engineering effectiveness. Needless to say, in determining overall system safety program effectiveness, there is some overlapping in the documents that are reviewed, such as the proposal, the system safety program plan, and the work breakdown structure. However, in this section, the emphasis is on evaluating technical documentation during the different program phases.

Requirements Definition, Concept Development, and System Definition. During these phases of the program, the contractor's safety effort is in updating the system safety program plan, working on trade studies, identifying safety requirements, and establishing the system design baselines. The government system safety manager is able to evaluate the contractor's activities by participating in system safety group meetings or technical interchange meetings and reviewing the following points:

a. Trade study reports for proper consideration of system safety requirements as a driver.
b. Proposed system safety program plan data, for compliance with the Attachment II checklist in this chapter, that was filled out during proposal evaluation.
c. Review contractor-prepared checklists for accuracy, completeness, and validity.

Allocation of Requirements. Safety requirements are generated from such items as trade study results, the preliminary hazard analyses, and the risk factor matrix. By attending the contractor technical interchange meetings, the government system safety manager should be able to

ascertain if the safety requirements are being incorporated into the design and, also, if the contractor's approach is satisfactory.

System Requirements Review. This review is conducted when the majority of the system functional requirements are established. By reviewing the system specifications and participating in the contractor/customer technical interchanges, the government system safety manager is able to evaluate the adequacy of the contractor's efforts to establish and incorporate safety requirements into the design specifications.

System Design Review (SDR)/SDR Safety Review. By SDR, the government system safety community determines if the contractor has the capability to accomplish the safety tasks satisfactorily. The government system safety manager should review such information sources as:

a. System safety program plan.
b. Work breakdown of system safety tasks, subtasks, and manpower.
c. Overview of system and mission, including safety-critical systems, subsystems, and their interrelationship with mission operations.
d. Proposed ground support equipment.
e. Mission operation scenarios.
f. Tabulation of hazards identified.
g. Review of initial checklist.

And, while reviewing the listed information sources, the following key points should be considered:

a. Identification of key safety people in the contractor's organization.
b. Authority and responsibility of key safety positions.
c. Key system safety personnel qualifications.
d. Safety program milestones
e. Proposed hazard analysis methods.
f. Control system for identification, recording, tracking, resolution, and close-out of problems.
g. Contractor manning and monetary resources.

After evaluating all the information, the government system safety manager should be able to determine if the minimum requirements for a successful program, at this phase, have been met. Minimum requirements are:

a. Contractor's demonstration of capability to perform system safety activities in compliance with MIL-STD-882.
b. Contractor's demonstration of understanding of applicability of safety requirements and specific hazard identification.

Preliminary Design Review (PDR)/PDR Safety Review. This phase occurs early in system development prior to the detailed design process. It measures the progress and adequacy of the design approach and establishes physical and functional interfaces between the system and other systems, facilities, and support equipment.

Associated with PDR is the PDR Safety Review which considers the identified hazards and mishap causes and looks at the intended design controls. The government system safety manager usually reviews the following documents at this point:

a. Preliminary Accident Risk Assessment Report verified by both program manager and system safety manager.
b. Draft preliminary checklists.
c. Mission scenarios, including planned operations.
d. Current hazards lists.
e. System and subsystem descriptions.
f. Hazard reports.

During the documentation review, the following key points should be checked:

a. Preliminary hazards analysis activities.
b. Effectiveness of verification effort.
c. Changes to the SDR baseline.
d. Proposed operations and ground support equipment.
e. Proposed facilities design.

Finally, the government system safety manager must determine if the following requirements have been met:

a. Preliminary design meets requirements established by the request for proposal.
b. All hazards have been identified.
c. Proposed hazard controls and verification methods are adequate.
d. Safety-critical interfaces have been established and properly analyzed.

Critical Design Review (CDR)/CDR Safety Review. CDR occurs when the detail design is complete and fabrication drawings are ready to release. The Safety CDR centers on the final hazard controls' incorporation into the final design and intended verification techniques. Requirements compliance is assessed. By this review, design-related safety issues must be closed. The information sources to review are:

a. Accident Risk Assessment Report verified by program manager
b. Operating hazards analysis approach.
c. Operating timelines matrices.
d. Operational scenarios identifying:

    (1) Hazardous operations,
    (2) GSE planning and preliminary design,
    (3) Proposed procedures list,
    (4) Proposed operational hazard controls.

And, while reviewing these information sources, the key points for evaluation are:

a. System hazard analysis activities.
b. Operating hazard analysis activities.
c. Training requirements.
d. Personnel protection requirements.
e. Safety-critical GSE design.
f. Effectiveness of design hazard controls.
g. Interface analysis.

At the CDR Safety Review phase, the requirements that must be met for a successful program are:

a. Final design meets goals set by request for proposal.
b. Hazard controls have been implemented and verification methods defined.
c. GSE preliminary design hazards and controls have been identified.
d. FSE design and proposed operational flow are acceptable.
e. All interface analyses are complete.
f. Contractor certification that all contractual design requirements are met.

Preoperational Safety Review. At this review, the contractor presents the final hazard reports with controls incorporated and verified for both the operational hardware and the support equipment. Ideally, procedures and technical orders are complete; however, if they are not, then a tracking system must ensure that controls are incorporated and safety validation is performed prior to first use. The following information sources should be reviewed:

a. Completed and verified operating hazards analysis.

b. Approved change proposals.
c. Completed and verified system hazards analysis.
d. Completed and verified checklists.
e. Contractor's hazard close-out logs.
f. Summary of hazards analysis results and assessment of residual risk.

The key points for evaluation are:

a. Operating hazards analysis.
b. Changes to CDR baseline.
c. System hazard analysis.
d. Close-out of action items.
e. Assessment of residual risk.

At the preoperational phase, the requirements for a successful safety program are:

a. Acceptable systems and operational hazards analysis.
b. Operational procedures/technical orders are complete and verified.
c. All hazards are controlled effectively and controls verified as effective.
d. Checklists are completed and actions verified.
e. Contractor has verified and certified that all requirements are met.

ATTACHMENT I

Basically, the sample position descriptions support the major job requirements listed in Figure 13-1, Sample Job Analysis Worksheet. These position descriptions support assignments at some of the system safety levels discussed in paragraph 13.2.

LEVEL I: MANAGER--SUPERVISOR

QUALIFICATIONS

Minimum of a baccalaureate degree in an engineering or an applied Science, Safety, or Business Administration curriculum; with a minimum of 4 years system safety experience; with approximately 8 years diversified experience in various systems and safety administration is desired; or demonstrated capability, through previous experience and education, to perform successfully the duties and responsibilities shown below.

DUTIES AND RESPONSIBILITIES

Under the direction of the corporate vice president, supervise employees who manage safety programs for programs during the design, production, test, maintenance, and use of company products and facilities; monitor all home office field safety operations to assure conformance with established requirements and criteria.

Develop and implement program system safety tasks based on contract, government, and corporate safety requirements. System safety tasks include the following: preparing program safety plans; developing and complying with program safety budgets; preparing hazards analysis and safety-related trade studies; participating in design reviews; reviewing engineering change summaries as required; reviewing approval and validation of test and maintenance procedures; monitoring hazardous operations and safety audits; permanent member of the program certification board; initiating safety requirements in training courses; and providing interface with the customer's safety representative to ensure a single point of contact for program safety functions.

Develop safety policy, techniques, and criteria which will assure division compliance with all corporate, governmental, and contractual safety requirements; maintain a continuing liaison with customer personnel to ensure their understanding of company's system safety program.

Select and assign an appropriate safety representative for each program/product or functional area, as required. Integrate all inputs from affected departments and resolve safety problem differences.

Establish and conduct audits to verify and measure the performance of the safety program.

Establish safety data files and maintain records of criteria, actions, and other applicable safety data.

Establish a working relationship with personnel/industrial safety.

Develop, maintain, and improve system safety technology, personnel skills, and physical resources to effectively support existing and future programs; administer personnel development and evaluation programs.

Publish and maintain procedures which describe and direct the system safety functions.

Convene and chair the Systems Accident Investigation Board and develop and implement Systems Accident Investigation Procedures; serve as a permanent member of the Division Central Standardization Board.

Evaluate and approve or disapprove experiments and tests conducted by the division that involve risk to humans; approve or disapprove environmental effects and equipment operating procedures.

LEVEL I

TITLE: ENGINEERING, PROGRAM--SYSTEM SAFETY

QUALIFICATIONS

Minimum of a baccalaureate degree in engineering or an applied Science, Safety, or Business Administration curriculum; with a minimum of 4 years system safety experience; with approximately 8 years diversified experience in system safety program development and administration is desired; or demonstrated capability, through previous experience and education, to perform successfully the duties and responsibilities shown below.

DUTIES AND RESPONSIBILITIES

Supports the activities of employees engaged in the planning, directing, and monitoring of the system safety program for one or more functional systems of company products covering the design, research and development, flight, installation, training, and operating of assigned systems. Plan, direct, and control activities of the group performing work typified by the following duties:

Coordinate with line, customer, and other company personnel to establish the system safety program requirements; review and analyze specifications, contracts, requests for proposal authorizations, to understand and become thoroughly familiar with basic program objectives and potential problems.

Prepare or provide program organizations data required to make contract changes of a technical, administrative, or management nature.

Develop and prepare program plans and schedules for system safety program organizations and issue directives for execution of basic plans and modifications to cover proposed, present, and potential aspects of assigned program area.

Monitor program status, reconcile and correct schedule delinquencies, report status, and establish recovery programs for significant program deviations. Review technical work produced by system safety line or program organizations for adequacy and compliance to basic program concepts and philosophies and reconcile conflicting technical or administrative viewpoints or approaches.

Establish and maintain control of manpower, costs, facilities, equipment, and budgetary program allocations.

Maintain liaison with customer and other concerned parties on technical matters related to program requirements and responsibilities of the system safety organizations.

Coordinate with line department to obtain technical assistance and required staffing in accordance with program budget.

LEVEL III

SUPERVISOR

TITLE: MANAGER PROGRAM--SYSTEM SAFETY

QUALIFICATIONS

Minimum of a baccalaureate degree in engineering or an applied Science, Safety, or Business Administration curriculum, including college courses in Safety and Human Engineering; with a minimum of 4 years system safety experience; with approximately 10 years diversified experience in various phases of Engineering, Safety, and Management is desired; or demonstrated capability, through previous experience and education, to perform successfully the duties and responsibilities shown below. Registration as a professional engineer or certification as a system safety professional is required.

DUTIES AND RESPONSIBILITIES

Manage the affairs of the system safety organization for one or more assigned programs. Has full responsibility to:

Establish safety requirements and criteria for incorporation into the design, research and development, flight, installation, checkout, training, and operating of the program product systems.

Monitor functional responsible organizations to ensure the generation of design, test procedures, operating and training manuals, and other technical data concerned with the test, operation, maintenance of product systems are in conformance with the program system safety program. Conduct mishap investigations involving product systems and related facilities, identify causes, and institute corrective action to customer and investigation board's satisfaction.

Audit all areas concerned with operational safety of product systems in the assigned program area, in order to eliminate hazards; recommend improvements and report effectiveness of the system safety program.

Review safety training courses, certification requirements, and manuals; audit the certification program and assure, through the administration and participation of Crew Certification Standboards, the selection of qualified personnel to test, operate, and maintain program product systems.

Review engineering and facilities changes or proposals to ensure incorporation and consideration of safety measures. Coordinate and collaborate with other programs, field test operations, other divisional organizations, associate contractors, and division safety organizations to accomplish an integrated system safety program. Participate in project management planning, affecting assigned functional activities; and establish basic programs for the system safety department, for the assigned programs, in conformance with project and divisional plans and objectives. Make outside contacts to fulfill functional responsibilities.

LEVEL IV

TITLE: ENGINEER, STAFF--SYSTEM SAFETY

QUALIFICATIONS

Minimum of a baccalaureate degree in an engineering or applied science, at Level III, some education or experience in Business Administration is desirable; certification as a Professional Engineer or certification as a system safety professional, with approximately 5 years diversified experience in various aspects of product safety activities and operations, is desired; or demonstrated capability through previous experience and education to perform successfully the duties and responsibilities shown below.

DUTIES AND RESPONSIBILITIES

Serve as a professional authority for the system safety program covering the planning, designing, producing, testing, operating, and maintaining of product systems and associated support equipment. May be assigned to small programs as system safety representative with duties as described below.

Review initial product system designs and advise design personnel concerning incorporation of safety requirements into product system, support equipment, test and operational facilities based on safety standards, prior experience, and data associated with preliminary testing of these items.

Assure a cooperative working relationship and exchange of operational and design safety data with government regulatory bodies, customers, and other companies engaged in the development and manufacture of aerospace systems. Act as a company representative for various customer and industry operational and design safety activities and assist in the planning and conducting of safety conferences.

Evaluate new or modified product systems, to formulate training programs, for updating operating crews and indoctrinating new employees in systems test and operational procedures. Establish training programs reflecting latest safety concepts, techniques, and procedures.

Direct investigations of accidents involving design, test, operation, and maintenance of product systems and associated facilities, and present detailed analysis to concerned customer and company personnel. Collect, analyze, and interpret data on malfunctions and safety personnel, at all organizational levels; and keep informed of latest developments, resulting from investigation findings, affecting design specifications or test and operational techniques. Collaborate with functional safety organizations in

order to set and maintain safety standards. Recommend changes to design, operating procedures, test and operational facilities and other affected areas; or other remedial action based on accident investigation findings or statistical analysis to ensure maximum compliance with appropriate safety standards.

Coordinate with line departments to obtain technical and personnel resources required to implement and maintain safety program requirements.

LEVEL IV

TITLE: ENGINEER, ASSOCIATE--SYSTEM SAFETY

QUALIFICATIONS

Minimum of a baccalaureate degree in an engineering or applied science curriculum with specialized courses in Safety Engineering is desired; or demonstrated capability through previous experience and education to perform successfully the duties and responsibilities below.

DUTIES AND RESPONSIBILITIES

Perform, under supervision, a variety of specific system safety tasks of moderate complexity and scope for an assigned program. Survey the assigned program to determine safety criteria and requirements.

Investigate changes in product design or test and operational procedures to determine where condition of such items could jeopardize functional safety. Prepare necessary reports.

Assist engineer or senior engineer in developing safe operating procedures dealing with product systems and related facilities.

Assist engineer or senior engineer in research of historical performance and in preparation of statistics and functional physical evident.

Submit recommendations to system safety training program.

Assist engineer or senior engineer in the establishment, implementation, and adherence to safety standards for product area.

ATTACHMENT II

SYSTEM SAFETY CHECKLIST

The following checklist has been developed to assist in the evaluation of system safety management and planning. Its use has proved most effective during source selection in the evaluation of contractor proposals. Each item is questioned against an item in the contractor-prepared system safety plan. Those items which are not applicable to the contractor are deleted. Those items which are not mentioned in the plan are considered noncompliant, and the center column is checked. For those items which are mentioned, varying degrees of compliance are possible. Compliance is graded in accordance with the Suggested Evaluation Scale. Comments and proposed resolutions are entered in the “Resolution” column. When the evaluation is complete, the compliance column is averaged.

0 Unacceptable (does not meet minimum requirements)

1 or 2 Marginal (success doubtful)

3 Acceptable (probable success)

4 Excellent (success likely)

5 Superior (success very likely)

6 Outstanding (high probability of success)

The four primary program drivers should be handled as separate issues independent of averaging, to maximize impact.

SUGGESTED EVALUATION SCALE

POINTS

0.....No management planning, personnel not qualified, no authority, resources minimal.

1.....Planning barely adequate, little management involvement, resources inadequate.

2.....Planning adequate, implementation weak, management modestly concerned, resources ineffectively utilized.

3.....Planning generally good, implementation good, management involved, resources adequate and used effectively, program well received in most program areas.

4.....Strong planning, implementation, management involvement; good use of resources, program well received in all affected areas.

5.....Strong, excellently implemented program in all areas.

6.....Outstanding innovative program. Industry leader.

SYSTEM SAFETY CHECKLIST CRITERION

The following requirements are the management items that will be examined in the safety review process. Many items from the general checklist will not be applicable to all types of programs and, thus, some items will not be marked, not applicable, or deleted. Some items are definitions, and no response is needed.

The contractor will establish a safety management system to implement provisions of this standard commensurate with the program contractual requirements. The contractor program manager is responsible for the establishment, control incorporation, direction, and implementation of the system safety program policies and shall assure that the mishap risk is identified and controlled or eliminated within established program mishap risk acceptability parameters.

The contractor will prepare a system safety program plan (SSPP) based on the requirements standard which is identified in the contract statement of work.

The SSPP will be implemented upon approval by the procuring contracting officer and describe the system safety activities required during the life of the contracted program.

The contractor SSPP will be updated at the end of each program phase to describe tasks and responsibilities required for the subsequent phase.

The approved contractor SSPP will account on a item-by-item basis for all contractually imposed requirements, tasks, and responsibilities.

The contractor SSPP includes the details of the system safety manager to program manager relationship and accountability.

The contractor SSPP includes the organization(s) directly responsible for each subtask accomplishment and company policies, procedures, and/or controls governing the conduct of each subtask.

The contractor SSPP includes a composite listing of applicable company policies, procedures, and controls, by title, number, and release date.

The contractor SSPP will be maintained current and subject to procuring activity review. The plan need not be resubmitted to the procuring activity for minor change or release date(s).

The contractor SSPP provides a chart showing the contractor's program organization and identifying the organizational element assigned responsibility and authority for implementing the system safety program.

The contractor SSPP identifies the system safety organization through all management and supervisory levels.

The contractor SSPP identifies the interfaces of the system safety organization and other organizations, including cross-references to applicable sections of other program plans.

The contractor SSPP describes the purpose of each interface.

The contractor SSPP details how resolution and action relative to system safety will be affected at the program management level possessing resolution authority.

The contractor SSPP provides a clearly detailed method by which problems encountered in the implementation of the system safety program and requirements can be brought to the attention of the program manager.

The contractor SSPP includes procedures to be used, to assure completion of action, regarding identified unacceptable risks.

The contractor SSPP provides a description of methods to be used in implementation of each task identified, including a breakout of task implementation responsibilities by organizational component discipline, functional area, or any planned subcontractor activity.

The contractor SSPP describes internal controls for the proper and timely identification and implementation of safety requirements affecting system design, operational resources, and personnel.

The contractor SSPP provides a schedule of the system safety activities and a milestone chart showing relationships of the system safety activities with other program tasks and events.

The contractor SSPP defines the level of effort required for successful completion of contractually required tasks.

The contractor has established a system safety organization which has centralized accident risk management authority, delegated from the contractor program manager, to maintain a continuous overview of the technical and planning aspects of the total program.

The system safety organization is headed by an experienced system safety manager who is directly accountable to the program manager for the conduct and effectiveness of all contracted safety effort for the entire program.

The system safety management provides a single point of contact for the purchasing office, all contractor internal program elements, and other program associate or subcontractors for safety-related matters.

The system safety management reviews and provides input to all plans and contractual documents related to safety.

The system safety management maintains a log, for purchasing office review, of all program documentation reviewed and records all concurrence, nonconcurrence, reasons for nonconcurrence, and actions taken to resolve any nonconcurrence.

The system safety management maintains approval authorityof safety-critical program documentation and all items related to safety contained in the contract data requirements list (CDRL).

The system safety management coordinates safety-related matters with contractor program management and all program elements and disciplines.

The system safety management provides internal approval and technical coordination on waiver/deviations to the contractually imposed system safety requirements, as defined.

The system safety management conducts or arranges for internal audits of safety program activities, as defined, and supports the purchasing office safety audits and inspections, as required.

The system safety management coordinates system safety, industrial safety, and product safety activities on the program to ensure protection of the system during manufacture and assembly.

The system safety management establishes internal reporting systems and procedures for investigation and disposition of accidents and safety incidents, including potentially hazardous conditions not yet involved in an accident/incident; such matters are reported to the purchasing office as required by the contract.

The system safety management provides participation in all requirements reviews, preliminary design reviews, critical reviews, critical design reviews, and scheduled safety reviews to assure that:

a. All contractually imposed system safety requirements, including those imposed by this standard, are complied with.
b. Safety program schedule and CDRL data deliveries are compatible.
c. Hazard analysis method formats, from all safety program participants, permit integration in a cost-effective manner.
d. Technical data are provided to support the preparation of the final analysis summary.

The system safety management participates in all test, flight, or operational readiness reviews and arranges for presentation of required safety data.

The system safety management provides for technical support to program engineering activities on a daily basis. Such technical support will include consultation on safety-related problems, research on new product development, and research-interpretation of safety requirements, specifications, and standards.

The system safety management provides participation in configuration control board activities, as necessary, to enable review and concurrence with safety-significant system configuration and changes.

The system safety management reviews all trade studies and identifies those that involve or effect safety. Provides

participation in all safety-related trade studies to assure that system safety trade criteria are developed and the final decision is made with proper consideration of accident risk.

The system safety management provides participation in program-level status meetings where safety should be a topic of discussion. Provides the program manager the status of the system safety program and open action items.

The system safety management provides for safety certification of safety-critical program documentation and all safety data items contained in the CDRL.

The contractor provides a system safety program milestone chart which identifies tasks and data inputs and outputs which correspond to the program milestones. Milestones are controlled by program master schedule and internal operations directives.

The systems safety integrator prepares an integrated system safety plan (ISSP) which establishes the authority of the integrator and defines the effort required from each associate contractor for integration of system safety requirements for the total system. Associate contractor system safety plans are incorporated as annexes to the ISSP.

The ISSP includes analyses to be conducted by each associate contractor and the format to be utilized.

The system safety integrator identifies data that each associate contractor is required to submit to the integrator and its scheduled delivery keyed to program milestones.

The ISSP includes the schedule and other information considered pertinent by the integrator.

The ISSP specifies the method for the development of system-level requirements to be allocated to each of the associate contractors as a part of the system specification, end-item specifications, and/or other interface requirement documentation.

The system safety integrator initiates action, through the contract manager, to ensure that each associate contractor is contractually required to be responsive to the system safety program; contractual modifications shall be recommended if the need exists.

The system safety integrator conducts safety analyses of the integrated system, operations, and interfaces between assembled end items. Analyses provided by associated contractors are used in the conduct of this effort.

The system safety integrator provides an assessment of the accident risk, presented by the operation of the integrated system, for customer approval.

The system safety integrator provides assistance and guidance to associate contractors in the implementation of interface safety requirements.

The system safety integrator resolves differences between associate contractors in areas related to safety, especially during tradeoff studies. Where problems cannot be resolved by the integrator, a statement of the problem and the recommended solution are provided to the purchasing office for resolution and action.

The system safety integrator ensures that information required by an associate contractor from other associate contractors to accomplish safety analyses is provided in a mutually agreed-to format for compatibility with the integrating process.

A system has been developed, for normal interchange and feedback interchange, and feedback of information related to safety between the purchasing office, integrating contractor, and associate contractors.

The system safety integrator schedules and conducts technical meetings between all associate contractors to discuss, review, and integrate the safety effort.

The system safety integrator notifies the contracting office, in writing, of any associate contractor's failure to meet contract, program, or technical system safety requirements for which they are responsible. The integrator for the effort sends a copy of the notification letter to the affected associate contractor whenever such written notification has been given.

The system safety integrator participates as an active member of the Purchasing Office System Safety Group (SSG); presents the integrated program safety status results of design, operations, or safety reviews; summarizes hazard analysis results; identifies all problems and status of resolutions; and accepts all responses to action items assigned by the chairman of the SSG.

Associate contractors provide sufficient level of effort, commensurate with contractual responsibilities, for conducting analyses of effects on end items; or inputs, normal or abnormal, from other subsystems until such time as the integrator determines that such support is no longer necessary; and such action is approved by the purchasing office.

The system safety manager for each associate contractor controls his own subcontractor system safety activities. Major subcontractors are required to maintain suitable documentation of safety analyses that they have performed, in formats which will prevent incorporation of their data in the overall analysis program.

Major subcontractors are required to develop system safety program plans that shall be included as annexes to the prime contractor's SSPP.

Lesser subcontractors and vendors are required to provide information on component and subassembly characteristics, including failure modes, failure rates, and possible hazards, which will permit contractor personnel to evaluate the items for their impact on safety of the system.

The contractor provides support to the SSG as required by the SSG charter.

The contractor provides assistance to safety review teams, to the extent necessary, to support the system safety certification process.

The contractor conducts the system safety program so that it supplements existing industrial safety and toxicology activities.

When contractor-owned or leased equipment is being used in manufacturing, testing, or handling products developed or produced under contract, analysis and operational proof checks are performed to show that risk of damage to those products has been minimized through proper design, maintenance, and operation by qualified personnel using approved procedures. This does not cover those functions the contractor is required to perform, by law, under Federal or State Occupational Safety and Health, Department of Transportation, or Environmental Protection Agency regulations.

The contractor system safety program encompasses operational site activities. These activities shall include all operations listed in operational time lines, including system installation, checkout, modification, and operation.

Particular attention is given to operations and interfaces, with ground support equipment, and to the needs of the operators relating to personnel subsystems, such as panel layouts, individual operator tasks, fatigue prevention, biomedical considerations, etc.

The contractor includes facilities in the system safety activity.

Facility safety design criteria is incorporated in the facility specifications.

Identified requirements for facilities include consideration of the compatibility with standards equal to or better than those specified by Air Force and federal regulations.

The test and operations safety procedures encompass all development, qualification, acceptance, and preoperational tests and activities.

The procedures include inputs from the safety analyses and identify test and operations and support requirements.

Safety analyses are conducted to evaluate impact of system design changes.

The design and operational criteria contained in the applicable range safety manuals, regulations, and standards are considered in the system safety analysis and the system safety criteria developed for the program. The contractor revises or updates subsystem hazard analyses and operating and support hazard analyses to reflect system design changes during the life of the program. Flight analysis and flight termination system requirements are applicable to the system, during all flight phases, until payload impact or orbital insertion. The final analysis summary includes all aspects of flight safety systems.

Verification of system design, and operational planning compliance with range or operating site safety requirements, is documented in the final analysis summary.

The contractor has established internal procedures for identification and timely action on elimination or control of potentially hazardous test conditions induced by design deficiencies, unsafe acts, or procedural errors. Procedures shall be established to identify, review, and supervise potentially hazardous, high-risk tests, including those tests performed specifically to obtain safety data.

The contractor system safety organization reviews and approves test plans, procedures, and safety surveillance, procedures, and changes to verify incorporation of safety requirements identified by the system analysis. The contractor system safety organization assures that an assessment of accident risk is included in all pretest readiness reviews.

Safety requirements for support equipment are identified in the system safety analyses.

Support equipment safety design criteria are incorporated in the segment specifications.

Safety requirements for ground handling have been developed and included in the transportation and handling plans and procedures. Safety requirements for operations and servicing are included in the operational procedures. The procedures are upgraded and refined, as required, to correct deficiencies that damage equipment or injure personnel.

Special attention is given to planning, design, and refurbishment of reusable support equipment, including equipment carried on flight vehicles, to assure that safety is not degraded by continued usage. Identified requirements for support equipment, used as the operational site, include consideration to the compatibility with standards equal to or better than those specified by Federal and Air Force Occupational Safety and Health regulations.

The contractor shall review engineering change proposals (ECP) to evaluate and assess the impact on safety design baseline. This safety assessment will be a part of the ECP and will include the results of all hazard analyses done for the ECP.

The contractor conducts safety analyses for all applications of radioactive sources, nuclear power systems, and other systems having sources of ionizing radiation. This analysis includes a complete assessment of the accident risk in areas of normal mission analysis and contingency analysis. A complete assessment of the accident risk in normal mission analysis includes:

a. Transportation, handling, calibration, testing, and processing during prelaunch operations at the launch site, including use of nonflight sources.
b. Flight safety (launch, flight to orbit or ballistic reentry, and random and random reentry).
c. Recover operations at mission termination site.

A complete assessment of the accident risk in contingency analysis includes:

a. Operational site accident (fire, explosion, impact, rupture, dispersal, and release quantity).
b. Flight accident
c. Abnormal reentry, recovery, or disposition.
d. Abort conditions.
e. Accident mode and characteristics.
f. Accident probability, normal mission, and worst case accident consequences.
g. Chemical toxicity and external radiation.
h. Conclusions.

System safety engineering personnel participate in all trade studies that have been identified as being safety-related and shall ensure that safety-impact items and accident risk assessments are significantly highlighted and given appropriate weight as decision drivers.

Trade study documentation shows that the accident risk for the recommended solution is equal to or less than the other alternative being traded, or provide sufficient justification for recommending another alternative.

Results of trade studies shall be reviewed to ensure that recommendations, for management-level decisions, include the optimum safety provisions developed for each option.

The contractor identifies any deficiencies regarding safety analysis or risk assessment, when they are not provided with government-furnished equipment and property and shall be brought to the attention of the purchasing office as a safety concern. (The contractor, upon direction of the purchasing office, performs a system safety analysis.)

Recommendations for action and resolution of identified problems are included in the final analysis summary to the procuring contracting office.

The contractor identifies any deficiencies where adequate data to complete contracted safety tasks is not provided to the purchasing office as a safety concern. Upon purchasing office direction, the contractor initiates efforts to develop or obtain the required data.

Deliverable safety data, as cited on the CDRL, are presented in the format specified unless a modification has been approved by the contracting officer. Where no format is indicated, the contractor may use any format that presents the information in a comprehensible manner.

Contractor has internal procedures and requirements which indicate an understanding that management approval and submittal of all safety data produced in compliance with contractual requirements constitutes certification that accuracy, completeness, and validity of safety data have been attested to by a qualified system safety engineer and that the system can be operated safely within the parameters specified by the inaugurating activity. Nondeliverable safety data, necessary for contractor's conduct of the system safety effort but not contractually required to be submitted, is available for onsite review, on request, to persons authorized by the purchasing office.

The contractor system safety manager pursues an aggressive program of acquiring and maintaining current safety-related information and data pertinent to the contract.

The contractor system safety manager maintains liaison with purchasing office data sources to obtain:

a. Safety data as a design aid to prevent repetitive design or procedural deficiencies.
b. Information on operational systems which are similar to the system under this contract and should be studied for past safety problems and their solutions.
c. Authority for access of personnel to nonproprietary information on accident and failure causes and preventive measures in possession of government agencies and contractors involved with those systems.

The contractor maintains safety-related data, generated on the program, in the program safety data file. A log of all safety-significant documentation shall be maintained showing concurrence or nonconcurrence, reasons for nonconcurrence, and corrective action taken to resolve the problem. The log is available for review by the purchasing office. The system safety organization also organizes and maintains frequently used reference data.

Safety inputs to training programs are tailored to the personnel categories involves and included in lesson plans and examinations.

Safety training includes such subjects as hazard types, recognition, causes, effects, and preventive and control measures; procedures, checklists, and human error; safeguards, safety devices, and protective equipment, monitoring and warning devices, and contingency procedures. Safety programs will be developed and provided for specific types and levels of personnel (i.e., managers, engineers, and technicians involved in the design, product assurance operations, production, and field support).

Test, operations, and field support personnel are certified as having completed a training course in safety principles and methods.

Specific certification requirements are established by a program certification board that includes the system safety manager as a member.

Contractor safety training also includes government personnel who will be involved in contractor activities.

System safety audits are conducted by the system safety manager and, on a periodic basis, by a contractor management team independent of the program. The audit clearly measures the status of each safety task, interrelationship between safety and other program disciplines, identification and implementation of safety requirements criteria, and documented evidence which reflects planned versus actual safety accomplishment.

Each audit evaluates program milestones and safety program milestones, incompatibility that require remedial corrective action, and safety outputs to program requirements. The contractor initiates positive corrective actions where deficiencies are revealed by the audits. The system safety manager also supports government system safety as may be directed by the purchasing office.

Components, equipment, conditions, designs, or procedures which provide unusual safety problems are also audited.

Audits include verification or corrective action on problems revealed by previous audits.

Subcontractors are audited by the prime contractor to ensure that:

a. They are producing items whose design or quality will not degrade safety,
b. Safety analyses are conducted as required, and
c. Problems are being brought to the attention of their own program managers and prime contractor management.

The system safety manager participates in all scheduled program safety and design reviews. Presentation of system safety program status and safety problems having program impact shall be included in each program review.

The contractor provides engineering and technical support for mishap investigations when deemed necessary by the management activity. This support includes providing contractor technical personnel to the mishap investigation board.

Figure 13-1

Sample Job Analysis Worksheet: System Safety Manager

Knowledge, Skills, and Abilities (KSA)

1. Knowledge and ability to manage interrelationships of all components of a system safety program in support of both management and engineering activities. This includes planning, implementation, and authorization of monetary and personnel resources.
2. Knowledge of theoretical and practical engineering principles and techniques.
3. Knowledge of hazardous systems and environments.
4. Knowledge of management concepts and techniques.
5. Knowledge of this life-cycle acquisition process.
6. Ability to apply fundamentals of diversified engineering disciplines to achieve system safety engineering objectives.
7. Ability to adapt and apply system safety analytical methods and techniques to related scientific disciplines.
8. Ability to do independent research on complex systems to apply safety criteria.
9. Skill in the organization, analysis, interpretation, and evaluation of scientific/engineering data in the recognition and solution of safety-related engineering problems.

10. Skill in written and oral communication.
11. Ability to keep abreast of changes in scientific knowledge and engineering technology and apply new information to the solution of engineering problems.

Major Job Requirements

1. Acts as agent of the program manager for all system safety aspects of the program. Provides monthly briefings to the program management on the status of the system safety program.
2. Serves as system safety manager or safety engineering functions of major programs. (KSA 1 through 10)
3. Manages activities that review and evaluate information related to types and location of hazards. (KSA 1,2,3,4,6,8)
4. Manages activities to perform extensive engineering studies to determine hazard levels and to propose solutions. (KSA 1,2,5,6,7,8,10)
5. Manages the development of system guidelines and techniques for new/developing systems and emerging technologies. (KSA 5,6,7,8,9)
6. Provides system safety engineering expertise to identify/solve multidisciplinary problems involving state-of-the-art technology. (KSA 10)

CHAPTER 14

FACILITIES SYSTEM SAFETY

14.1 Facility System Safety Process. (15:C-56)

The facility design system safety process concentrates Army Corps of Engineer (USACE) and user resources on identification and control of hazards in the criteria development and early design stages of the military construction process. Further, the program is structured to emphasize hazards that are not already adequately covered by codes and standards. This design effort examines the specifics of the hazards involved, the level of risk, and the appropriate control means. The process is intended to vary from project to project in scope and complexity. In other words, the system safety requirements must be tailored to a specific project and the effort expended should be commensurate with the degree of risk involved. This is accomplished through a facility risk assessment process during the project's programming stage.

14.2 Facility Life-Cycle Phases. (33:27)

In the development of DOD facilities, special life cycle phases have been defined. The development of facilities under the direction of the Army Corps of Engineers has two concept phases, a Programming and Requirement Development Phase in which the installation that will use the facility does their planning and the Concept Design Phase, which is the US Army Corps of Engineers (USACE) activity. There is no Validation Phase as such in facilities development, and the Final Design Phase is akin to the EMD Phase. This is followed by a Construction Phase (Production) and a Use and Operations Phase, which is similar to the Development portion of the usual Production/Deployment Phase, with the added point that the user has an acceptance inspection.

These specialized facility acquisition phases dictate specialized system safety activities. Wherein a major portion of the system safety analyses are focused on the EMD Phase in a regular life cycle procurement, in the acquisition of a facility much of the system safety functions are in the Concept Design and in the Construction Phase. Because many of the military facilities are built to standards rather than to detailed, original designs, much of facility system safety has to do with interfaces and with Change Orders. (33:27)

14.3 Preliminary Hazard List (PHL). (11:163-164)

The first of these tasks and the key to the success of this system safety effort is the development of a PHL early in the project development phase of a program. This PHL is developed by the user of the facility and forwarded along with the documentation to obtain funding for design and construction of the facility. This places the first safety effort in the initial stage of project.

This PHL effort serves several important functions. It provides the user with an early vehicle for identifying safety and health concerns. It is the initial assessment of the inherent hazards in a facility and classifies the facility in terms of low, medium, or high risk. Once this determination is made, the scope of the safety effort for the rest of the design and construction can be determined.

By requiring the PHL to accompany the funding documentation, funding for system safety tasks becomes as 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. This will identify areas of concern that are of special interest to the user because of safety implications. Areas that need special safety emphasis (i.e., hazards 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.

The PHL also generates an initial list of hazards which is used to start a Hazard Tracking Log. Safety hazards are identified in the PHL and entered in the hazard tracking system. At this point in time, all the hazards will be "open." New hazards are identified throughout the design process and entered in the log. As the design progresses, corrective actions are included and hazards are eliminated or controlled. The status of these hazards is updated. Hazards remaining open will continue to be tracked throughout the design process.

Hazards may be closed in one of three ways. Hazards eliminated or controlled by design are simply "closed." Hazards that are to be controlled by procedures or a combination of design and procedures are closed but annotated to ensure SOPs are developed to reduce the hazard. A list of SOPs to be developed is generated and turned over to the user. Hazards that are to be accepted as is, or with partial controls, are closed and risk acceptance documentation is prepared. Using this process, by the end of final design, all hazards will be closed, with any additional actions required highlighted. Thus, the Hazard Tracking Log serves to document the status of hazards throughout the facility.

14.4 Facility Risk Categories. (15:C-57)

After completion of the initial PHL, categorization of the planned facility into one of three general risk categories is accomplished. This categorization is based on several factors, such as number of people exposed, type and degree of inherent hazard of operation, criticality of the facility to defense readiness, vulnerability, and cost. Questions must be asked relative to whether the facility is "one of a kind" or a standard design and how it impacts (e.g., weapon facility) on the rest of the installation. This designation should directly

reflect the local concern for operational safety and health risks presented by the facility and its mission. The three general risk categories and typical system safety levels of effort are:

a. Low-risk facilities; i.e., housing, warehouses, and administrative buildings. In these types of facilities, risks to building occupants are low and limited normally to those associated with everyday life. Accident experience with similar structures is acceptable, and no additional hazards (e.g., flammable liquids, toxic materials, etc.) are to be introduced by the building occupant. Except in special cases, no further system safety hazard analysis is necessary.
b. Medium-risk facilities; i.e., maintenance facilities, heating plants, photographic laboratories. This grouping of facilities generally presents industrial-type hazards to the building occupants. Accidents are generally more frequent and potentially move severe. A preliminary hazard analysis (PHA) may be required of the designer.
c. High-risk facilities; i.e., high-energy-related facilities, explosive plants, chemical agent facilities, etc. This category 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 prepare the PHA in addition to the PHL. Additional hazard analyses (e.g., operating and support hazard analyses may be required of the designer).

The importance of the PHL and risk categorization cannot be overemphasized as their outputs establish the basis for the project system safety management plan.

14.5 Facility System Safety Working Group (SSWG). (11:164-165)

The SSWG is responsible for preparation of the PHL. Initially, the SSWG consists of representatives of the user of the facility, facility engineer personnel, installation safety personnel, installation medical personnel, and installation fire personnel. As the project evolves, the makeup of the team may change to incorporate appropriate personnel. The responsible district of the Corps of Engineers provides representation to the SSWG during design and construction of the facility. Other members with specialized expertise may be included if the type of facility so dictates.

The SSWG oversees the system safety effort throughout the facility life cycle. The first task the SSWG performs is the preparation of the PHL and a PHA, if required. The Corps District then uses these documents and the recommendations of the SSWG to write the scope of work for additional safety efforts during design. The SSWG will then assist in monitoring the system safety effort to ensure it is commensurate with the level of effort planned. Tasks included in this effort may include review of analysis, design review, review of risk acceptance documentation, constructive site reviews, and participation in occupancy inspection to ensure safety measures are designed into the facility.

If the PHL indicates that the facility is a “low-risk” building and no further analysis is necessary, a list of applicable safety standards and codes will be generated. In this case, the only other task for the team will be participation in design reviews.

14.6 Preliminary Hazard Analysis (PHA). (11:163)

If the facility is a “medium” or “high” risk, the next analysis performed will be a PHA. The PHA is an expansion of the PHL. The PHA expands the PHL in three ways. Additional details on the corrective action to be taken is provided. The level of detail of hazards already identified is increased. A more detailed analysis to identify additional hazards is performed. The PHA will then be used to determine the system safety effort for the rest of the project.

The PHA can be performed either in-house or by a contractor. If done in-house, the system safety engineer, with the help of the SSWG, will perform the PHA. This would normally be done on a medium-risk facility where the detailed functional specifications are being prepared in-house and the installation involved has the resources and expertise to perform the analysis.

The PHA is based on Task 202 (DOD Deskbook). As an expanded version of the PHL, the PHA contains greater detail in three areas. First, hazard control information is added to identified hazards. Second, a more comprehensive and systematic analysis to identify additional hazards is performed. Third, greater detail on hazards previously identified in the PHL is provided. Detailed knowledge of all operations to be conducted within the facility and any hazards presented by nearby operations is required. Based on the best available data, including lessons learned, hazards associated with the proposed facility design or functions shall be evaluated for hazard severity, hazard probability, and operational constraints.

14.7 System Safety Management Plan (SSMP). (15:C-58)

The SSMP is a document prepared by the USACE district and becomes the road map for the project’s system safety effort. This plan tailors the system safety program requirements of the government to the specific project. The SSMP establishes management policies and responsibilities for the execution of the system safety effort. The SSMP should be written so design system safety tasks and activity outputs contribute to timely project decisions. Evaluation of system safety project progress will be in accordance with the SSMP. The minimum elements of the SSMP are as follows:

a. Establishment of 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.
b. A specific listing of all tasks, including hazard analyses, which are a part of the design system safety effort; designation of the responsible parties for each task. Optional tasks should be designated as such, listing the conditions which would initiate these tasks.

c. Establishment of a system safety milestone schedule, keeping in mind that the purpose of the hazard analysis is to beneficially impact the design and that, therefore, early completion of these analyses is vital. The schedule for analysis completion must complement the overall design effort.

d. Establishment of procedures for hazard tracking and for obtaining and documenting residual risk acceptance decisions.
e. Outline of procedures for documenting and submitting significant safety data as lessons learned.
f. Establishment of procedures for evaluating proposed design changes for safety impact during the later stages of design or during construction after other safety analysis is complete.
g. Establishment of a communication system that will provide timely equipment requirements and hazard data to the facility design. This is necessary when equipment to be installed or utilized within the facility is being developed or procured separately from the facility.

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 additional guidance for deciding which ones to select. Therefore, design system safety tasks (adapted from the DOD Deskbook) must be tailored to facilities acquisition.

14.8 Design Phase. (11:166)

Once the project reaches this phase, performance of safety tasks will be turned over to the designer. The tasks to be performed during design are dependent upon the decisions made by the SSWG based on the PHL/PHA and specified in the contract. If the cost of the facility and the degree of hazard or mission criticality justify their use, the analysis types that may be performed include fault tree analysis, failure mode and effects analysis, and operating and support hazard analysis.

Besides monitoring hazard analyses, there are several actions the SSWG will be performing during the design process. They will be participating in design reviews. They will review designs to ensure that corrective actions identified in analyses are incorporated in the actual design. They will review and accept risk based upon the documentation provided.

Final design phase tasks will be similar to the concept design phase. The SSPP is updated to reflect any changes necessary. Necessary hazard analyses are performed or updated to reflect the more detailed design.

14.9 Construction Phase. (11:166)

During the construction phase, two activities 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 District may be made for one or two site visits to check on the progress of the facility.

The final step before the user takes over control of the facility is the occupancy inspection. This inspection will verify the presence of critical safety features incorporated into the design. At this point in time, the hazard tracking system is very important. Review of the tracking system will identify safety features that should be looked at during this inspection. The Hazard Tracking Log will generate a checklist for safety items that should be part of this inspection.

After successful completion of the occupancy inspection, the Hazard Tracking Log, other system safety documentation, and responsibility for the ongoing system safety effort are turned over to the user. A benefit of having user participation in the system safety effort throughout the design and construction process is the additional historical safety background the user will have.

The occupancy inspection also serves as a measure of the effectiveness of the system safety program. Any hazards discovered during the inspection will fall into one of two categories. A hazard that was previously identified and the corrective action to be taken to control the determined. Or a hazard that was not previously identified. Items falling in this second category can be used to measure the effectiveness of the system safety program for a particular facility. If many new hazards are identified after construction, the system safety effort failed to design a desired level of safety into the facility and fell short of its goal.

14.10 Facilities Safety Analysis (PHA) Example. (11:166)

The preparation of facility safety analyses is normally the responsibility of industrial/occupational/plant safety. However, the system safety and occupational safety disciplines complement each other in their respective spheres of influence and often work together to provide a coordinated safety program and accomplish safety tasks of mutual interest. Due to the extreme high cost of today's hardware, especially space hardware, and the many accidents and incidents that involve this hardware before it is ever delivered to the customer, the SPO/MAs are requesting system safety, as part of the contract, to perform facility safety analyses to ensure their high-ticket items are protected during the manufacturing/assembly process.

The clear message here is the Air Force has become increasingly aware that the safety effort not only involves system safety performance during the initial design development phase but also extends to the contractor's manufacturing capability and the measures taken to protect valuable hardware from damage or total loss. Figure 14-1, Facility Safety Analysis, is a typical example of this type of analysis.

14.13 MIL-STD-882 Guidance. (30:B-7)

As part of the continuing system safety program for facilities, the system safety tasks for this phase will include the following:

a. Ensure the application of all relevant building safety codes, including OSHA, National Fire Protection Association, and US Army Corps of Engineers safety requirements.
b. Conduct hazard analyses to determine safety requirements at all interfaces between the facility and those systems planned for installation.

c. Review equipment installation, operation, and maintenance plans to make sure all design and procedural safety requirements have been met.
d. Continue the updating of the hazard correction tracking begun during the design phases.
e. Evaluate mishaps or other losses to determine if they were the result of safety deficiencies or oversight.
f. Update hazard analyses to identify any new hazards that may result from change orders.

Figure 14-2

APPLICATION MATRIX FOR FACILITIES ACQUISITION

TASK	TITLE	TASK TYPE	P & R DEV	CON DES	FIN DES	CON
101	SYSTEM SAFETY PROGRAM	MGT	G	G	G	G
102	SYSTEM SAFETY PROGRAM PLAN	MGT	S	G	G	G
103	INTEGRATION OF ASSOCIATE CONTRACTORS, SUBCONTRACTORS AND AE FIRMS	MGT	S	S	S	S
104	SYSTEM SAFETY PROGRAM REVIEW/AUDITS	MGT	G	G	G	G
105	SSG/SSWG SUPPORT	MGT	G	G	G	G
106	HAZARD TRACKING AND RISK RESOLUTION	MGT	S	G	G	G
107	SYSTEM SAFETY PROGRESS SUMMARY	MGT	S	S	S	S
201	PRELIMINARY HAZARD LIST	ENG	G	N/A	N/A	S
202	PRELIMINARY HAZARD ANALYSIS	ENG	G	S	N/A	GC
203	REQUIREMENTS HAZARD ANALYSIS	ENG	G	S	S	GC
204	SUBSYSTEM HAZARD ANALYSIS	ENG	N/A	S	G	GC
205	SYSTEM HAZARD ANALYSIS	ENG	N/A	G	G	GC
206	OPERATING & SUPPORT HAZARD ANALYSIS	ENG	S	G	G	GC
207	HEALTH HAZARD ANALYSIS	ENG	G	S	N/A	N/A
301	SAFETY ASSESSMENT	MGT	N/A	S	G	S
302	TEST AND EVALUATION SAFETY	MGT	G	G	G	G
303	SAFETY REVIEW OF ECPS & WAIVERS	MGT	S	S	S	S
401	SAFETY VERIFICATION	ENG	N/A	S	S	S
402	SAFETY COMPLIANCE ASSESSMENT	MGT	N/A	S	S	S
403	EXPLOSIVES HAZARD CLASSIFICATION/ CHARACTERISTICS	ENG	N/A	S	S	S

NOTES

TASK TYPE

ENG - System Safety Eng
MGT - System Safety Mgt

PROGRAM PHASE

P & R DEV - Programming and requirements development
CON DES - Concept Design
FIN DES - Final Design
CON - Construction

APPLICABILITY CODES

S - Selectively Applicable
G - Generally Applicable
GC - General Applicable to Design Changes Only
N/A - Not applicable

Figure 14-1

FACILITY SAFETY ANALYSIS

ITEM/FUNCTION	PHASE	CONCERNS/HAZARD SOURCES	SAFETY FEATURES AND/OR MITIGATING CIRCUMSTANCES	CORRECTIVE ACTION OPEN/CLOSED
Cranes (2) 1000 lb (top of paint booth frame)	lifting	Loads exceed crane hoist capability	Each crane hoist block has its rated capacity painted on both of its sides in figures readable from the floor or ground level (Ref. Safety Manual, Sect 17.1)	Closed 1000 lb cranes will not be used to lift subject hardware
(1) 10,000 lb bridge (crane in front of paint booths)	lifting	Crane fails to carry load	All bridge cranes are proofload tested every 4 years, and have proofload tags attached to hoist grip denoting proofload date, capacity and next due date. (Ref. Safety Manual, Sect 17.4.2)	Closed. (hardware to be lifted weighs less than 5000 lbs)
	lifting	Loss of control caused by operator error	All crane operators are qualified and authorized by supervision. Cranes are equipped with braking devices capable of stopping a weight 1.25 times the rated maximum load. (Ref. Safety Manual, Sect 17.1)	Closed.
High pressure 100 lb Compressed Air Lines	All Ops	Pressure lines not properly identified	Facility Review encountered lines/sources not identified in paint booth (Ref. Safety Manual, Sect 28.3 all piping shall be color coded to ANSI A.13.1 Standards)	Closed. Lines identified and direction of flow added 4/10/89
Facility Access	All	Injury to personnel due to emergency pathways blocked with dollies, cabinets, and other stored hardware	Reference, Safety Manual, Sect 10.4, “Fire equipment, aisles, and exits shall be kept free of obstructions.”	Closed. Area manager has instructed his people to keep access pathways clear of obstructions
Emergency Doors	During Evacuation	Doors not labeled as exit doors	Access doors have been labeled	Closed.
	During Evacuation	Area around doors not marked to keep clear	Areas around door opening marked with bold striped lines	Closed
Housekeeping	All	Trash/congestion in area	area manager has cleaned up area and instructed his personnel to keep it that way. (Ref. Safety Manual, Sect 12.1.4)	Closed. Surveillance control checklist initiated to keep area clear of trash.
Electrical 110 Volts AC 240 Volts AC 480 Volts AC 600 Volts AC 20 Amp 125 VAC 100 Amp 250 VAC	Painting Payload/ All operations	Loss of electrical power Use of nonhazard proof electrical equipment	No hazards associated with loss of electrical power have been identified. No electronic equipment is installed on hardware to be painted. In emergencies, power kill switches are located on back side (NE corner) of paint booth	Closed. Closed.
Electrical Grounds	All	Lack of ground in NE corner of building	Ref. Safety Manual, Sect 6.1.2, “Electrical Equipment shall be grounded in accordance with article 250, National Electrical Code NFPA #70.	Closed. Paint booths are properly grounded

CHAPTER 15

SUPPLEMENTARY REQUIREMENTS

15.1 Acceptable/Unacceptable Risk.

The program office can specify additional specific safety requirements in the contract: Unacceptable Conditions. The following safety-critical conditions are considered unacceptable. Positive action and implementation verification are required to reduce the risk to an acceptable level as negotiated by the contracting and the purchasing office.

a. Single component failure, human error, or design features which could cause a mishap.
b. Dual independent component failures, dual human errors, or a combination of a component failure and a human error involving safety-critical command and control functions.
c. Generation of hazardous ionizing/non-ionizing radiation or energy when no provisions have been made to protect personnel or sensitive subsystems from damage or adverse effects.
d. Packaging or handling procedures and characteristics which could cause a mishap for which no controls have been provided to protect personnel or sensitive equipment.
e. Hazard level categories that are specified as unacceptable in the contract.

Acceptable Conditions. The following approaches are considered acceptable for correcting unacceptable conditions and will require no further analysis once controlling actions are implemented and verified.

a. A system design which requires two or more human errors or which requires two or more independent failures or a combination of independent failures and human error to result in a mishap that does not involve safety-critical command and control functions which could cause system loss.
b. System designs that require at least three independent failures, or three human errors, or a combination of three independent failures and human errors for safety-critical command and control functions.
c. System designs which positively prevent errors in assembly, installation, or connections which could result in a mishap.
d. System designs which positively prevent damage propagation from one component to another or prevent sufficient energy propagation to cause a mishap.
e. System design limitations on operation, interaction, or sequencing which preclude occurrence of a mishap.
f. System designs that provide an approved safety factor or fixed design allowance which minimizes possibility of structural failure or release of energy sufficient to cause a mishap.
g. System designs that control energy buildup which could potentially cause a mishap (fuses, relief valves, electrical explosion-proofing, etc.).
h. System designs in which component failure can be temporarily tolerated because of residual strength or alternate operating paths so that operations can continue with a reduced but acceptable safety margin.
i. System designs which positively alert the controlling personnel to a hazardous situation for which the capability for operator reaction has been provided.
j. System designs which minimize/control the use of flammable materials.

15.2 Industrial Safety. (37:Chapter 14)

Program Activity. Industrial safety activities are designed to protect the workers in the industrial environment. There are extensive standards imposed by the federal codes of regulations which provide for a safe workplace. Few, if any, of these apply to protection of a product being manufactured. The contractor system safety program is designed so that it supplements industrial safety activities to protect government equipment and property being used or manufactured under contract. Use of contractor-owned or leased equipment is also subject to review. Figure 15-1 compares the concerns of system safety versus industrial safety.

When contractor-owned or leased equipment is being used in manufacturing, testing, or handling products being produced under contract, the system safety effort is required to analyze such equipment and require operational proof tests. This is done to show that risk of damage to the product has been minimized with proper design, maintenance, and operating procedures and to assure the equipment is operated by qualified personnel. It is not intended that the contracted system safety effort get involved with the implementation of the requirements of the Federal Occupational Safety and Health Administration, Department of Transportation, or Environmental Protection Agency. The contractor is required by law to implement these regulations. The contracted system safety effort is concerned only to the extent that these regulations affect the operation of the system being built and that risk of damage to government equipment and the product being developed has been minimized.

Figure 15-1

SYSTEM SAFETY VS INDUSTRIAL SAFETY (53:14-4 to 14-10)

GENERAL CONCERNS

SYSTEM SAFETY	INDUSTRIAL SAFETY
Safety of Product	Safety/Health of
Design	Contractor employees and other persons exposed to hazards of contractor operations
Test	
Operation, Maintenance, Servicing (OM&S)	Contractor Property
Assembly/Installation, & Checkout	GFP in Contractor Custody
Modification	Work Environment
Disposal	General Environment

OPERATIONS

SYSTEM SAFETY	INDUSTRIAL SAFETY
Assure that all operations on or with the deliverable product elements can be performed legally and safely by both customer and contractor personnel.	Assure that all potentially hazardous operations to be performed by contractor personnel are identified properly controlled under normal conditions, that necessary backout/ emergency response capability specified by system safety is provided and in place for rapid use.
Assure that all potentially hazardous operations are identified and that all concerned are notified of the potential risks and operating constraints. Develop appropriate backout/emergency responses for such operations.	Assure that all normal contractor operations satisfy regulatory requirements for employee safety and health.
Assure industrial safety personnel are aware of system hazards which can be dangerous and of design controls over mishap risk.	Assure system safety personnel are made aware of problems that occur during operations that present a threat to operating personnel.

EQUIPMENT

SYSTEM SAFETY	INDUSTRIAL SAFETY
Assure deliverable equipment is designed to meet specified safety requirements for use as part of the total system and operational support such as maintenance and safety equipment.	Assure that production/transportation and handling (T&H) personnel are aware of and use proper procedures for control of hazardous characteristics and/or hazardous materials in deliverable equipment.
Assure test support equipment/ test article/Assembly/Installation & Checkout (A/I&CO). T&H support equipment is designed to meet specified safety requirements to protect test personnel, test facilities, and other system/test equipment and environment.	Assure tooling meets and remains in compliance with regulatory requirements for protection of personnel.-
Assure tooling design will not allow or cause degradation of safety designed into deliverables.	Assure contractor- and government-furnished equipment is properly maintained, proofloaded, tested, and certified.
Identify requirements for contractor's T&H equipment to prevent undetected degradation of safety designed into deliverables (e.g., prevention of overstressing, structural damage from environmental conditions, etc.)	Identify requirements for personnel protective equipment in the production operations environment.
Identify requirements for special equipment to protect personnel from possible product defects.	Assure that contractor- and government- furnished production and processing equipment satisfies regulatory requirements for safety of personnel. --
Identify hazardous characteristics of, and hazardous materials in, deliverable or test assembly & checkout support equipment which includes explosives, flammables, corrosives, and toxics.	Assure that government-furnished equipment (GFE) in contractor custody is protected from damage due to contractor operations.
Provide information to industrial safety personnel on protection needs for sensitive equipment.	Feed back information to system safety personnel on better ways to protect sensitive equipment.

Figure 15-1 (cont.)

FACILITIES

SYSTEM SAFETY	INDUSTRIAL SAFETY
Assure that new facilities used as a part of, or in customer support of, the system are designed to meet specified safety requirements to properly protect system equipment and personnel.	Assure that contractor- and government-furnished facilities used to produce (e.g., fabricate, assemble, process, functionally test, etc.) or store materials, assemblies or deliverable items meet, and remain in compliance with requirements for the protection of personnel, property and the environment.
Assure that existing facilities used to house, test, maintain, or store system equipment contain safety features/provisions necessary to such equipment and personnel.	

PROCEDURES

SYSTEM SAFETY	INDUSTRIAL SAFETY
Assure procedures for user-performed operations contain appropriate Requirements/Warnings/Cautions and sequencing constraints to protect personnel, equipment, property, and outside environment.	Assure that procedures, instructions, and planning for production, functional test, storage, and T&H operations provide for the safety of contractor personnel and property GFP in the contractor's custody and the environment.
Assure procedures for contractor servicing performed operations on deliverable system elements contain appropriate Requirements/ Warnings/Cautions and out-sequencing constraints to protect the deliverables.	Assure that operating personnel are aware of the dangers involved with the conduct of the procedure. Assure that warnings and caution notes listed in the procedures are followed.
Assure procedures/instructions/ planning for production and functional test will minimize and detect safety-critical faults in, or damage to, deliverable products.	

PERSONNEL

SYSTEM SAFETY	INDUSTRIAL SAFETY
Identify personnel contributions to potential mishaps associated with the deliverable product during production Operations & Maintenance (O&M), test, or A/I&CO activities, and specify personnel qualifications and training needed to control/minimize such contributions.	Identify special training/certification requirements to qualify personnel to perform safety-critical production and T&H operations. Feed back to system safety personnel. Provide surveillance of contractor actions during operations to identify and initiate corrective action for unsafe practices.
Assure industrial safety personnel are aware of system characteristics which may present a danger to operating personnel.	Assure that system safety personnel are informed of areas which need further design corrective action.

CHANGES / UNPLANNED EVENTS / MISHAPS

SYSTEM SAFETY	INDUSTRIAL SAFETY
Assess impact on safety of the system of all design/procedure/ operations planning changes and all unplanned events, and assure safety of design is not degraded.	Assess impact on safety of contractor personnel/facilities and the environment of changes to, or unplanned events involving, production/T&H operations.
Evaluate results of mishap/potential mishap investigations to identify need for safety changes to deliverable product designs or procedures operations involving deliverables.	Evaluate results of mishap/potential mishap investigations to identify need for safety changes to designs of facilities and equipment, processes and equipment, and qualifications and training of personnel involved with production/T&H operations.
Provide information to industrial safety personnel on specific design features which will protect operating personnel.	Feed back information to system safety personnel on specific design improvements which can better control mishap risk.

The system safety activity is conducted to complement the industrial safety activities by addressing occupational safety and health needs in system design analysis and manufacturing planning. Often the interface between the two safety functions is not covered or is insufficient. This may leave gaps in the overall mishap prevention program. For example, in one case, a satellite was being assembled and checked out in a controlled area; however, during the night, the plastic cover on a mercury-vapor light melted and the hot plastic, which dripped on some papers that were left on a wooden bench, started a fire. Before the fire was detected, most of the support and checkout equipment was badly damaged. Also, the dense smoke caused extensive damage and contamination to solar cells and other sensitive equipment. When the system safety manager was asked what his analysis had indicated in this area, he said, "We didn't look at that. That's industrial safety." When the industrial safety manager was asked when last he looked into the area, he responded, "They were testing a satellite in there. That is system safety's job." Further investigation showed that the system safety analysis had considered this problem and recommended metal benches be used. However, this analysis was not made available to the industrial safety people, and no follow-up action had been taken on the recommendation. While this is an example of bad management, by both system and industrial safety, this attitude is far too prevalent to be ignored. Methods must be developed within each program which allow system and industrial safety engineers to adapt to each others needs.

During early program planning, a cooperative industrial safety effort is needed to write the system safety program plan (SSPP) so that it includes industrial safety operations. An agreement must be reached on how to separate those functional elements which are required by contract and those required by law. This should be done carefully to avoid payment for contractual tasks which also are paid for as overhead. This separation must take place without loss of the cooperative effort necessary to take full advantage of the methods and talents that are available in both functions.

MIL-STD-882 provides an option for the contractor to conduct the system safety program so that it complements existing industrial safety activities to assure protection of government equipment and property. To accomplish the task, the contractor has to know the concerns and requirements of each function. Once this is understood, it becomes obvious where the overlapping concerns are. Then, agreements can be reached on which functional element will deal with the overlap. A description of how these areas are to be addressed is then included in the SSPP. Joint analyses and risk assessments are performed and should be included in the Mishap Risk Assessment Report.

Figure 15-2

INDUSTRIAL SAFETY PROBLEMS/PROBLEM AREAS

1. Compliance with federal, state, and local industrial codes and regulations.
2. Required state inspections of equipment, such as boilers, cranes, elevators, degreasers, fire systems, etc.
3. Fire prevention and control program.
4. Personnel accident prevention program and statistical records.
5. Temperature and humidity control.
6. Noise level control within the plant.
7. Personal protective clothing requirements, i.e. safety glasses/shoes, hard hats, nonstatic work clothes, etc.
8. Safe and adequate tools for the job to be done.
9. Safety guards for moving parts of machinery, such as pulleys, gears, saws, grinders, conveyors, etc.
10. Material handling and storage methods.
11. In-plant cleanliness and good housekeeping practices.
12. Motor vehicle safety program.
13. Adequate lighting for type of work.
14. Warning alarms and signs.
15. Employee safety training.
16. Personal hygiene and first aid programs.
17. Proof testing and identification of lifting sling, ropes, etc.
18. Security control of identified hazardous areas.
19. Guard rails on platforms, stairs, walkways.
20. Personnel protection during hazardous testing.

SYSTEM SAFETY PROBLEMS/PROBLEM AREAS

1. Manage and implement the product system safety program plan.
2. Identification of hazards associated with the system or desired product.
3. Incorporate safety into the product design, operation, test, and maintenance.
4. Evaluation of identified hazards and design action to eliminate or minimize and control the hazards.
5. Develop safety design criteria to be incorporated into the product design.
6. Conduct hazard analyses on the product being developed.
7. Maintain product safety records.
8. Identify hazardous characteristics of hazardous materials and energy sources, including explosives, flammables, corrosives, toxics, and methods of control and disposal.
9. Assure that all operations on or with the deliverable product elements can be

15.3 Biomedical Safety. (37:Chapter 10)

The law of the land, executive order, and Air Force policy require that each employee be provided employment and that the employment place be safe, healthful, free from recognized hazards, that environmental pollution from weapon systems, operations and other activities be controlled. This cannot be accomplished with passive avoidance of hazards but requires an aggressive effort beginning with the acquisition of all systems and continuing through the establishment of health and safety programs.

The term biomedical, as used in the Air Force and in this manual, refers to physical and chemical agents which impact on the health and well being of humans. Chemical agents, which may have a negative effect on man, may be hazardous because of their toxic, corrosive, flammable, or reactive nature. Physical agents include all forms of sound and vibration, all forms of electromagnetic radiation, and all forms of particle radiation. The recognition, evaluation, and recommendations for control of biomedical hazards are the responsibility of bioenvironmental engineering.

Not all chemicals are hazardous, not all radiation is harmful. As Alice Ottoboni says, "The dose makes the poison." All but about 20 of the 92 natural elements are essential to life, yet excessive amounts of any one of them will be toxic. Sound and electromagnetic radiation in the proper amounts and frequencies are pleasing to the ear and eye, or in other amounts and frequencies can be discordant and unpleasant or downright harmful. Being smart is knowing when to seek help to evaluate potential hazards from chemical and physical agents.

Each program officer and project officer is required to ensure that potential biomedical problems are considered at the earliest appropriate time in the acquisition cycle. This requires two decisions of the program officers and project officers: (1) is a chemical or physical agent a potential biomedical problem?, and (2) when is the earliest appropriate time in the acquisition cycle to address potential biomedical hazards?

While the statement of work is being written is the appropriate time to consider what biomedical input will be required. The necessary biomedical input, reflecting the hazard potential, will vary widely from program to program. For example, a software study involving no physical hardware may require no biomedical input because there are no physical or chemical agents involved. Whereas each statement of work for a major hardware system to be utilized at an Air Force installation may require the generation of an entire annex which documents both known and potential biomedical hazards, the development of new criteria for hazards for which there are no consensus standards, and new formulation of a plan for mitigating the effects through process change, engineering and procedural controls, and personnel protective equipment, etc.

Some systems are so large and complex that environmental impacts, on both the working environment within the system and on the community around the system, cannot be foreseen. The development of the biomedical data becomes a major tasks and has a major impact on the development of the system. To avoid running up blind alleys, the biomedical data must be made available early in the program to people specifying and defining the system. There are many examples to choose from to illustrate this point.

In the early days of propulsion system development, the emphasis was on maximizing specific impulse. A quick look at the periodic table of the elements reveals that the maximum specific impulse can be obtained by burning hydrogen with fluorine. When the system was built and test fired, the hydrogen fluoride generated in the rocket exhaust was so toxic and corrosive that this propellant combination cannot be used on terrestrial systems. Had timely biomedical data been provided, the system would never have left the drawing board.

Reporting. The reporting and documentation of biomedical hazards is easy and straightforward when the hazards are "routine," such as the fuels and oxidizers that are in the inventory and that are used in an ordinary way. However, when the state of the art is advanced in materials, bonding agents, familiar chemicals used in novel ways, new applications of radiant energy, etc., it is time to seek assistance from bioenvironmental engineering to determine what biomedical data are required and to interpret the information supplied. Reporting of data can be achieved using Task 207, Health Hazard Assessment (DOD Deskbook).

Evaluations. Bioenvironmental engineers trained in industrial hygiene and environmental engineering can draw upon the resources of the Air Force Occupational and Environmental Health Laboratory and other information resources, that reach throughout the United States and the world, to assist in the identification, evaluation, and control of biomedical hazards. This vast network of resources has yielded timely and cost-effective solutions to problems such as real-time monitoring in the parts per billion and trillion range, exhaust cloud modeling, laser footprint prediction, and sonic boom measurements. Air Force policy is that no hazard is too great to be controlled. However, time, money, and mission constraints must be balanced, and this is where the professional expertise of the bioenvironmental engineers, when applied early in the acquisition cycle, pays big dividends to system acquisition.

Highest priority should be given to controlling medical hazards with engineering controls. This is often practical only when identification of the biomedical hazard is made early in the system definition.

15.4 Operational Safety.

In the first 14 chapters of this handbook, we discussed system safety in the classical sense—from the perspective of the design process. MIL-STD-882 is written primarily from that perspective, emphasizing the system safety process during acquisition. We could refine the definition of system safety from that viewpoint: the application of engineering and management effort to ensure that the system is designed so that it is inherently safe to operate, maintain and dispose of. In Chapter 18, we discuss system safety in logistics, or as it pertains to the support of the system during the operational phase of its life cycle. Here, system safety could take on a slightly different definition: the application of engineering and management effort to ensure that inherent design safety is maintained or improved during the later phases of the life cycle.

From either perspective, system safety is an engineering and management process related to system design and logistical support. This process, like other engineering and management processes, should be closed-loop. During each phase of the life cycle, data acquired about the system is fed back to people who are responsible for using the data to iterate the design process or improve the logistics process (reference Figure 2-2). The sources of data include testing and field experience (service reporting, materiel deficiency reporting, reliability and maintainability experience, etc.). Ideally, this data is also shared between programs (crossfeed or feed forward). Formally this can be done through documentation in the Air Force Lessons Learned database, Design Handbooks, or Military Prime Specifications.

Informally, raw data about similar systems and common problems should also be shared by engineers working on different systems. Program office personnel should be familiar, in general, with most aspects of this feedback/feed forward process and associated databases since they are covered by AFMC directives and are inherent in day-to-day operations in acquisition and logistics.

Once the first system unit representing the result of the design process is delivered for testing, the test agency assumes a share of the responsibility for safety. When the system becomes fully operational, the operating command assumes that responsibility. In either of these cases, those aspects of the overall safety program involving actual system use can be called operational safety. Operational safety programs are broad in scope and are tied to system safety in many ways, including conduct of operational safety reviews and participation in system safety groups. Communication between systems and operational safety programs is important, and crossfeed of data and lessons learned between the two is essential.

This section covers one aspect of operational safety—mishap investigation. If in the course of testing or operations a mishap occurs, the organization with responsibility for operational safety must investigate to determine the cause(s) of the mishap and make recommendations on how to prevent future mishaps due to those causes. The results of such investigations often include information related to system design and support. These results can provide very important inputs to the overall feedback/feedforward process for system safety, so it is important for the system safety manager to have a basic understanding of the process.

The primary regulation that governs this process is AFI 91-204, Investigating and Reporting USAF Mishaps, which implements DODIs 6055.7 and 7730.12. As the title suggests, this regulation establishes the program for investigating and reporting all USAF mishaps. It includes policies and responsibilities, mishap definitions and classification, the conduct of safety investigations, and reporting procedures. It also includes information on restrictions pertaining to the release and dissemination of information about mishaps.

Mishap categories include aircraft mishaps (flight mishaps, flight related mishaps and aircraft involvement mishaps), foreign object damage mishaps, missile mishaps, explosives mishaps, ground mishaps, nuclear mishaps and space mishaps. Mishaps are also classified by the amount of damage or injury caused, for example:

- Class A--$1,000,000/fatality or permanent total disability/ destruction of an Air Force aircraft
- Class B--$200,000/permanent partial disability/ hospitalization of five or more people
- Class C--$10,000/injury or illness resulting in lost workdays/other specific criteria based on system type
- HAP--Another term used to describe a safety concern is the high accident potential (HAP). HAPs are events which have a high potential for causing injury, occupational illness or damage if they recur. These events may or may not have reportable costs.

The actual type and extent of the investigation for a given mishap varies with the mishap category and a determination by the responsible commander (the commander of the MAJCOM that had the mishap). The sole purpose of the safety investigation is to find the causes of the mishap and prevent recurrence. The makeup of a safety investigation board (SIB) varies with the situation, and program/test organizations as well as contractor personnel may be asked to provide technical assistance. A separate accident investigation governed by AFI 51-503 is also convened for all Class A mishaps. This accident investigation preserves available evidence for claims, litigation, disciplinary and administrative actions. The accident board's report is fully releasable to the public.

Often much of the information needed by the SIB can only be provided by persons directly or indirectly associated with the mishap (pilots, controllers, maintenance, designers, manufacturers, etc.). To ensure a frank and open exchange of such information without fear of incrimination or other adverse action, several restrictions are placed on SIB reports. The most important restriction is that findings, conclusions, causes, recommendations and deliberative processes of certain category SIBs are exempt from disclosure outside of the Air Force safety community. This "government privilege" also applies to statements given to the board pursuant to a promise of confidentiality, which includes the statements of government contractors who built, designed or maintained the equipment. Such information is contained in Part II of the SIB report and is not releasable to AFI 51-503 boards, or for any type of punitive process, or as evidence in liability claims. It can only be used by the USAF safety community for mishap prevention activity. Strictly factual data, which is releasable to the public, is contained in Part I of the SIB report and is fully included in the accident investigation report.

On the positive side, the protection provided by the government privilege makes the investigative process much more effective in determining causes; on the negative side, it makes it much more cumbersome for program office personnel to gain access to information in historical SIB reports. Access can only be given through the organizational safety office, and then only to the extent necessary to advance mishap prevention. This is frequently done through the use of sanitized reports in which the relationship between the identity of the mishap and the findings, causes and recommendations has been obscured.

Findings are the board's conclusions, arranged in chronological order in the mishap sequence. Causes are those findings which, singly or in combination with others, resulted in the damage or injury. A new concept was recently implemented which analyzes all causes in a "what-who-why" manner; this leads to more clearly defined accountability, responsibility and reason for the mishap. The concept is called the CAR taxonomy (category-agent-reason) and should provide both a sharper focus on root causes and the ability to determine more precise intervention strategies.

Recommendations are those actions which will likely prevent a similar mishap in the future; they are directly related to the causes. Recommendations are assigned to responsible agencies, such as operating or supporting MAJCOMs. This is where program office personnel generally become involved in the "loop-closing" process. Recommendations frequently result in design changes or revisions to maintenance or operating procedures, and the risk assessment process described in the appendix entitled "An Approach to Risk Assessment" should be applied to ensure that new hazards are not introduced. Of course, what we learn about system design from these mishap experiences should be documented by the program office in the applicable lessons learned database; we can't afford to learn these costly lessons twice!

The Air Force Safety Center maintains a computer database covering USAF mishaps. The database includes the full narrative description of the mishap, findings, recommendations, and a host of fields which enable searches for related mishaps. These fields include (but are not limited to):

- Date/time/meteorological conditions

- Mishap Class/system identification/MAJCOM
- Associated Work Unit Codes (WUC)
- Phase of mission
- Systems tied to causes (engine, landing gear, etc.)
- Results codes (fire, explosion, structural damage, etc.)
- Accountability (operator, supervision, tech data, design deficiency, etc.)

The database can be searched to provide statistical data, “one-liner” mishap descriptions, or complete limited-use (privileged) reports. Requests for this information must come through command safety channels. Questions about the database can be addressed to HQ AFSC/SECD, Kirtland AFB NM 87117-5670, DSN 246-1448.

Proactive efforts on the part of program office engineers and system safety personnel can also help to “lead turn” the occurrence of serious mishaps. The field reliability of components identified as safety critical should be tracked to ensure their performance meets predictions. When a Class C or HAP mishap is tied to a failed component, searching for similar or related historical failures can help in making early identification of the need for design changes or changes in the logistics process. The Materiel Deficiency Report and Service Report databases can provide the data needed to highlight problem areas before a more serious mishap occurs.

CHAPTER 16

NUCLEAR SAFETY

16.1 Nuclear Safety Program. (28:65)

Program managers must consider nuclear safety an integral part of the development, test, or acquisition of all systems equipment carrying nuclear weapons or containing radioactive material. This includes nuclear weapon systems, nuclear power systems, radioactive calibration, and components which become radioactive during use. Nuclear safety must be planned in the conceptual phase, designed into components in the development phase, and continually examined throughout the test and operational phases of each device. The system safety manager may be responsible to the project manager for the application of nuclear safety, or a separate nuclear safety representative may be appointed.

The USAF nuclear safety program is designed to prevent accidental or unauthorized nuclear detonations, to minimize both the number and consequences of nuclear accidents, incidents, and deficiencies, and to provide adequate nuclear weapon system security. The goal of the program is to achieve maximum nuclear safety consistent with operational requirements by: (AFI 91-101)

a. Designing safety into systems.
b. Developing safety rules and procedures.
c. Adhering to approved procedures, standards, and safeguards.
d. Identifying, reporting, and correcting unsafe conditions.
e. Training
f. Advancing nuclear safety technology.

16.2 Responsibilities. (28:65-67)

Many organizations and activities have responsibilities supporting nuclear safety. The application of nuclear safety is the responsibility of the program manager. The system safety manager is responsible for assuring that nuclear safety requirements are integrated into a program and tracked throughout the acquisition cycle. Other functional areas also support the nuclear safety activity. Program engineers provide technical support to the project manager and system safety manager. Before a nuclear system can become operational, it must be reviewed and approved by the Nuclear Weapons System Safety Group (NWSSG). The NWSSG is chaired by the Chief, Weapons, Space and Nuclear Safety Division (HQ AFSC/SEW) and is technically supported by the Air Armament Center, Nuclear Weapons Product Support Center (AAC/WNS). The following paragraph is intended to provide an overview of Air Armament Center in support of the AF Nuclear Safety Program:

Air Armament Center/WNS

(1) Is the USAF focal point for nuclear safety technical aspects.
(2) Provides nuclear safety certifications for AFMC.
(3) Prepares technical nuclear safety analyses (TNSA) for HQ AFSC/SEW and NWSSG.
(4) Member of the NWSSG and Operational Review Board.
(5) Technical advisor to HQ AFSC/SEW and program offices.

16.3 Nuclear Safety Goals. (31:14)

The Department of Defense has established four safety standards that are the basis for nuclear weapon system design and the safety rules governing nuclear weapon system operation. These standards require that, as a minimum, the system design shall incorporate positive measures to:

a. There shall be positive measures to prevent nuclear weapons involved in accidents or incidents, or jettisoned weapons, from producing a nuclear yield.
b. There shall be positive measures to prevent DELIBERATE prearming, arming, launching, firing, or releasing of nuclear weapons, except upon execution of emergency war orders or when directed by competent authority.
c. There shall be positive measures to prevent INADVERTENT prearming, arming, launching, firing, or releasing of nuclear weapons in all normal and credible abnormal environments.
d. There shall be positive measures to ensure adequate security of nuclear weapons.

16.4 Nuclear Safety Analyses. (31:15)

The normal hazard analyses apply to nuclear weapon systems. However, because of the dire political and military consequences of an unauthorized or accidental nuclear or high explosive detonation, additional analyses are specified to demonstrate positive control of nuclear weapons in all probable environments. The following analyses, in whole or in part, are performed by the contractor on nuclear weapons programs as specified in the contract by the project manager.

a. A quantitative analysis to assure that the probability of inadvertent nuclear detonation, inadvertent programmed launch, accidental motor ignition, inadvertent enabling, or inadvertent prearm meets the numerical requirements specified in applicable nuclear safety criteria documents.
b. An unauthorized launch analysis to define the time, tools, and equipment required to accomplish certain actions leading to unauthorized launch. The results of this analysis are used by the nuclear safety evaluation agency in determining which components require additional protection, either by design or procedural means.

c. A Nuclear Safety Cross-check Analysis of software and certain firmware which directly or indirectly controls or could be modified to control critical weapon functions. This analysis, by an independent contracting agency, must determine that the final version of software or firmware is free from programming which could contribute to unauthorized, accidental, or inadvertent activation of critical system function.
d. A safety engineering analysis of all tasks in modification or test programs at operational sites. This analysis is specifically oriented towards identifying hazards to personnel and equipment in the work area and is in addition to the analysis of the safety impact of the change to the weapon system.

16.5 Nuclear Studies/Reviews. (28:68)

The above safety standards are met by accomplishing the requirements of Air Force instructions and 11N-series technical orders. Program managers are primarily concerned with AFIs 91-102, 91-103, 91-118/119, and 91-115. AFR 91-115 states the minimum safety requirements for the design and construction of nuclear weapon systems. AFI 91-102 establishes the NWSSG and Operational Review Board; describes safety studies, surveys, operational reviews, and safety rules; and specifies responsibilities for performing functions related to nuclear weapon system safety. AFI 91-103 establishes responsibility for procedures associated with nuclear weapon systems.

Nuclear Safety Studies and Reviews. A sequence of reviews, designated as safety studies or operational reviews, have been established to ensure continuing nuclear safety during the lifetime of each weapon system. AFI 91-102 establishes schedules for major safety studies or reviews. These studies or reviews are:

a. Initial Safety Study. Conducted by the NWSSG early in the development cycle of a weapon system as adequate design information becomes available. Its purpose is to identify safety deficiencies and provide guidance for any further development to enable the system to meet the safety standards. The study is usually conducted after the preliminary design review but prior to the critical design review of those subsystems directly affecting nuclear safety.
b. Preoperational Safety Study. Conducted by the NWSSG and completed 60 days before safety rules are required. (Safety rule requirements are established by the using MAJCOM). This study determines the adequacy of safety features in the weapon system design and operational procedures and provides a basis for developing safety rules.
c. Operational Safety Review. Conducted by the NWSSG in the second year after the first unit of the weapon system has become operational. It reexamines the adequacy of safety features, safety rules, and operational procedures throughout the stockpile-to-target sequence.
d. Special Safety Studies. These are special studies and reviews conducted which the Chief, Weapons, Space, and Nuclear Safety Division (HQ AFSC/SEW) deems necessary. The purpose of these activities is to evaluate:
   (1) Unsafe conditions revealed by operational experience.
   (2) Modifications, alterations, retrofits, and special tests which affect nuclear safety.
   (3) Significant changes in operational concept of stockpile-to-target sequence.
   (4) Proposed changes to an approved safety rule.
   (5) Other nuclear matters which Chief, Weapons, Space, and Nuclear Safety Division (HQ AFSC/SEW) considers significant.

16.6 Use in Space. (37:8-2 to 8-5)

Required Actions. Prior to the use of radioactive sources, systems, or devices in space, certain approvals must be obtained. Basically, the required actions are:

a. Approval by the Nuclear Regulatory Commission (NRC) of a license for the users of the radioactive material.
b. Nuclear safety launch approval by the Chief, Weapons, Space, and Nuclear Safety Division.
c. Clearance by the President for large source space nuclear power systems.
d. Approval of appropriate range safety office.
e. Approval of environmental protection committee.
f. Coordination with the program office system safety officer is required prior to submittal for approval. The responsibility for initiating the actions required to obtain these approvals rests with the project manager, in coordination with the bioenvironmental engineer, and the safety staff. AFI 91-110 delineates the responsibilities and timing of the various actions required to obtain these approvals.

License/Permit. The use and handling of most radioactive materials require an NRC byproduct, source, or special nuclear material license. In most cases, where an NRC license is not required, an Air Force Radioisotope Permit is needed (AFI 40-201). In all programs where radionuclides are to be used, including depleted uranium, the project manager will determine the necessity of an NRC license and obtain instructions on processing an NRC license or Air Force Radioisotope Permit application. AFI 90-201, Attachment 3 delineates the information and format required when processing an Air Force Radioisotope Permit application.

Safety Analysis Summary. The Chief, Weapons, Space, and Nuclear Safety Division (HQ AFSC/SEW must approve the launch of radioactive material. This approval is effected through a Safety Analysis Summary (SAS). The SAS is an accurate detailed report on the nuclear safety hazards, both existing and potential, from a worse case standpoint, of the radioactive device during the time it is in custody or under control of the Air Force. An outline which can be used for a complete SAS, as well as the shortened or modified form acceptable under certain circumstances, is contained in AFI 91-110, Attachment 3. The circumstances which allow a modified SAS are also contained in AFI 91-110.

The project manager of those programs using airborne radioisotopes has the responsibility for preparing the SAS. Normally, the SAS will be prepared by the payload contractor and submitted to the project manager for subsequent transmittal through the program office system safety manager. After reviewing and approving the SAS, it is forwarded to the Chief, Weapons, Space, and Nuclear Safety Division (HQ AFSC/SEW), who establishes the USAF nuclear safety position. The Chief, Weapons, Space, and Nuclear Safety Division will review the prepared evaluation and forward any recommendations to HQ USAF for approval. When nuclear

safety launch approval has been obtained, the project manager will be notified through the program office system safety manager. Programs involving a series of launches using the same radionuclides within the same category (AFI 91-110) may submit, after the initial submittal, only addendums showing changes to the initial safety analysis summary.

Large Source Space Nuclear Power Systems. The requirements applying to large source space nuclear power systems are contained in the National Environmental Policy Act (NEPA) and the Presidential Directive/National Security Council Memorandum Number 25 (PD/NSC-25). Basically, the sponsoring agency will prepare two reports. One, the environmental impact statement (EIS) describing the potential hazard and alternatives to the proposed mission, and two, the Safety Analysis Report (SAR), a detailed evaluation of the importance of the particular mission and the possible direct or indirect environmental effects that might be associated with it. Both the EIS and SAR are provided to the Director of the Office of Science and Technology Policy (the Director) for review. Additionally, an ad hoc Interagency Nuclear Safety Review Panel (INSRP) will evaluate the risks associated with the mission and prepare a Nuclear Safety Evaluation Report (SER). The EIS, SAR, and SER will be used by the Director to evaluate the safety implications of the flight and request the President's approval for the mission. NOTE: Large Source is defined in PD/NSC-25.

16.7 Radiological Safety. (31:16)

The contractor shall conduct safety analyses for all applications of radioactive sources, nuclear power systems, and other systems having sources of ionizing radiation. This analysis shall include a compete assessment of the accident risk in the following areas:

a. Normal mission analysis:

   (1) Transportation, handling, calibration, testing, and processing during prelaunch operations at the launch site, including use of nonflight sources.
   (2) Flight safety (launch, flight to orbit, or ballistic reentry, and random reentry).
   (3) Recovery operations at mission termination site.

b. Contingency analysis:

   (1) Operational site accident (fire, explosion, impact, rupture, dispersal, and release quantity).
   (2) Flight accident.
   (3) Abnormal reentry, recovery, or disposition.
   (4) Abort conditions.
   (5) Accident mode and characteristics.
   (6) Accident probability, normal mission, and worst case accident consequences.
   (7) Chemical toxicity and external radiation.
   (8) Conclusions.

CHAPTER 17

EXPLOSIVES SAFETY

17.1 General.

There are many variations in system safety procedures as they are applied by different organizations to a variety of systems. A common thread for many of them is Mil-STD-882. Procedures of this standard apply to a system life cycle and include five major elements: 1) System Safety Program; 2) System Safety Program Objectives; 3) System Safety Design Requirements; 4) System Safety Precedence; and, 5) Risk Assessment. In order to be effective, safety considerations must be an integral part of the system life cycle phases and adequately addressed the hazards associated with the system under development.

The explosives safety discipline (includes missile safety for discussion purposes) developed out of the need of standardizing the storage and dispersal of explosives in the United States following several major explosive mishaps that occurred between 1901 and 1926. During this 26-year period, 67 mishaps were reported and credit with killing 382 people and injuring 794. The 1926 Lake Denmark, New Jersey incident raised the ire of the public and with help from the press, forced Congress to take action. The congressional law enacted in 1928, (Title 10, USC 172) codified the permanent formation of an oversight board we know today as the Department of Defense Explosives Safety Board (DDESB). The DDESB established explosives safety standards and requirements in DOD Standard 6055.9-STD, *DOD Ammunition and Explosives Safety Standards.* The Air Force uses the publication AFMAN 91-201, *Explosives Safety Standards*, to implement the DOD level requirements and establish a major part of its explosives safety program.

17.2 Safety Program.

The Air Force explosives safety program is designed to provide criteria and actions to prevent mishaps or to mitigate the damage (loss control) when mishaps do occur. It should be noted that in applying some explosives safety criteria, specifically with regards to quantity-distance criteria (explained later), that the publication prescribes "minimum" standards. While it is a known fact that minimum standards can not preclude damage to all resources, some personnel insist that the minimum standards are impediments to maximizing capacities. In other instances, assigning a higher priority to other concerns at the sacrifice of explosives safety criteria has led to catastrophic outcomes. The most recent example of this erroneous risk assessment is the U.S. Army's mishap at Doha, Kuwait where a seemingly minor accident escalated until the combat capability of the unit was lost. For security reasons, the unit parked all of their vehicles loaded with munitions right next to each other without regard to proper quantity-distance separation. A fire began in one vehicle and failure of people and fire suppression equipment to react properly led to detonation of onboard ammunition. This initiated fires and explosions on adjacent vehicles and nearby stores of ammunition. After 12 hours of explosions and fire, the combat capability of the unit was lost. A total of 68 vehicles were lost or damaged (over $40 million in replacement costs) and 52 people were injured. While there were no deaths in the initial incident, three Explosives Ordnance Disposal technicians were killed during the clean-up operation. For the Army, there was more equipment lost during this one event than during the entire Desert Storm war. The hazards associated with explosives don't often manifest themselves, but when they do, it's too late to implement controls!

17.3 Explosive Hazards.

To have an effective safety program one must understand the hazards associated with the product. There are three main causes of damage and injury from explosions. The most common cause of damage is a blast wave or pressure wave that radiates from the explosion. Another source of damage results from projectiles or fragments of the product and from surrounding structures affected by the explosions. A third source of damage is thermal radiation derived from combustion. While blast waves impacting on a secondary object tend to produce additional projectiles they decay with distance from the explosion source. The effects of blasts are explained by the associated overpressures created from the explosions. For instance, a blast overpressure of 1.0 psi (pounds per square inch) will knock a person down; an overpressure of 3 psi will shatter a 12-inch thick concrete wall; and, an overpressure of 7 psi will overturn a railroad car. The second hazard source, fragments, and the resultant scatter of the fragments depends on the size of explosion and the failure modes for materials. Again, distance is a primary consideration where fragmentation products are concerned. The last hazard mentioned, thermal effects, is difficult to predict since size of the fireball and its duration directly effect thermal radiation. As a general rule of thumb, most fireballs reach temperatures on the order of 2400°F and their radiant energy dissipates in relationship to distance squared. The one common thread that runs through these hazards is their shared relationship to distance.

17.4 Quantity-Distance (Q-D) Principle.

The experts have formulated required separation distance for a given quantity of explosives as $D = KW^{1/3}$, where D = required distance in feet, K = a constant protection factor depending on the degree of risk assumed, and $W^{1/3}$ = cube root of the new explosives weight (NEW) in pounds. Q-D is defined as the quantity of explosives material and the distance separation relationships which provide defined types of protection. The relationships are based on the level of risk considered acceptable for each stipulated exposure. Separation distances are not absolute safe distances but are relative protective distances. We recognize that the hazards we have to protect ourselves from in our munitions products are the exact effects we want these products to inflict on our enemies. The idea is to ensure the primary hazard is not released in the wrong place and at the wrong time. Since we do not want to eliminate the hazards of munitions we

must control their characteristics and mitigate their effects should a mishap occur, where a mishap is an unplanned event. Besides controlling through Q-D applications, other means for minimizing explosives hazards include controls during manufacture, distribution and use. Controls include training and licensing of handlers, users and distributors.

17.5 Hazard Classification of Ammunition and Explosives.

One of the first steps to implement controls is to hazard classify a product specifically for transportation and storage environments. Distribution or dispersal of explosives was of particular concern and one of the oversight areas for the DDESB. It is this transportation of explosives that is of extreme concern within DOD and the Department of Transportation (DOT) when commercial routes and carriers are involved. One method of control is manifesting explosive materials from factory to final user to minimize their getting into hands of unqualified users or being improperly used. Another control area, and the second primary oversight concern, was storage. Proper storage controls include separating different compatibility grouped munitions from each other when co-mingled storage would increase risks, limiting the quantity of explosives stored at any one location or facility and insuring storage facilities meet peculiar design specifications such as fire resistance, physical security, etc.

The DOD hazard classification system is based on the system recommended for international use by the United Nations Organization. It consists of nine classes for dangerous goods. Most ammunition and explosives items are included in "Class 1, Explosives." Explosives, to be acceptable for transportation by any mode, must have an assigned hazard classification (Q-D hazard class/division; storage compatibility group; DOT class, markings, shipping name and label; and United Nations (UN) serial number). Developmental or test items without a final classification must be assigned an interim hazard classification. Procedures and authority for assigning classifications are in TO 11A-1-47, *Department of Defense Ammunition and Explosives Hazard Classification Procedures*. Final and interim hazard classifications assigned by the Army and Navy authority are acceptable to the Air Force. Commercial explosive items purchased for official use must have a hazard classification assigned in accordance with TO 11A-1-47 before transportation and use. A hazard classification is assigned for each ammunition and explosive item in the form and packaging in which it is normally stored and offered for transportation as cargo in commercial or military vehicles. These hazard classifications are listed in TO 11A-1-46, and in the DOD Joint Hazard Classification System listing.

Air Force organizations that develop, or first adopt for use, ammunition or explosive items are responsible for obtaining hazard classifications using the procedures in TO 11A-1-47. The hazard classification reflects the type and degree of hazard associated with the item and is used to determine the degree of protection (such as distance separation) needed for various exposed locations and people. When ammunition or explosive items are not in the form and packaging in which they are normally stored and shipped, different hazard classifications may apply due to changes in spacing, orientation, confinement, and other factors. Sometimes testing of unpackaged components may be required in order to demonstrate the validity of classifications used for sitting unpackaged ammunition, or conservative assumptions must be made about the potential severity of an accidental explosion. In many cases, these "unpackaged" or "in-process" hazard classifications will be established and approved as part of the site plan approval process.

17.6 Nonnuclear Munitions Safety Board (NNMSB) Certification.

NNMSB is the review and certification authority and the System Safety Group (SSG) for all nonnuclear munitions with only limited exceptions. As the review authority, the NNMSB mission includes various approvals and safety certification assessments conducted at specified points in various munitions acquisition phases. As a System Safety Group, the NNMSB mission includes providing design and qualification safety guidance to program management authorities during the life cycle. The NNMSB reviews and establishes design safety and qualification test criteria, standards, and requirements for nonnuclear munitions and related items; provides guidance to program management authorities throughout the life cycle of munitions programs to ensure that the criteria which form the basis for the safety certification review are receiving adequate consideration during all; and, maintains safety cognizance over all new or modified nonnuclear munitions, including those developed by the Air Force, those obtained from other US military services, and those obtained from foreign sources for nonnuclear munitions intended for Air Force operational use. If a munitions or equipment item is safety certified under the Air Force Nuclear Safety Certification Program (AFI 91-103), then the item is certified for nonnuclear use, provided the nonnuclear portion of the system was evaluated. Such nuclear certified munitions and equipment items are not reviewed by the NNMSB unless specifically requested.

Aspects of munitions systems, such as add-on components, software, and off the shelf equipment, will be evaluated as integral parts of the systems to which they belong. The following nonnuclear munitions systems, subsystems, components, and related equipment items, except as noted, are within the purview of the NNMSB as it carries out its mission: nonnuclear explosive devices, to include their training configurations, which are capable of producing a hazardous reaction and are used as implements of war or training; nonnuclear missiles to include those designed for air-to-air, air-to-ground, air-to-space, ground-to-ground, ground-to-air, and ground-to-space; release, control, suspension, and dispersal devices used to contain or disperse nonnuclear explosive devices, or used as the direct launching platform for a complete nonnuclear munitions system; safing, arming, and target-detecting devices; guidance and control mechanisms; igniters and initiators; guns and ammunition; propulsion devices; and, support and test equipment

Exclusions the NNMSB does not evaluate include explosive components of aircraft egress and life support systems; unmanned aerial vehicles except their explosive flight termination systems or unless the vehicle designed supports delivery of nonnuclear munitions; nuclear, space or nuclear missile systems that require separate system safety groups review and certification; most locally manufactured equipment (LME); general purpose equipment, such as, ground transport and passenger vehicles and commercial forklifts; explosive items peculiar to a specific aircraft which are exempted from NNMSB review by the NNMSB Executive Secretary when an adequate systems safety review is conducted by another qualified agency; and aircraft-munitions interface equipment whose functional

characteristics are under configuration control of the aircraft design authority.

The following general policy applies to all nonnuclear munitions systems, subsystems, components, and associated support equipment over which the NNMSB maintains cognizance authority: approval by the NNMSB is required prior to airborne testing of live-loaded uncertified munitions and initiating devices; ensuring no munitions or related equipment item will be certified for operational use until adequate technical data are available to the user; and certification by the NNMSB prior to entry of a nonnuclear munitions into the Air Force inventory, regardless of source. The NNMSB accomplishes certain technical safety functions to include: tailoring design safety criteria and standards and establishing safety performance requirements for nonnuclear munitions systems, subsystems, components, and related items; identifying and evaluating of the hazards in the design of munitions systems, subsystems, components or related items using the system safety engineering principles outlined in MIL-STD-882; establishing or approving procedures and warnings to help protect personnel, equipment, and property when risks cannot be adequately controlled through design provisions; developing safety recommendations which minimize risk during the life cycle of nonnuclear munitions, with consideration for mission requirements, employment concepts, and operating environments; minimizing retrofit actions required to improve design safety by ensuring safety design criteria exists during the development phase of each munitions system, subsystem, component or related item; and using historical safety data and lessons learned from similar munitions programs to help evaluate new munitions designs.

The primary tool used by the NNMSB to evaluate the nonnuclear munitions and related equipment items under its cognizance is a positive safety study and review program. This involves application of system safety techniques to make sure nonnuclear munitions and associated support and test equipment items, other munitions related items, and all operating procedures and technical data meet the highest safety standards. The safety evaluation process considers design, logistics, and operational requirements throughout the items' life cycles. The program requires the maximum use of existing safety documentation and lessons learned. Commanders, System Program Directors, Product Group Managers, Joint Program Offices, etc., responsible for procuring or modifying nonnuclear munitions, including all nonnuclear missiles and related items are also responsible for ensuring the requirements of this directive are satisfied. These responsibilities include: ensuring munitions/items requiring NNMSB study and review are identified to the Executive Secretary early in the design or acquisition process to minimize adverse schedule and cost impacts generated from NNMSB review; ensuring all required design safety standards are complied with and that adequate resources are allocated for explosives hazard classification actions as specified in TO 11A-1-47; and ensuring the appropriate safety studies such as Technical Munitions Safety Study (TMSS), Munitions Safety Analysis (MSA), or Test Hazard Assessment Review (THAR) are prepared at the earliest time during development.

NNMSB Certification is typically based on a Technical Munitions Safety Study (TMSS) or Munitions Safety Analysis (MSA) reviewed during a regular or special meeting. The TMSS is a comprehensive safety study of nonnuclear munitions, used to document safety engineering evaluations and to submit safety findings for NNMSB review. The TMSS must contain sufficient information to fully support the certification recommendations formulated by the board. The MSA is less comprehensive than the TMSS and is typically prepared for modified munitions and munitions support equipment having minor impacts on safety. Like the TMSS, the MSA must fully support NNMSB recommendations.

Chapter 18

SYSTEM SAFETY IN LOGISTICS

18.1 Introduction.

Early in this handbook we stated that system safety must be applied throughout the life cycle of the system. We have discussed in detail how system safety must look forward from the design phase to envision and control hazards that might occur during the operational life of the system as well as its disposal. Up to this point, however, we have not explicitly discussed the mechanics of the system safety process during the operational phase of the system life cycle.

Emphasis on the application of system safety principles in the early phases—the earlier the better--of the life cycle (concept through deployment) generally provides the greatest payoff since it is still possible to impact the basic design of the system and support infrastructure. This is reflected by the top choice in the general system safety order of preference for controlling hazards—design for minimum risk. Expenditure of considerable resources by both the government and contractors for system safety in these phases is easily justified by the potential avoidance of much greater costs later in the life cycle. MIL-STD-882 is written primarily to cover the joint government/contractor program during these early phases. Because of the level of emphasis and resources applied, system safety programs have generally been quite effective in helping to provide safer system designs with the potential for lower life cycle losses due to mishaps.

On the other hand, many safety problems are identified or even created during the operational phase of the system life cycle. There are many reasons for this.

a. Despite efforts to identify all hazards during the earlier phases, some end up as the part of the residual risk pie (see Chapter 3) labeled "Unidentified Risk." If we are lucky, these hazards may be identified as a result of High Accident Potential (HAP) reports or Class C mishaps. Unfortunately, it sometimes takes a Class A or B mishap to bring a hazard to our attention. Once these "new" hazards are identified, the system safety process must be brought to bear to help control or eliminate them.
b. While mishap experience may result in safety modifications, other identified deficiencies often lead to proposals for other types of modifications to improve performance, add capabilities to perform new missions, insert new technologies, or improve maintainability. Just because a system is fielded, design activity doesn't cease. All proposed modifications must be analyzed to ensure that they do not have a negative impact on system safety, either by introducing new hazards or by removing controls on hazards previously identified.
c. Logistics activities involving programmed depot maintenance, condition inspections or organizational maintenance often require changes or improvements. If changes are made to procedures or materiel to streamline operations or reduce costs, we must ensure that these changes do not delete or circumvent hazard controls dictated in the design phase. Sometimes we find that the logistics activities planned by the designers are not sufficient to make sure the initially safe design stays that way. For example, we may find that the inspection interval for jet engine fan blade cracks is insufficient to catch normal propagation prior to failure. Had this been foreseen in the design phase, a redesign of the blades might have been the obvious best move, in accordance with the system safety order of precedence. However, if the problem occurs in an operational system, redesign may be altogether impractical due to the cost of performing the modification. Even if a redesign action is chosen, inspection intervals and/or procedures will have to be altered temporarily to maintain safety until the modification to the fleet is complete. System safety principles must again be applied.

While contractors are participants in design system safety in nearly all cases (usually the major contributors to the effort), they may or may not be on contract to provide significant follow-on system safety support during the operational phase. This may mean that the relatively small formally designated system safety organization at the Air Logistics Centers (ALC) will have to conduct or supervise a great deal of important work on their own. Because (at least historically) the fielded system is supported by different people than those involved in the design (who are now busy acquiring the next new system), it is vitally important that ALC personnel provide feedback to government and contractor designers about what was learned during the operational phase. This is can be done in a variety of ways, including the Air Force Lessons Learned Program and through inputs to the AFMC Design Handbooks and Military Prime Specifications (MIL Primes).

We can see, therefore, that system safety plays an important role in the operational phase of the system life cycle. The purpose of this chapter is to describe some of the unique aspects of system safety programs conducted at the ALCs. We'll cover typical organizational structure and responsibilities, interfaces with other agencies and the conduct of risk assessments for modifications.

18.2 ALC System Safety Organization.

The basic requirement for system safety programs in air logistics centers (ALC) is stated in AFI 91-202, AFMC Supplement 1. It tasks ALCs to provide the manpower and resources to conduct system safety programs for each system or in-house effort and to integrate system safety into the overall program. Included are requirements to track hazards and conduct risk assessments (in particular to provide risk assessments for all safety modifications), and to address changes to the operational environment for the system. Also included are requirements to track failures of critical components related to catastrophic hazards so as to identify deviations from predictions, to track mishap experience versus predictions to help identify system deficiencies, to follow up system changes to ensure new hazards are not introduced, to ensure that historical data is applied to modifications and to document modifications for future reference. System safety is further tasked to ensure that safety is considered in all testing, to help develop procedures for the handling of hazardous materials, and to conduct five year safety audits for each system.

The AFMC supplement to AFI-91-202 provides details on how this work is to be done by outlining responsibilities for the command as well as the ALC. Personnel qualification requirements are outlined. At the ALC, a full time Center System Safety Manager (CSSM) is tasked with:

a. Making sure all players with system safety responsibilities fulfill their roles.
b. Manage the ALC system safety organization, training requirements, contract applications, system safety analyses, system safety groups, mishap and service report evaluations, and lessons learned applications.
c. Ensuring proper analyses and reviews are accomplished by directorates.
d. Coordinating on mission need statements, program management directives and other program documents.
e. Participating in system safety groups (SSG) and system safety working groups (SSWG).
f. Ensuring that mishap and materiel deficiency reports (MDR) are reviewed for application of system safety techniques.
g. Representing the safety office at Materiel Safety Task Group (MSTG) and Configuration Control Board (CCB) meetings.
h. Placement and training of system safety program managers (SSPM)in the program offices and product directorates.
i. Coordinating on safety modification risk assessments.
j. Conducting system safety staff visits within the ALC.
k. Providing an interface with bio-environmental engineering, fire protection and environmental planning agencies.
l. Ensuring that the system safety program complements the materiel safety program.

To assist the SSPM in the administration of the system safety programs, each of the ALC directorates may appoint a system safety program coordinator (SSPC

Participation in system safety meetings is required even during the acquisition phases, and the product directorate is responsible for reporting any inadequate acquisition system safety programs. The SSPMs are responsible for much of the detailed system safety work at the ALC. They must assess each modification or new design for its effect on system safety. If the effect is unknown, a preliminary hazard analysis (PHA) is required. If system safety is affected, further analysis is called for. As in the acquisition phase, the SSPM is required to certify the management decision to accept the risk for unabated catastrophic or critical hazards with probability levels worse than occasional and remote. A risk assessment must be accomplished by the SSPM for all safety modifications.

See AFI 21-101 for further information on management of modifications, including the classification of modifications as temporary (T) or permanent (P). Each type of modification can have an additional “Safety” classification, as long as it meets certain criteria: It must be shown that the modification can prevent loss of or serious injury to systems or personnel, and this must be agreed upon by the program manager, the using command, and the AFSC. A formal risk assessment (se para 18.3) must be prepared to justify any modification as a safety modification.

AFI 91-204, AFMC Sup 1 outlines the materiel safety program to “ensure the timely identification and correction of deficiencies which pose a hazard to the safe operation of weapons systems and support equipment.” It requires a materiel safety program for each system; the need for extensive two-way coordination to ensure this program complements the system safety program is obvious.

The ALC is required to establish and manage the MSTG and conduct meetings at least monthly. The ALC may also choose to set up a Deficiency review Committee (DRC) to review and provide MSTG inputs regarding mishap recommendations and MDRs, and to resolve disagreements between the SPM, item manager and using commands involving safety validation of materiel deficiencies. The DRC also reviews MSTG-related materiel improvement project priority assignments, part of the Product Improvement Program , to ensure they equal the criticality of the materiel safety deficiency.

Clearly, there are a lot of activities at the ALC that involve or relate to system safety. Figure 18-1 gives an indication of the complexity of the relationships between some of the various groups and programs discussed. Since there is only one required full-time system safety specialist, the selection, training and motivation of SSPCs and SSPMs is critical to a good program. In addition to conducting mandated reviews of others’ work and meeting attendance, a proactive approach on the part of the CSSM/SSPC/SSPM team is required to make the system effective. There is significant potential payoff to actively tracking available data sources such as MDRs, Class C and HAP reports, Joint Oil Analysis Program (JOAP) statistics, etc. to help identify deficiencies, bring them to the attention of others and begin corrective actions before the deficiencies have a chance to cause serious losses.

18.3 Risk Assessments for Safety Modifications.

Risk assessments of one form or another have always been accomplished at least informally for safety modifications. Formal risk assessments are now required to substantiate that a proposed modification is in fact a “safety” modification and that it is the justified alternative to correct the identified deficiencies. Risk assessments help minimize Band-Aid fixes, since they force consideration of the effect of the identified deficiency and the proposed corrective action on the total system (people, machine, environment, mission). They help ensure proper allocation of limited modification funds. The risk assessment summary, described in this section, is the minimum risk-assessment documentation required to accompany and support safety modification packages (reference AFI 21-101, para 2.14).

To be effective, the risk-assessment process must begin when any deficiency (design, maintenance, materiel, quality, software, etc.) having safety implications is initially identified. As such, it should be a part of the Configuration Control Board and Materiel Safety Task Group processes. It is a means to identify and substantiate the best alternative method of corrective action, and to identify any needed interim corrective action. If the best corrective action is judged by management to be a safety modification, the documentation resulting from the risk-assessment process becomes the basis for the safety modification risk assessment summary when the modification process is begun. To reiterate, the risk-assessment process does not begin when a decision is made to initiate the modification process. It must begin when the safety deficiency is initially identified.

Risk assessments must be coordinated with the ALC system safety manager and sent to AFSC/SEFE for approval.

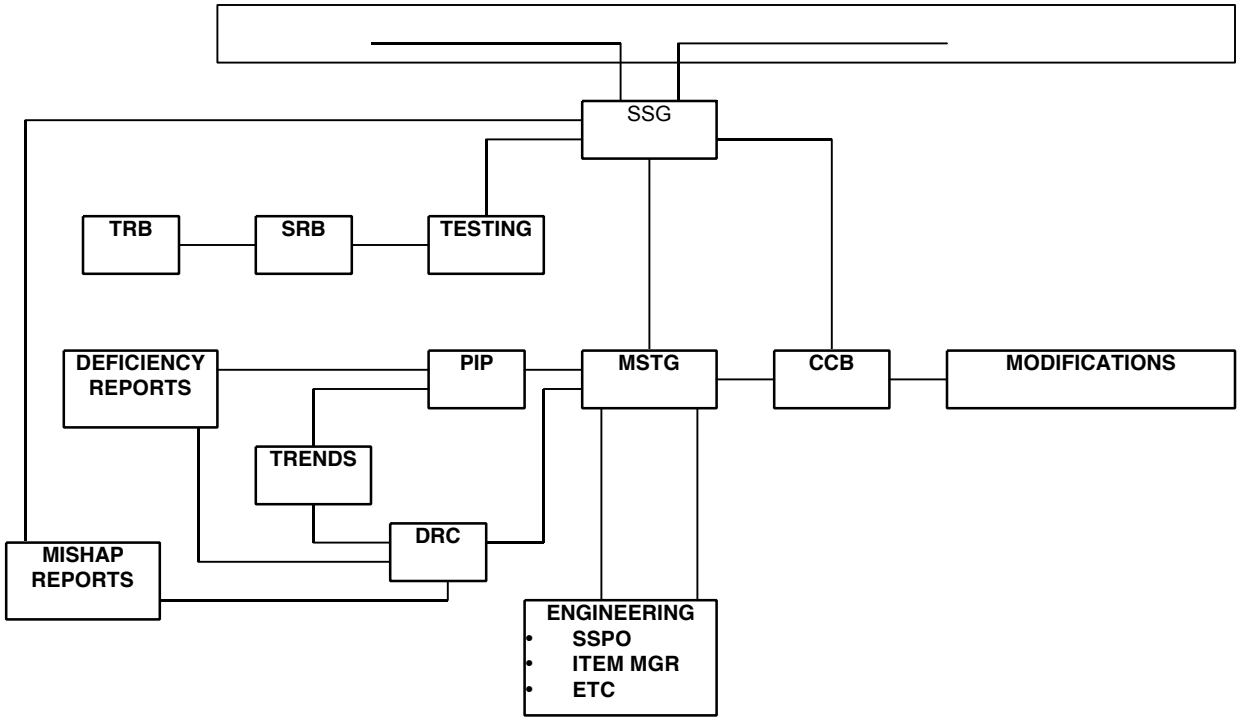
Definition of Terms:

a. Deficiency. Any design, maintenance, materiel, quality, or software problem, inadequacy, failure, or

fault. The deficiency can result from inability to meet original baseline requirements (hardware, software, operations, performance, etc.) or can be created from baseline changes which have evolved since the original baseline was established. Thus, the deficiency can evolve from noncompliance with the specified configuration, or can result from inadequate or erroneous configuration identification. Deficiencies, in combination with the human, machine, environment, and mission elements, can cause hazardous conditions to exist.

(1) Design Deficiency. Any condition that limits or prevents the use of materiel for the purpose intended or required where the materiel meets all other specifications or contractual requirements. These deficiencies cannot be corrected except through a design change.
(2) Maintenance Deficiency. A deficiency which results in excessive maintenance man-hour consumption. Factors to be considered are accessibility, simplicity, supportability, standardization, and interchangeability. Examples are: unsatisfactory accessibility to areas requiring inspection, servicing, replacement, and repair; inadequate interchangeability of parts; high rate of nonavailability of special tools, test equipment, and facilities required to accomplish scheduled and unscheduled maintenance.
(3) Materiel Deficiency. The failure of an end item which was attributable to neither the repair nor the manufacturing process, but was due to an unpredictable failure of an internal component or subassembly.

Figure 18-1
LIFE AT THE LOGISTICS CENTER



(2) Quality Deficiency. A deficiency attributable to errors in workmanship, nonconformance to specifications, drawings, standards, or other technical requirements, omission of work operations during manufacture or repair, failure to provide or account for all parts, improper adjustment or other condition that can be identified as nonconformance to technical requirements of a work specification. Failures or malfunctions which cannot be attributed to error in workmanship or nonconformance to technical specifications are not quality defects.

(3) Software Deficiency. An error in the instructions that comprise a computer program used by an embedded computer system. The deficiency may consist of syntax, logic, or other discrepancies that cause the program to fail the intended functions.

b. Hazard. Hazard is an important term that is often used rather loosely in the safety business. Our definition is "any condition that is a prerequisite to a mishap."

c. Mishap. An unplanned event or series of events that result in death, injury, occupational illness, or damage to or loss of equipment or property.

d. Risk. Risk has been defined in a variety of ways, most of which are unacceptable for purposes of understanding this term as associated with system safety. Our definition is "an expression of possible loss in terms of mishap severity, mishap frequency or probability (and exposure where applicable)." The expression of loss can be multidimensional. For instance, mishap severity and associated frequency or probability can be categorized with associated subcategories of direct or direct and indirect loss (lives, injury, property damage, equipment damage, etc.).

e. Safety Modification. A configuration change to a produced configuration item designed to correct a deficiency which has caused or can cause a mishap to occur.

f. Safety Modification Risk Assessment Summary. A document, assembled to support a safety modification, which summarizes the assessment of the risk associated with an identified deficiency.

It is useful to expand somewhat on the definition of risk to discuss the exposure parameter and to think of risk as an expression of expected loss over a period of time, number of operations or events, amount of activity, number of items, or a given population. Loss is measured in lives, dollars, equipment, property, and mission capability. Risk assessment, therefore,

involves determining the hazard involved, predicting resulting mishap frequency of occurrence, assessing severity or consequences, determining exposure, and identifying action to avoid or minimize the risk.

One may attempt to quantify the risk as an aid in deciding on a course of action. Risk ®, which may be only a "rough ballpark" figure, is for the purpose of this handbook represented by the mathematical expression:

R = L x M x E

Where:

Loss Rate (L) = loss per mishap, or severity

(How bad?)

Mishap Rate (M) = mishap per time or event,

or probability or frequency of mishap

occurrence (How likely?)

Exposure (E) = amount of time, number of events,

or amount of activity during which mishap

exposure exists. (How often?)

It is relatively easy to quantify risk when dealing with direct loss of lives and equipment per mishap, an established mishap rate for a given system in a specific operation, and known exposure such as can be obtained from flight or maintenance records. The follow-on action can then be based on risk reduction versus cost tradeoff to ensure safety. By trading off the reduction in risk (the benefit) against the cost of corrective action, the decision maker is able to pursue a logical course of action.

Unfortunately, the loss may not always be so tangible, or the mishap rate or exposure may not be known or available. As stated earlier, the loss may primarily be one of lost or reduced mission capability. What is that capability worth? What are the consequences? Perhaps mishap data does not exist. How does one assess the mishap potential or rate? We may be able to correlate to similar operations with similar weapons systems, or very likely may have to rely almost entirely on intuition. In any case, management should have the benefit of some kind of risk assessment on which to base its decision. What is needed is a framework within which risk analyses may be performed even when minimal mishap data exists.

The equation R = L x M x E appears as a straightforward approach, but seldom is such. More likely, it is simply a framework for thought. Especially when dealing with modifications, one might not expect to find neat, clean numbers to apply. Nevertheless, an increase in knowledge or information should result from this approach, thereby providing a better understanding of the overall problem. When insufficient information exists to use this approach, the more subjective hazard risk index method of MIL-STD-882 can be used.

The statement that one will accept no risk at all is sometimes made. Philosophically, it might be argued that there is some risk involved in everything we do, and that such a statement is therefore unrealistic. Accepting risk is something we do virtually every day of our lives.

Theoretically, there may be such a thing as risk-free environment. However, when operating systems in the Air Force inventory, we must assume that some risk exists. Determining what level of risk is "unacceptable" is left to managerial judgment. This judgment should be based on the best information and analysis possible. In accepting any degree of risk, the manager is always faced with doing something that ranges from accepting the risk associated with the system the way it is to not accepting the risk under any condition. In between, there are a number of actions that could reduce the hazards and, therefore, the level of risk. These actions run the gamut from simple procedural changes to major design modifications.

A safety modification risk assessment is an analysis of total modification cost versus the safety benefit to result from the modification. The safety benefit is risk avoidance. Risk is a measure of total expected future losses expressed in quantitative and qualitative terms. A safety modification (reference AFI 21-101) is structured to correct an identified safety deficiency. Each risk assessment must analyze the human, machine and environmental factors which, in the light of the mission, combine to produce the abnormal functions which cause the undesired losses. The assessment must describe how the modification will prevent or control this flow of events. Assessment of loss is difficult and is never all encompassing, but the analysis must consider the pertinent direct and indirect losses to be expected if the modification is not adopted. The primary focus is on direct loss prediction supplemented with indirect loss prediction.

Direct losses include mortality, injury, morbidity, system damage or destruction, and environmental damage or destruction. Direct loss prediction is primarily based on mishap data. This includes listing all losses per mishap which would have been prevented by the modification, identifying the associated mishap rate, determining future system exposure (remaining useful life flight hours, etc.), and predicting the anticipated total direct loss avoided.

Indirect losses include human productivity, system productivity, litigation, and investigation costs, to name a few. These losses are difficult to express quantitatively, but can supplement the direct loss assessment.

The following paragraphs summarize a step-by-step risk assessment process based on the very generic approach depicted in Figure 18-2. This process, which can be applied to any type of risk assessment or top-level hazard analysis, is described in much more detail in Appendix E. Sequentially, the steps are: (1) definition, (2) identification, (3) analysis, (4) action, and (5) feedback. Each step is briefly described.

a. Definition Process. The mission and system requirements, including the aerospace vehicle or subsystem, environment, facilities, support equipment, payload or armament, and personnel are examined. This is accomplished by reviewing current and planned operations describing the mission. The using command defines what is required to accomplish the operations and the conditions under which these operations are to be conducted. The implementing or supporting command defines the logistics support considerations.

b. Identification Process. Hazards and factors that could generate hazards are identified based on the deficiency to be corrected and the definition of the mission and system requirements. The output of the identification phase is a listing of inherent hazards or adverse conditions and the mishaps which could result. Examples of inherent hazards in any one of the elements include fire (system), explosion (payload), collision with ground (mission), wind (environment), or electrocution (support equipment). The analyst may also search for factors that can lead to hazards such as alertness (personnel), ambiguity (procedures), or escape route (facilities). In addition to a hazard list for the elements above, interfaces between or among

these elements should be investigated for hazards. An airman required to make a critical fine-tune adjustment to an aircraft on a cold, dark night (personnel—procedures—system—environment), handling of an air-to-air missile with missile-handling equipment (personnel—armament—support equipment), or frost-bite (personnel—environment) would be examples of the "interface hazards."

c. Analysis Process. Using the hazard list developed and some readily available "input" information, such as mishap records, mission plans, and previous hazard analyses, the analyst is now ready to evaluate the potential mishaps. The primary questions to be assessed are:

(1) How likely is it that a mishap will occur?
(2) How severe would be the injury or damage?
(3) What is the exposure to the mishaps during the planned operations, or for what percentage of the operating time is there exposure to the hazards or potential causal factors?

The answers to these questions form the basis for either a quantitative or qualitative determination of the risk involved and essentially complete the analysis phase.

d. Action Process. Having arrived at a conclusion as to the risk involved, management must now make decisions and take action to either accept, reduce, or eliminate the risk. Several options may be available, depending on mission, budget, and schedule constraints. Should management determine that the risk is too great to accept, they could theoretically choose from a wide range of options including changing the mission, selecting an alternate weapon system or modifying the existing system. Changing the mission because it is too risky or selecting an alternate weapon system to perform the mission are pretty drastic steps, requiring very high-level agreements among both logistics and operational commands—it is not a practical choice in most cases, and is certainly beyond the scope of this chapter.

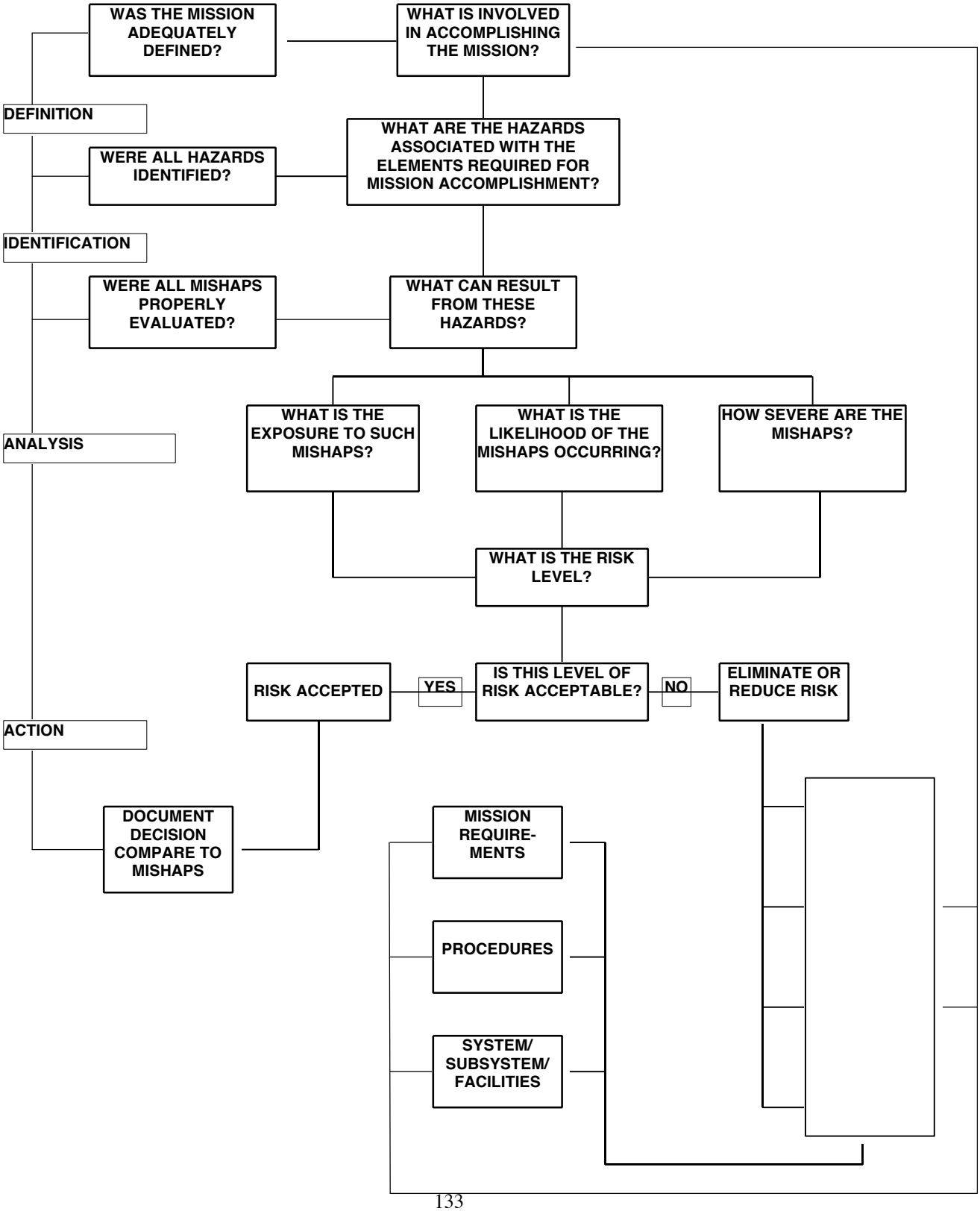
(1) The system safety order of precedence says the ideal action is to "design for minimum risk" with less desirable options being, in order, to add safety devices, add warning devices, or change procedures and training. This order of preference makes perfect sense while the system is still being designed, but once the system is fielded this approach is frequently not cost effective. Redesign to eliminate a hazard or add safety/warning devices is both expensive and time consuming and, until the retrofit is complete, the hazard remains unabated.
(2) Normally, revising operational or support procedures may be the lowest cost alternative. While this does not eliminate the hazard, it may significantly reduce the likelihood of a mishap or the severity of the outcome (risk) and the change can usually be implemented quickly. Even when a redesign is planned, interim changes in procedures or maintenance requirements are usually required. In general, these changes may be as simple as improving training, posting warnings, or improving operator or technician qualifications. Other options include preferred parts substitutes, instituting or changing time change requirements, or increased inspection.
(3) The feasible alternatives must be evaluated as to their costs in terms of mission performance, dollars and continued risk exposure during implementation. These costs must also be traded off versus the expected benefits. A completed risk assessment should clearly define these tradeoffs for the decision maker.

e. Feedback Process. This phase consists of two distinct functions. First, once the decision is made to take a particular form of action, one must return to the identification and analysis phases to verify that the recommended action will satisfactorily reduce the risk. Secondly, a mission feedback system must be established to ensure that the corrective or preventative action taken was effective and that any newly discovered hazards identified during the mission are analyzed and corrective action taken. When a decision is made to assume risk, the factors involved in this decision should be recorded. This action is necessary for two reasons. First, when a risk is assumed it is likely that future mishaps or incidents will occur. When they do, it is likely that the risk assumption decision and the risk analysis which supported that decision will be called up for review. Second, it is unlikely that every risk analysis will be 100 percent correct. When risk analyses contain errors of omission or commission it is important that those errors be identified and corrected. Without this feedback loop on the analyses, we forecast without the benefit of knowing if the previous forecasts were accurate, contained minor errors, or were completely incorrect.

If the risk-assessment process indicates that a safety modification is the best alternative to correct a deficiency, then the results of that process must be summarized. The documentation assembled during the risk assessment process serves as the basis for supporting the modification and for preparing the safety modification risk-assessment summary. The summary should answer all of the following questions, and is subject to the limited use reporting procedures of AFI 91-204, if limited use information is included in the summary. If a question is judged "not applicable," the discussion should explain why it is "not applicable."

Figure 18-2

GENERALIZED RISK ASSESSMENT PROCEDURE



The modification risk-assessment summary can be in any format, but it should, as a minimum, address and answer these questions:

a. What were the preliminary hazard-risk index results when the safety deficiency was initially identified?
b. What is (are) the identified deficiency (deficiencies) (design, maintenance, material, quality, software, etc?)
c. What are the hazards caused by the deficiencies in light of known requirements and interrelationships with man, machine, and environmental system elements?
d. What, if any, supporting historical data substantiate need for the modification? (List Class A, B, C mishaps, HAPs, Cat I MDRs, etc.) Trends?
e. What, if any, interim corrective action has already been taken to reduce risk? (Change in mission, operational restrictions, grounding, increased inspection, TCTO action, etc.)
f. What, if any, additional action has been recommended by the Materiel Safety Task Group, system safety group, system safety working group, or other group?
g. What are the expected future mishap rate(s) (A, B, C, etc.) to be caused by this deficiency if it is not corrected?
h. What is the affected fleet size, and its expected future life exposure? (List average number of operationally available aircraft per year, years of operational life remaining, average programmed flying hours per year.)
i. What are the expected total future direct losses (and indirect losses) if the modification is not approved? If sufficient data exists to make these predictions, what are the current mishap severity, probability and frequency, and resulting hazard-risk index values?
j. How will the proposed modification eliminate or control these losses?
k. How effective will the control of losses be?
l. If the modification is approved, what are the expected losses to be avoided, and any other quantitative or qualitative benefits?
m. Does the proposed modification create any new hazard for the system? (Consider mission and people, machine, environmental system elements.)
n. Why are other alternatives to risk reduction unacceptable? (Accept losses, preferred parts substitution, time change, training, procedural changes, increased inspection, etc.)
o. If the modification is approved, what will be done to reduce risk until the modification is fully implemented?

The office with primary responsibility for the system to be modified has responsibility for preparing the safety modification risk assessment summary. However, the information needed to answer the question required by the summary is obtained from various sources. The following matrix identifies sources:

Question	System Manager	Item Manager	Using Command	AFSA
a	X	X		
b	X	X	X	
c	X	X	X	
d	X	X		X
e	X	X	X	
f	X		X	
g	X			X
h	X		X	
i	X			
j	X	X		
k	X	X		
l	X	X		
m	X		X	X
n	X	X	X	
o	X		X	

In summary, a safety modification risk assessment weighs total modification costs against the total expected future losses to be avoided. This must be accompanied with sufficient rationale to explain how the proposed modification will control or prevent these losses, and to what degree it will be effective. The resulting assessment should not be structured primarily to attempt a direct dollar-to-dollar comparison. The objective of the analyst should be to justify that the modification has safety benefit (loss avoidance), and that benefit, expressed in nondollar qualitative and quantitative terms, outweighs the modification cost. A dollar assessment of the safety benefit, if available, can supplement this objective. It is management's responsibility to make final judgments as to the relative value of the safety benefit versus the modification cost.

CHAPTER 19

ACQUISITION MANAGEMENT OF HAZARDOUS MATERIALS

19.1 Hazardous Materials Impacts. (43:1-2)

The potential impacts of hazardous materials on a weapons system are many and varied. Some are readily apparent, such as the need for personal protective equipment or a high cost for disposal. Others are less obvious, but often just as significant. These can include the costs associated with special storage and handling, medical surveillance and workplace monitoring, and even the possibility of legal liability. The goal of integrated weapons system management of hazardous materials is to ensure that these potential operational impacts are considered whenever material selection or process design is performed during the development of a new system. Hazardous materials management personnel may also be able to provide assistance in assuring environmental compliance and occupational health at a contractor or government facility, but the main thrust of the program is the protection of future AF workers and the prevention of future environmental pollution.

Hazard analyses must include the effects of incorporating hazardous material into the system. The best method of controlling hazardous materials is to substitute them, i.e., use a non-hazardous material as an alternate. If that cannot be done, then other controls, such as containment and protective equipment and procedures will be necessary. The overall DOD policy on hazardous materials can be found in DOD 5000.2-R, para 4.3.7. USAF implementing documents are AFI 32-7080, Pollution Prevention Program, and AFI 32-7086, Hazardous Materials Management.

An effective contractual tool for hazardous materials management and control is the National Aerospace Standard 411 (NAS411), "Hazardous Material Pollution Prevention." This is a DoD-adopted commercial standard that can be used to require hardware system contractors and their subcontractors and vendors to eliminate and reduce the use of hazardous materials in systems, system components, associated support items, and facilities. NAS411 was created by the Aerospace Industries Association for application to the acquisition of systems, system components, associated support items and facilities. NAS411 can be contractually applied to each acquisition phases. NAS411 only applies to contractor's performing system engineering related work in one or more of the acquisition phases. The purpose of NAS411 is to influence the system and product design process to eliminate and reduce hazardous materials for the protection of human health and the environment while also considering cost and risks to system performance. NAS 411 does not specifically require the contractor to address all of the government's hazardous materials concerns during operations and support. Thus, the scope of coverage of NAS411 should be carefully tailored for each contract. NAS411 also does not provide for the Government's own in-house reduction or elimination of its procured hazardous materials and processes that utilize those materials. Finally, NAS411 will not reduce or eliminate hazardous materials in a straight non-developmental item procurement.

NAS411 is imposed on contractors in the request for proposal (RFP) phase of negotiated procurements. An offeror is required by the RFP to propose a hazardous material management plan for consideration and negotiation by the PM. The hazardous material management plan is the Contractor's own internal plan to assure appropriate consideration is given to the elimination/reduction of hazardous materials within systems, components, parts and support items the contractor is tasked with developing. NAS411 tasks the contractor to consider the effects that hazardous materials will have on operations and support, but specific tasks are included in the Standard. If NAS411 is going to be used to meet the PM's responsibility for identifying, minimizing use, tracking, storing, handling, and disposing of hazardous materials that will be used during operations and support, the RFP should specifically address each issues. NAS411 also provides for a contractor provided hazardous material management program report. The PM should tailor the contents of the report requirement to meet the actual data requirements of the program including the data requirements of the user.

CHAPTER 20

TEST AND EVALUATION SAFETY

20.1 General.

Test and Evaluation (T&E) consists of two elements: testing and evaluation. These are two distinct efforts and have two distinct safety responsibilities.

a. The testing effort consists of collecting data on the operation or support of the system under test. There are two primary safety functions during the testing effort. The first safety function is to ensure that mishaps/incidents do not occur during the test. The secondary function is to collect data on the effectiveness of any safety components of the system or identify new hazards that were not previously identified.

b. The evaluation effort consists of compiling the data from the test effort and making determinations about the "safeness" of the system. One safety function during evaluation is to determine if the safety features of the system functioned as expected and controlled identified hazards to an acceptable level of risk. Another function is to identify previously unidentified hazards. If it is determined that the safety features are inadequate or new hazards are identified, feedback is provided to the implementing and/or using command for resolution. This resolution can be redesign of the system, acceptance of the risk by the user, or some compromise.

20.2 Types.

There are two kinds of T&E in the system acquisition process: Development Test & Evaluation (DT&E) (AFI 91-101) and Operational Test and Evaluation (OT&E)(AFI 91-102). Either may occur at any point in the life-cycle of the system, subsystem, network, facility, software or item of equipment. OT&E usually follows DT&E, but they may be combined. The primary purposes are: to identify, assess, and reduce the acquisition risks; to evaluate operational effectiveness and operational suitability; to identify any deficiencies in the system; and to ensure delivery of operationally effective and suitable, supportable systems to operation forces. Sufficient T&E must be done before each major decision point to ensure that the primary objectives of one phase are met before the next phase starts.

a. Through DT&E, the implementing command must demonstrate the system engineering design and development is complete, that design risks have been minimized, and that the system will perform as required in its intended environment. This involves engineering analysis of the system's performance, including its limitations and safe operating parameters. It may involve testing product improvement or modifications designed to correct identified deficiencies (including safety), improve reliability and maintainability, or reduce life-cycle costs. A major objective of DT&E is to certify that the system is safe and ready for dedicated OT&E.

Qualification Test and Evaluation (OT&E) is like DT&E except it is performed on programs where there has not been a preceding research, development, test and evaluation (RDT&E) funded development effort. These programs might include: Temporary or permanent modification (see AFI 21-101), off-the-shelf equipment requiring minor modification to support system integration, commercially developed items, and other items that may require no development. The test policies for DT&E apply to QT&E.

b. OT&E is conducted under conditions that are as operationally realistic as possible and practical. These conditions must represent combat stress and peacetime conditions throughout the system life-cycle. OT&E evaluates (or refines estimates of) a system's operational effectiveness, maintainability, supportability, suitability, and safety; and identifies operational and logistics support deficiencies, and the need for modifications, if any.

Through OT&E, the Air Force measures the system's operational criteria outlined in program documentation developed by DoD, HQ USAF, and operating and support commands. Types of OT&E include: Initial OT&E (IOT&E), Qualification OT&E (QOT&E), and Follow-on OT&E (FOT&E).

(1). IOT&E begins as early as possible in a system's development and is structured to provide inputs at remaining program decision points.

(2). QOT&E is conducted instead of IOT&E on programs where there has been no preceding RDT&E funded development effort such as those described in "a. (QT&E)" above. The policies for IOT&E apply to QOT&E.

(3). FOT&E is operational testing normally conducted after the full-rate production decision. Individual FOT&Es may be conducted as needed through the remainder of the system life-cycle.

c. In a combined test program, development test usually occurs first to answer critical technical questions. As testing progresses, development and operational requirements are combined, where possible, to satisfy common data requirements. Before dedicated operational testing, the implementing command will formally certify that the system is ready for OT&E. OT&E tests production representative articles and must be conducted in an environment as operationally realistic as possible. In every case, the development and operational evaluations are performed independently.

Responsibility for the safety program generally resides with the responsible test organization. In combined test programs, the safety responsibility resides with the DT&E test organization. The implementing command reviews and approves all safety aspects of the combined test program. The individual with the test organization that shoulders the safety responsibility is the test director. They have the ultimate authority for decisions relating to the safe conduct of the test.

Mishap accountability is clearly with the owning organization of the system/personnel conducting the test. When more than one command is involved, accountability can become less clear. Accountability for aircraft, drone, missile, explosive, and ground mishaps, nuclear accidents and incidents, and safety deficiencies will be as specified in AFI 91-204 or established memoranda of agreement (MOA) among all agencies. Since there can always be different interpretations of regulations, it is best to spell out any accountability issues in an MOA. This will minimize the chance of confusion and "finger pointing" after a mishap/incident has occurred. A mishap/incident investigation is not the time to be discussing accountability.

20.3 Conducting a Safe Test.

As mentioned earlier, the first function of test safety is to ensure that mishaps/incidents do not occur during the test. The first step is to review documents such as: lessons learned, hazard analyses, training plans, technical data, mishap/incident reports, and test plans. Additional steps include review of the test site/range and actual equipment, attendance at system safety group meetings (SSG), and conduct of Safety Review Boards (SRB) (see Chapter 13 of AFI 91-202, AFMC Sup 1) and Flight Readiness Reviews (FRR). These efforts allow all involved personnel the opportunity to address safety concerns and discuss various methods to ensure a safe test. This interchange is critical as the knowledge of the group members far exceeds the knowledge of any single organization.

20.4 Testing the Safety of the System.

As mentioned earlier, the secondary function is to collect data on the effectiveness of any safety components of the system or identify new hazards that were not previously identified. This is, predominantly, part of the evaluation effort. The process is the same, however the purpose and results are quite different. Here the purpose is to provide an assessment of the effectiveness of the safety features of the system. This may be as simple as observing the operation of the system under test, or as complex as performing a special test on a particular safety device (e.g., the operation of the "pull-up" warning of a ground collision avoidance system). Additionally, written observations of the system operation and support activities can identify previously unidentified hazards. Any safety deficiencies will be documented for correction or further evaluation using the Product Quality Deficiency Reporting (PQDR) system described in Technical Order 00-35D-54.

20.5 The Test Safety Process.

The test safety process encompasses both the safety of the test, and the evaluation of the safety of the system. Both are interweaved to produce a consolidated safety effort to ensure a mishap free test and a concise test report. The process can be broken down into six steps (See Figure 20-1) Usually these steps do not have distinct bounds but overlap to provide a continuity of effort throughout the test program.

a. **TEST REQUIREMENTS**. The first step in determining the scope of the test effort is identifying the safety requirements of the test. This consists of: identifying the system requirements; selecting either simulation, modeling, or actual testing; developing the test scenarios; and reviewing the lesions learned.

(1). It is the responsibility of the using command, together with the implementing, supporting, and participating commands, to establish system safety criteria. The implementing command then evaluates the proposed systems to identify safety tradeoffs such as system performance, cost, interoperability, schedule, reliability, maintainability, human factors engineering, manpower, personnel, training, survivability, producibility, supportability, and integrated logistics support elements. The using command must concur with these tradeoffs and coordinate with the supporting and participating commands. These requirements become test criteria. It must be emphasized that the operational requirements are developed through an interactive process. Evaluation of requirements and tradeoffs lead to clarification and refinement of the requirements. The safety staff must keep abreast of all changes that might impact the safety of the system.

One must know the system requirements before the test events can be developed. If there are special safety requirements that the system must meet, they must be included in the test. Alternately, there may be no special safety requirements identified. In either case, it must be determined whether there are new safety requirements that were not originally foreseen. If the latter is the case, an attempt must be made to change the original system requirements documents. If it is impossible to change the original requirements, any new requirements must still be included in the test and evaluation. Lack of inclusion of a safety requirement in the requirements documents is insufficient reason to exclude it from the test and evaluation.

(2). Sometimes simulation or modeling is done in place of actual testing. This is appropriate when cost or safety factors make it necessary. Safety can be a driver in the decision to use simulation or modeling, but it should not be used as an excuse. If the test is too hazardous to conduct, what does that say about the potential operation of the system? Will the operator be the first one to be exposed to the hazard? When testing an aircraft ejection system, it is not feasible to test the system in a fully operational aircraft. In this case the aircraft can be modeled by a rocket sled and the ejection system tested accordingly. However, if you are testing a terrain following system, it is important to test the system in the operational environment. To say that it is hazardous to test this system would be correct, but it is more hazardous not to test the system in its intended environment. From this you can see that the use of simulation or modeling must be carefully evaluated to ensure that we are not moving a hazard exposure from the test to the operational arena.

(3). Once the operational safety requirements are identified and it is decided what should be tested, the test scenarios must be identified.

Development of these scenarios creates the environment in which the system will be tested. It is these scenarios that must be evaluated for potential hazards to the test. These same test scenarios will ensure that safety features are tested. In both cases the scenarios may have to be modified to include any safety issues related to test.

(4). Once the requirements are identified and the test scenarios established, lessons learned should be reviewed to identify potential hazards with the test. It is best to learn from the successes and failures of others. We should not be doomed to losing people or equipment because "we didn't have time to check the lessons learned." We should check the design lessons learned data bank to eliminate bad designs before they get into production. We should review the test lessons learned to prevent mishap occurrence.

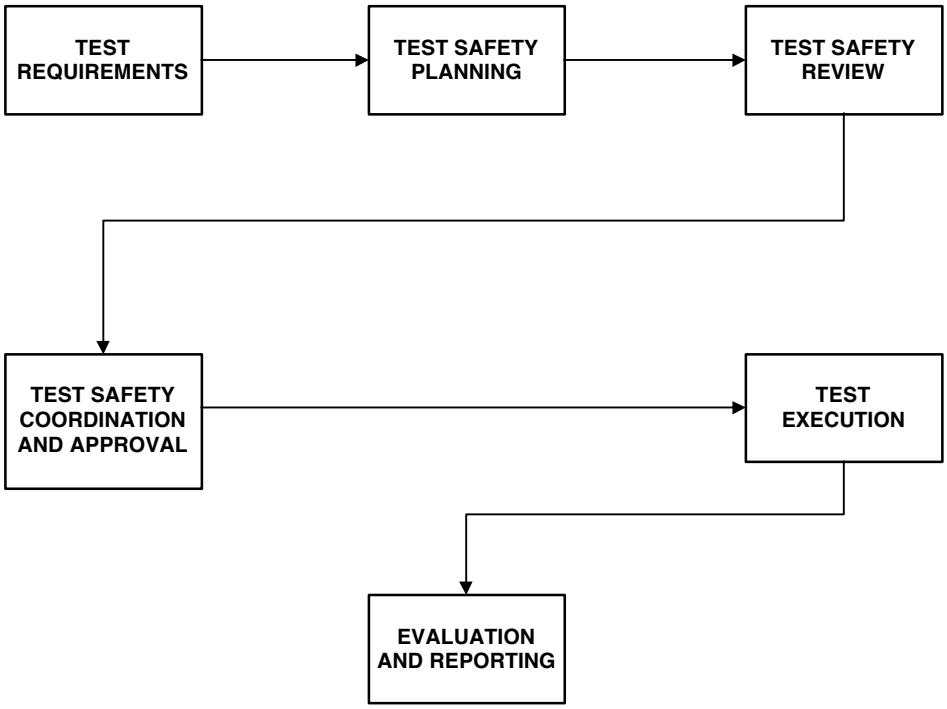
b. **TEST SAFETY PLANNING**. The next step is determining the scope of the test safety effort in test planning. Now that the requirements are identified and the type of test has been determined, the "how", "where", and "when" must be determined. From a safety perspective, the "how" and "where" are key safety concerns. Determining the "how" requires an evaluation of the test environment, training, status of the operation and support documentation, and history of similar systems. DT&E can test sub-systems independently before integrating into a system for test. This can minimize risk due to information learned from the sub-system tests. DT&E can conduct "test until break" testing to validate safety margins. OT&E must test the system in the intended operational environment. This takes the test out of the laboratory and into the real environment. Additionally, the emphasis on using "regular troops" to accomplish the testing requires that they are adequately trained and provided with accurate documentation. Whichever type of testing is conducted, several areas must be addressed to ensure a safe test and adequate evaluation.

(1). As mentioned in a previous paragraph, the environment in which the test can be conducted presents a challenge to the safety personnel. Usually the DT&E environment is more constrained while the OT&E environment is less so.

The system in DT&E has more unknowns, while the system in OT&E is well known. Since we know less about the operation of the new system, we must minimize the exposure from potential mishaps. We test new rocket motors

Figure 20-1

TEST SAFETY PROCESS



on special test stands away from anything that might be damaged by an explosion. When we get to OT&E, we have more confidence in the rocket motor and we test the system in a launch facility. If we have the same explosion now, it will result in significantly more damage. We must ensure as safe a test as practical by knowing and understanding the environment in which we are testing.

Another factor that we must consider is ensuring that the system is tested in all the environments in which it is to be used. Extremes in environment can cause equipment and personnel to respond differently. Wearing of cold weather gear can hamper the operation and maintenance of equipment. Hot tropical climates can cause significant degradation to electronic systems. Sandy climates can induce excessive wear on moving parts. These conditions can lead to unanticipated hazardous conditions. During both DT&E and OT&E the safety personnel must ensure that all expected environmental conditions are considered for the test.

(2). After identifying the environmental test conditions, the "where" can now be determined. There are several test ranges that provide the entire spectrum of environmental conditions. Once a suitable range is determined, the planning for use of that range should be started. Not only to ensure scheduling for the time needed, but to identify the safety requirements of that particular range. As will be discussed later, each range has unique safety requirements. Each range also has their own safety regulations and Safety Review Board (SRB) requirements. Early planning minimizes the potential for last minute conflicts and potential test delays.

(3). To conduct a test of a system requires personnel that know how the system functions. The only way to do this is to provide training. This includes training in normal operation/support and emergency procedures. Most systems have some residual hazards (e.g., high voltages, hot surfaces, toxic materials, etc.), but procedures and training should be the last resort for control of hazards. Personnel must receive training in how to deal with these hazards. Also, when a system fails, there are emergency procedures developed to minimize the impact of those failures. Personnel must be trained and practiced in these procedures. Safety must review all operations and emergency procedures to ensure adequacy of the procedures and training.

(4). Just as training is required to correct operation and support of a system, adequate documentation is required. People cannot remember everything taught to them. They must rely on manuals to supplement their training. These manuals must be accurate and include everything for safe operation and support. The manuals for the system must be reviewed before start of test to verify that the safety portions are complete and provide adequate instructions and cautions/warnings to personnel and equipment.

(5). For the same reasons that lessons learned should be reviewed, the mishap/incident data for similar systems, both in operation and test, should be reviewed to identify any potential risks during the test.

c. **TEST SAFETY REVIEW**. As part of the planning and before test start, there are several safety reviews that should be accomplished. Some of these efforts are continuous while others are single events.

(1). From the beginning of the program, the hazard analyses should be key elements of the safety review process. These analyses document the hazards and track corrective actions. Before test start, a final review should be made to verify the implementation of the recommended corrective actions. Sometimes several corrective actions may be recommended to reduce the risk to an acceptable level. In this case, all recommendations must be implemented before testing starts.

The hazard analyses not only assist in preventing mishaps during test, they identify those areas that require testing. If the analysis calls for training or procedures to minimize the risk, that training and those procedures must be evaluated for sufficiency. If they do not control the risk adequately, then either modifications to the procedures must be made or other methods to control the risk must be implemented.

(2). One of the best forums for safety is the SSG/SSWG. Every command involved in the development and fielding of the system should attend the SSG/SSWGs. Everyone contributes their experience and knowledge to identification and control of hazards in the system. This group has the attention of management and recommends the changes needed to ensure as safe a system as possible. The SSG should have recommended corrective actions for all identified hazards in the system. The test agency should include any test specific hazards. The test agency should use the information from the group when developing the test scenarios. This will minimize the probability of a mishap or delay in testing due to a hazardous condition.

(3). Obviously, the test agency wants a mishap free test. To accomplish this, the test agencies, whether they are test wings/groups, using commands, or AFOTEC, conduct their own safety boards. These go by many names: Safety Review Board (SRB), Flight Readiness Review (FRR), Flight Safety Review (FSR), Test Safety Review Board (TSRB), etc.; but the intent is to review all aspects of the test to ensure all identified hazards are controlled to an acceptable level. An appointee of the commander accountable for the assets or personnel usually chairs the board. All agencies involved in the test should be represented by membership on the board.

Test ranges require SRBs before testing on their range. There are few test ranges and, because of this, schedules are full. In addition to the potential loss of a system, we cannot afford range down time due to mishaps and mishap investigations. The high cost of rescheduling a range is prohibitive. Because ranges plan years in advance, it is no simple matter to reschedule tests while an investigation is going on. For these reasons, the ranges are particularly sensitive to safety.

d. **TEST SAFETY COORDINATION AND APPROVAL**. Upon completion of the planning and safety reviews, the coordination and approval cycle begins. There are generally two types of coordination and approval.

(1). The first is easy. All hazards are controlled and everyone agrees that the test should start. The commander, test director, safety manager, and other interested agencies all concur and the commander formally approves test start.

(2). The second can be very challenging. There are residual risks greater than the acceptable level of risk. At this time it must be determined whether to accept that particular risk and continue with testing, to put limitations on the test to minimize the risk, to make changes to the test to eliminate or further minimize the

risk, or to stop the test until the system is redesigned. This is not a simple decision. The initial attitude will be to accept the risk and proceed with the test. Safety personnel must be sensitive to the needs of the program. Not every risk is a show stopper, nor should a test proceed just to meet the schedule regardless of the risk. Some risk, with full knowledge of the possible consequences, can be accepted. The risk during test may be accepted with the caveat that the deficiency will be corrected before fielding of the system. It is the task of the safety personnel to provide all the information relating to the subject risk so that the commander or test director can make that informed decision. Risk levels and necessary risk acceptance authorities are delineated in Chapter 13 of AFI 91-202, AFMC Sup 1.

e. **TEST EXECUTION**. Now comes the test execution effort. This effort includes pre-test site reviews, deficiency reporting during test, and potentially, stopping and restarting the test due to safety problems.

(1). Once the test approval is provided, there are two actions that the safety office must complete. A test site visit and safety training validation must be done. Before start of test, the safety personnel should do a test site review to ensure that everything is ready for start of test. This ensures that those items highlighted by the SRB, or equivalent group, are done. System, facility, and ground safety items are reviewed. This is not an inspection. It is simply a last minute review to ensure no loose ends remain. During the site visit, completion of any required safety training is reviewed.

(2). During the test, the system is constantly being watched for potential safety problems. If any are identified, one of two things happen. For minor safety problems, a Product Quality Deficiency Report (PQDR) is filed in accordance with T.O 00-35D-54. For Cat I and II safety deficiencies, a Cat I PQDR is filed. For Cat III and IV safety deficiencies or recommended safety enhancements, a Cat II PQDR is filed. If the PQDR is not resolved by end of test, the hazard is identified in the final test report.

It should be emphasized that proper categorization of hazards is crucial. Not ranking a hazard high enough will reduce the emphasis on correction of the problem, possibly leading to a mishap. Ranking a hazard too high will distort the process and reduce the credibility of the whole system.

(3). If the Cat I or II hazard is an immediate risk, the test director should stop the test. At this time the problem will be evaluated and corrective actions will be taken. Limitations to the test may be necessary to continue the test while a permanent solution to the problem is worked. Another alternative action is to accept the risk until end of test and limit operational use until correction of the problem. If no appropriate corrective actions are available, the test may be postponed until resolution of the problem.

A follow-up SRB may have to be conducted before restart of the test. Whatever the reason for stopping the test, all personnel must be informed of the reasons for the stop and what actions were accomplished to allow a restart of the test. All involved parties must concur with the decision to restart the test. Some formal method to approve test restart should be developed during the test planning phase. This minimizes the chance of disputes during the test.

f. **EVALUATION AND REPORTING**. When the test is complete, the evaluation must be done. A key part of the evaluation is the filing and updating of PQDRs. The next action is the writing of an interim report and/or briefing, if required. For all tests, a final report will be written. If any significant safety events occurred, they should be included in the final report. Major safety issues should be included in the executive summary. The final report is coordinated through all involved agencies before publication of the final report. Since each major test supports a program decision point before the program progresses to the next phase, the SSG should review the draft final report and submit recommendations to the test agency.

20.6 Test Organizations.

As mentioned previously, there are different types of testing. There are also several different types of test organizations. There are those that plan and conduct testing, those that provide places to do the testing, and those that do both. The program offices plan and conduct most of the DT&E, while AFOTEC does most of the OT&E. There are several test wings and groups that conduct testing for the program offices. The test ranges conduct both types of testing.

East testing organization has their own set of regulations governing how testing will be conducted within their organization. All agencies involved in the subject test needs to be aware of the appropriate requirements early enough in the test planning process to prevent unresolveable conflicts. You should be aware that each range has unique safety requirements justified by the unique environment of each range. If you plan to test on more than one range you should be aware that you may have to meet different safety requirements for each range on which you conduct testing.

Almost every test organization requires an SRB or equivalent before start of test. It is the tester's responsibility to identify the necessary documentation to support the SRB. Thorough test safety planning will minimize the potential of a negative result from the SRB.

20.7 Directives, Regulations, and Documentation.

The following lists the application directives, regulations, and documentation relating to testing.

a. These documents provide guidance relating to test safety.

DOD 5000.2-R
MIL-STD-882C
AFI's 99-101 and -102
AFI 91-202
AFI 91-202, AFMC Sup 1, Chapter 13
AFI 91-204
TO 00-35D-54

b. These documents support the development and conduct of the test.

Operational Requirements Document (ORD)
Requirements Correlation Matrix (RCM)
Test and Evaluation Master Plan (TEMP)
Test Plan
Program Introduction Document (PID)
Host Tenant Support Agreement (HTSA)

Appendix

AN APPROACH TO RISK ASSESSMENT

A-1. Introduction. This appendix describes a very generalized technique for conducting risk assessments. It was originally published by the old Directorate of Aerospace Safety as a document called "A Risk Management Guide for Air Force Operations" to help our own people as well as using commands assess and find means to minimize risks. It was later incorporated in AFP 127-5, "Risk Assessment for Air Force Safety Modifications" with changes to address the role of the (system) program manager instead of the operational commander. This version attempts to address both roles, and can be used to evaluate overall mission risks or to assess the risk contributed by an identified deficiency. Because the suggested technique is both general and comprehensive it is applicable regardless of the situation and who is the final decision-maker. It is not necessary to conduct the analysis from scratch for each situation. Prior analyses of the baseline mission and system can be built upon to provide insight into new risks and controls. The risk assessment process is a detailed expansion of the risk assessment discussion in Chapter 18 of this handbook as depicted in Figure 2 from that chapter. Figure E-1 expands that previous figure, and will be the primary reference for our discussion.

a. As a starting point, one should assess the mission and system and ask a series of questions such as: "Have we or other units with similar missions or equipment done this mission before? If so, are the elements required to accomplish the mission, such as the aerospace vehicle, personnel experience or armament any different from previous missions? Is the environment any different between that experienced in the past versus what is now proposed? Are mission parameters the same? Essentially, what should be established here is that, if a "baseline" exists, one may be able to extrapolate or interpolate a certain cargo-type aircraft has a to determine the risk involved in changes to the baseline.

b. A cursory examination of a hypothetical situation will help to illustrate this method. Let us assume that landing phase mishap rate of 5 mishaps/l,000 landings during daytime assault landings. A planned exercise calls for night assault landings using the same aircraft, something that this unit has not previously attempted. Analysis shows that the only condition being changed is the environment from daylight to darkness. Comparison of all past mishaps for that aircraft reveals that the mishap rate is doubled at night. Analysis of pilot training received and experience level of pilots indicates that pilots are not as well qualified for the night mission. With this added information and perhaps other considerations, such as the analyst's intuition, a rate of perhaps 14 mishaps per 1,000 landings may be derived. The operations plan for the exercise requires 200 nighttime assault landings, which translates to 2.8 expected mishaps for the exercise. Armed with this information, management can proceed with a decision to accept or reject the risk, to cancel the operation or modify the operation in some way to reduce the risk.

c. A good case can be made for the argument that we have done most missions before and virtually anything we do is merely a variant of previous missions. Mishap data for past missions by type weapon system are available from HQ AFSC/SER. For most cases, SER has developed a mishap potential index for each weapon system under various mission and environmental conditions. This information alone provides an excellent assessment of the risk involved and can be provided to the operational units.

d. In some cases, the operational units may feel that the mission or exercise is too much removed from what had been done in the past to draw a meaningful relationship or comparison. The proposed operations, or anything similar, may never have been attempted. When these situations exist, the procedure illustrated in Figure A-1 is useful and should be tailored to the unit's specific need. The procedure helps to answer the following questions:

(1) What are the requirements and characteristics of the elements we are dealing with?
(2) What problems or hazards are associated with these elements?
(3) How frequently can we expect mishaps to occur, and how severe are they?
(4) What can we do to alleviate problems?

e. A structured approach to answering the above questions, at least in part, is described in this appendix. Each block number is keyed to Figure E-1. The approach is comprehensive, but the analyst should concentrate on those portions most applicable to the specific risk assessment being accomplished. Judgment, based on consideration of the identified deficiencies, must be used to determine those portions requiring evaluation.

A-2. Define Mission Requirements/Elements (Block 1). The first logical function in performing a risk analysis is to learn as much as possible about the operation to be conducted or the mission of the system being analyzed. Many weapon systems remain in the inventory much longer than originally planned, and are assigned missions completely different than what the original planners had in mind 20 or 30 years before. This leads to a number of potential safety problems. For example, flying at altitudes and airspeeds other than originally intended, carrying payloads or cargo that are far from being optimized for a particular airframe, extending operating limits or life, or operating in a weather environment that was not even considered when the system was designed.

It is, therefore, extremely important to understand the system and the requirements imposed on it today, not as it was initially designed or envisioned. Many questions can be asked. What are the parameters: altitude, speed, number of sorties, number of launches, duration etc.? What aerospace vehicle and subsystems are to be used? How will the operations be controlled? Is there an operations plan, logistics plan, test plan, safety annex? What are the personnel qualification requirements? How closely is the operation expected to simulate actual combat conditions? Will we be working with other services or allies? Are there any special requirements such as quick-turn refueling or ammo loading? When a thorough understanding of the mission is obtained and the elements required to accomplish the mission are identified, then each element can be individually analyzed for any inherent hazards or potential conditions that could lead to a mishap. Reference Figure A-1.

Figure A-1. Mission Requirements/Elements

- Mission (original baseline)
- Mission (new baseline)
- Elements
  - Aerospace Vehicle/Subsystems
  - Organizational/Personnel
  - Procedures
  - Environment
  - Support Equipment
  - Hazardous Materials
  - Payload/Armament
  - Facilities

A-3. Identify Hazard/Mishap Causes (Block 2-9). Based on the mission definition in Block 1, the analyst is now able to identify the applicable mission elements (weapons system/subsystems, personnel, procedures, environment, support equipment, payload/armament, and facilities) and potential hazard/mishap causes. A suggested approach is to take each element and list all known potential mishap conditions. This is no easy task; however, the suggested lists, which are by no means intended to be all inclusive, are included in Figure A-2 through A-8 for each of the elements. These lists will define those hazard conditions that should receive further evaluation.

a. As a general guideline, development of these lists should be predicated upon close scrutiny of existing energy sources—electrical, mechanical, thermal, radiant and chemical. Uncontrolled or undesirable transfer/loss of energy can be traced as a basic cause of many of our mishaps. An in depth review of past mishaps will show this theory to have a good basis in fact. Any mishap prevention effort involving Air Force systems and operations should include a search for sources of available energy—electrical, mechanical, thermal, radiant, and chemical—existing in the weapon system or subsystem, mission environment, facilities or equipment. As "energy hazards" are identified the analyst should identify unnecessary sources of energy that could be eliminated and search for means that are, or should be, incorporated to reduce and control the level of energy, control the transfer of energy, absorb free energy or isolate energy sources so as to minimize damage. Ideally, eliminating the source of the energy hazard is most desirable. However, recognizing that this is seldom possible, means for controlling energy—preventing hazardous accumulation or amounts; modifying or preventing the release; isolating the source; providing barriers to shield, protect, block, and attenuate-- should be actively pursued. When appropriate, energy monitoring devices (meters and gauges) should be installed to inform the operators of the presence and level of an energy source. This type of evaluation will be invaluable in determining the likelihood of a mishap occurring and the severity of the mishap should it occur.

(1) Electrical Energy. In carrying out most Air Force operations, use of some type of electricity is involved. An electrical circuit powered by any means of power generation carries with it the potential for electrical shock, burns and damage to equipment. A safety evaluation should include a search for possible causes which may include dirt, corrosion, moisture, fraying or chafing of wires, faulty or erroneous connection, exposure of bare conductors, improper voltage/current flow, power source failure, stray current/electromagnetic interference or presence of loose foreign objects (loose solder, components, or tools).

(2) Mechanical Energy. The category of mechanical energy transfer includes a wide variety of physical events resulting from a change in velocity or direction. Falling objects, impact, breaking, shearing, fracture and acceleration/deceleration are commonplace events. Impact is generally classified as active (a person or equipment running into a fixed object or falling from heights) or passive (a falling or moving object striking a person or equipment). Power machinery, hand tools, hydraulic and pneumatic devices, vehicles, cables, ropes, chains, storage tanks, valves, armament and structures serve to illustrate the wide range of hazard sources involving transfer of mechanical energy. In general when dealing with mechanical energy transfer, one has only to consider kinetic energy (energy of a body resulting from its motion) and potential energy (energy such as in a coiled spring or tank of high-pressure gas).

(3) Thermal Energy. In this category of energy transfer, the prime concerns are fire and excessive heat that can lead to injury, possible death or damage to equipment and property. A myriad of combustible materials are involved in Air Force operations (fuels, solvents, lubricants, gases, various solids, etc.). The analyst should be familiar with the properties of these combustible materials and the events that could initiate combustion. Engine starts, braking, an open flame, electrical arcing, lightning, static discharges, hot particles or metal and chemical reactions are examples of events that could provide an ignition source.

(4) Radiant Energy. Sometimes overlooked in a hazard analysis are the dangers presented by radiant energy from both natural and man--made sources. Solar radiation, which can cause burns, blindness and sunstroke, and cosmic radiation are the prime sources of natural radiant energy. When dealing with Air Force weapon systems and equipment, man-made sources of ionizing radiation (alpha, beta, and gamma rays from radioactive isotopes and x-rays from x-ray machines and televisions) and non-ionizing radiation (infrared and ultraviolet light, lasers, microwaves) generally present more concern. Knowledge, awareness, and appropriate protection are prime considerations when working with these "invisible" hazard sources. For example, an aircraft radar radiating the fuel tank of another nearby aircraft could result in an explosion; or a person unaware of the hazards of a laser beam may fail to wear an appropriate eye protective device (proper wavelength and optical density), stare into the beam, and end up with severe corneal or retinal injury.

(5) Chemical Energy. The transfer of chemical energy has the potential for explosion injury, toxicity (ingestion, inhalation, or absorption through the skin), and burns to humans as well as damage to equipment from an explosion

(mechanical and thermal energy also involved) or corrosion. Typically, what should be evaluated are incompatibilities among certain chemicals, incompatibilities between chemicals and other materials (metal containers, plastic plumbing, rubber seals, etc.) and electrolytic action (dissimilar metals) which may produce a hazardous or otherwise undesirable reaction. Potential for leakage or other forms of undesired release should be thoroughly considered in the evaluation.

b. Aerospace Vehicle/Subsystem Analysis (Block 2). The aerospace vehicle and any key subsystems to be employed in accomplishing the mission should be analyzed for existing sources of available energy as described above. This is a good method of starting an analysis since some form of energy flow is involved in virtually every mishap. An assessment of the various energy sources provides a good framework for this analysis. In many cases, a single energy source can present a problem; for example, electrocution. In other cases, it may take a combination of these energy sources, such as bursting of a high-pressure tank (mechanical) releasing a flammable fluid which, when combined with oxygen and an ignition source (thermal), could result in a catastrophic explosion. When analyzing a weapon system such as a fighter aircraft, a subsystem-by-subsystem (engines, landing gear, flight controls, etc.) assessment can be very revealing, particularly in what we classify as logistics-caused failures. The operational phases of the aircraft's mission (taxi, takeoff, cruise, approach, landing, etc.) provide another means for uncovering potential problem areas. Analysis of this element is one of the key activities of the overall risk analysis. A review of this portion of the analysis by competent system operators and maintenance personnel will help verify the identification of the hazards. Figure A-2 can serve as a starting point for analyzing the system and subsystems.

Figure A-2. Element: Aerospace Vehicle/Subsystem (Block 2)

- Fire
- Explosion/Implosion/Overpressure
- Electrocution
- Electrical Burns
- Electrical Failure
- Inadvertent Electrical Activation
- Structural Failure
- Radiation
- Engine Failure
- Mechanical/Hydraulic Failure
- Humidity
- Leakage
- Impact
- Corrosion/Toxicity
- Acceleration
- Air/Fluid Contamination
- Extreme Heat/Cold
- Excessive Noise/Vibration
- Flooding/Loss of Buoyancy
- Instrument Readability
- Control Accessibility
- Software Hazards

c. Personnel (Block 3). Analysis of the next element, personnel, should ideally be accomplished by a human factor engineer or someone thoroughly versed in human factors. Recognizing that these types of disciplines are seldom available in operational units, the analyst normally will defer to those with previous similar weapon system or mission-related experience. Flight surgeon assistance can be used to complete this block. The key to analyzing this element lies in understanding the role each person plays in accomplishing the mission, the demands the mission places on the person, the type of person involved (age, experience, attitude, maturity, etc.) and the possibilities of human error leading to a mishap. Once again a prerequisite is total understanding of the mission or operation to be performed. In turn, the analyst should assess whether the number, types, and qualifications of the people identified to carry out the operation are adequate to do the job safely. Human capacities, skill levels, tendencies, susceptibilities, and attitude can all have an effect. These factors should help to determine the amount of supervision and training required to minimize human error. Certain permanent or temporary conditions of the human, such as color blindness or fatigue, will play a key role in human error-caused mishaps. The potential effects of these conditions should be carefully analyzed. In operations involving military services of other countries, communications may have a critical effect on safety, particularly when there is a language barrier among the participants. Additionally, factors such as emotional instability and stress could impact mission safety. Their contribution as potential causal factors should be cited. Many of the potential cause factors are listed in Figure A-3.

Figure A-3. Element: Personnel (Block 3)

- Supervisory Factor
- Experience
- Acceptance of Responsibility
- Morale
- Qualifications/Intelligence
- Training (including emergencies)
- Illness/Physical Disability
- Vertigo/Disorientation
- Visual Illusions
- Alertness

- Responsiveness
- Perception/Human Factors
- Reactions
- Sight/Color Blindness
- Hearing
- Strength/Fatigue
- Stress (physical, psychological,
- physiological)
- Buddy System Reliance
- Emotional Stability
- Physical Fitness
- Communication/Language Problems
- Clothing/Protective Gear
- Boredom/Complacency
- Fixation/Hypnosis
- Efficiency

- Capability (task loading)
- Overconfidence

d. Procedures (Block 4). Block 4, Procedures, covers a lot of territory and is worthy of in depth treatment. In general, we are concerned with procedures which, if improper, could result in death, injury or equipment damage/loss. Many of the procedure-related causal factors are listed in Figure A-4. The mishap may occur while the improper procedure is being applied or at a subsequent time as in the case of mishaps which result from previous faulty maintenance. One means of illuminating this subject is through a task analysis to help determine workload, criticality of timing and coordination, necessity of the procedure, protective equipment required, emergency procedures and criticality of a particular task to the safety of the overall mission. Adequacy of tech data can be ascertained and the evaluator can also get an idea of how tedious, boring, tiring, and difficult the task is. Procedural task analyses may even find that certain safety equipment or devices actually hinder rather than help in the prevention of mishaps. For example, use of certain types of protective eye goggles during hazardous activity may degrade vision to a point where a mishap far more serious than eye injury is probable as a result of impaired vision. A dry run of the procedures may prove the tech data to be in error, ambiguous or confusing. Such a task analysis should also help to determine supervisory and training requirements. Also classified under procedures should be any caution and warning notes (in the tech data) or posted signs and their conspicuity. Several facets must be kept in mind at all times when analyzing procedures. They are:

(1) Murphy's Law. If the task or procedure can be performed incorrectly, it eventually will be done that way.
(2) If the procedures are lengthy, tedious, strenuous, uncomfortable or require patience, the operator may tend to skip steps or take shortcuts.
(3) Procedures that appear to be very simple and straightforward may lull you into a false sense of security.
(4) The way equipment is used leads to more mishaps than faulty equipment design.
(5) Unnecessary or extraneous steps should be eliminated from the procedures. The operators will skip these extraneous steps and, in turn, may start to skip critical steps.
(6) Some personnel "know it all." They have a disdain for checklists and procedures. Although they may be highly experienced, they may also take the greatest risk and be more prone to mishaps.
(7) Procedures that require intense concentration for long periods of time should be minimized or eliminated especially when interruptions or distractions could cause a person to lose his place in the procedure and possibly lead to a mishap.
(8) Checklists should be clear, concise and easy to follow.
(9) Procedures should identify all the proper parts, tools and equipment a person may need before the task is started. Once a job is started, the operator may be reluctant to stop the task to obtain the proper supplies and may delete an important step such as application of a sealant or the use of a wrong part. If the task is stopped to obtain the necessary material, the person may forget where he/she was in the procedure.
(10) Procedures requiring excessive communication between persons should be minimized especially when failure of the communications system or misinterpretations could lead to hazards.
(11) Training and qualifications required should be analyzed with the thought of how much on-the-job supervision will be available.
(12) Backout or emergency procedures should be simulated in as realistic a manner as possible and carefully tested for all possible contingencies.

Figure A-4. Element: Procedures (Block 4)

- Communications/Navigation Aids
- Supervisory Requirements
- Conciseness/Clarity/Ambiguity
- Emergencies/Backouts
- Tech Data/Checklists/Placards
- Buddy System
- Requirements for Attentiveness
- IFR/VFR Conditions
- Procedures Review
- Length/Repeatability
- Conformability
- Necessity
- Specialized Training
- Effects of Interruption
- Clothing Compatibility
- Instructions for Anomalies
- Hurried Judgments
- Protective Gear
- Specialized Equipment
- Servicing
- Maintenance/FOD Prevention
- Testing
- Operations/Crew Discipline and

Coordination

- Proximity of Instructions, Tables and Charts
- Checkout Procedures
- Criticality of Adjustments
- Criticality of Control Settings, Control Sequencing

e. Environment (Block 5). The environment, Block 5, plays a key role in Air Force mishaps. This element is often the only meaningful change from the norm or baseline. That is, missions that are relatively low risk during good weather and daylight conditions may present an unacceptably high risk when attempted under inclement weather and nighttime conditions. Over the years we have learned a lot about weather and other natural phenomena. We have learned of environmental effects, how to improve forecasting techniques and how to design to minimize or eliminate the damaging effects. Risk analyses of Air Force operations should fully consider the environment, whether natural or induced, in which the operation is to be conducted. The environment may have an effect on the

equipment being used or the person conducting the operation.

(1) Under the term "natural environment" is an extensive list of meteorological and other natural conditions. High crosswinds may cause landing problems. Extreme cold may cause carburetor icing. High humidity may cause personal discomfort and lead to human error. Lightning could cause a fuel tank to explode. A new operating locale may present a problem in terms of weather and topography: warm, clear weather versus cold weather and limited visibility; or smooth, level desert versus mountainous terrain.

(2) Artificial or induced environment includes the environment created by man or induced by the machine. Examples include pressurization systems such as those used to pressurize aircraft cabins, the "g" conditions under which a pilot often operates, toxic or asphyxiating environments, and the temperature and humidity control systems in aircraft or buildings.

(3) In compiling a preliminary hazard list (Figure A-5), the analyst should identify the natural and artificial environmental conditions under which the operation is expected to take place. By itself, the environment may not be a hazard. However, it will receive major consideration during the interface analysis particularly in how it affects man and the weapon system or subsystem.

Figure A-5. Element: Environmental (Block 5)

- Acceleration
- Deceleration
- Visibility (clouds, darkness, brightness, observation)
- Humidity/Rain
- Temperature
- Radiation
- Pressure
- Vibration
- Magnetic Fields
- Contamination/Pollution
- Wind
- Noise/Acoustics
- Lightning
- Snow/Icy Surfaces
- Ice/Sleet/Hail
- Turbulence
- Asphyxiation
- Topography/Terrain
- Midair Collision
- Ground Collision
- Birdstrike
- FOD Potential
- Effects from Other Systems (jet engines, rotors)

f. Support Equipment (Block 6). An area often overlooked in assessing risk is the general area of support equipment. Much of this equipment is mission essential and has a direct bearing on the safety of operations and support functions. Safety files are full of mishap and incident reports where maintenance, servicing, test equipment and tools contributed either directly or indirectly to mishaps. Examples include improper tools, instruments that are out of calibration, motorized vehicles striking aircraft, missile handling cranes running off the road, improperly grounded refueling systems and improperly secured loads on forklifts.

Analyzing mission support equipment requires an in depth review of the operations plan, test plan and any technical manuals or checklists that call out support equipment requirements. Inputs from ground safety, maintenance, servicing, test support and transportation supervisors will help to illuminate this subtle, but important, mission element. Figure A-6 lists many of the items to be analyzed.

Figure A-6. Element: Support Equipment (Block 6)

- Load Tolerance/Limit
- Special Adapter Requirements
- Securing of Load
- Movement/Motion Clearance
- Ignition Sources
- Fire/Explosion
- Fuel/Toxicity/Exhaust
- Operator Visibility
- Warning Device Requirements
- Deadman Controls
- Adequacy of Tools
- FOD Potential
- Mechanical/Hydraulic Failure
- Electrical Shock/Burns
- Electromagnetic Radiation
- Noise Levels
- Tool/Instrument Calibration

g. Hazardous Materials (Block 7). This element received inadequate attention for many years. Legislation now on the books as well as greater concern for both the environment and the costs to clean it up have brought increased emphasis to the issue of hazardous materials. Consideration must be given to use, handling, storage, transportation and disposal of hazardous materials either contained in the system or used in its support.

h. Payload/Armament (Block 8). This area could properly be considered under Block 2 as a subsystem; however, we cover it separately because of the unique explosive hazards inherent in the payload and armament area. Virtually any mishap associated with this mission element could prove to be catastrophic. Hence, this element deserves specialized, in depth treatment.

(1) Some ordnance and pyrotechnic devices are directly associated with the weapon system such as those devices found in ejection seat systems or strategic missile holddown bolts. While the items should be analyzed as part of Block 2, the effects of mishaps associated with these devices are similar to what one might expect from payload/armament mishaps.

(2) Units concerned with nuclear munitions will have at least one individual well versed in nuclear safety and surety and the person performing the risk analysis should defer to that individual's knowledge and experience. Likewise, nonnuclear munitions personnel are knowledgeable on all safety aspects of the weapons in their custody and serve as a reservoir of knowledge to help develop a

preliminary hazard list. The major output of this initial effort is to define the characteristics of the weapons to be used during the operation and the potential hazards these weapons represent.

(3) Characteristics of weapons include explosive propagation, sensitivity and blast effects. Some potential mishap causal factors are cracked propellant grain, corrosion, vibration, shock, careless or rough handling and electromagnetic interference. A more thorough list is contained in Figure A-7.

(4) The presence or absence of certain safety features should be noted. Explosive safety features may be of various types, including safe and arming mechanisms; out-of-line fuzing trains; material compatibility; electromagnetic compatibility; self-destruct capability; shock resistant design; ignition safety interlocks; dud-ding capability and protection against inadvertent jettison, release, or launch.

Figure A-7. Element: Payload/Armament (Block 8)

- Nuclear Blast/Radiation
- Inadvertent Arming
- Fuze Detonation
- Primer/Pyrotechnic Device Detonation
- Inadvertent Jettison/Release/Launch
- Inadvertent Electrical Initiation
- FOD Potential
- Burns
- Fire/Ignition Sources
- Explosion/Overpressure
- Gassing
- Corrosion
- Rocket Motor Ignition
- Warhead Cookoff
- Electromagnetic Interference/Pulse
- Explosives/Chemical Incompatibility
- Toxic Substances (liquid/gas)
- Leakage
- Damage During Handling/Loading/Storing

i. Facilities (Block 9). In conducting a risk analysis of an operation involving Air Force weapon systems it is often easy to overlook the facilities involved. Figure A-8 may be helpful in identifying potential facility problems. Building codes, Occupational Safety and Health Act (OSHA) and Air Force Occupational Safety and Health (AFOSH) standards usually cover the general safety design aspects of a facility's construction. However, it is unlikely that full consideration can be given to the way a facility may be used several years after construction. Also, facilities, such as runways, may deteriorate over a period of time and pose a threat to safety.

(1) Buildings should have appropriate facilities for the safe storage of hazardous materials and appropriate venting of any toxic or asphyxiating gases. Machinery and equipment should have required safety devices and noise levels should not increase the probability of mishap occurrence.

(2) When potential for injury from chemicals exists, appropriate antidotes or first aid should be available. The need for eye wash and wash-down facilities should be assessed.

(3) On occasion, temporary facilities or construction may be necessary for certain operations. These facilities should not present significant hazards.

(4) Buildings housing any type of hazardous activity must be designed to be compatible with the enclosed operation. The design should mini-mize the effects of any hazardous activity such as fire, explosion, toxicity, radiation, and asphyxiation. Visual and aural warnings and alarms should be readily seen and heard. The building design should further facilitate the rapid evacuation of occupants. Fire extinguishing agents should be readily accessible and effective, but by themselves should not present a significant hazard to personnel. An example here might be a high pressure Halon fire extinguishing bottle mounted in a manner such that, if inadvertently activated, it could fatally or critically injure a person near the nozzle outlet.

(5) Buildings housing lasers or other electromagnetic radiating devices should be designed to minimize hazards and provide controlled access.

(6) For air operations, runway conditions and airfield lighting should always be investigated for hazard potential. Virtually any facility in an aircraft or aircraft engine environment should be evaluated for foreign object damage (FOD) potential. Included are test cells, hangars, runways, engine runup areas, ramps, trim pads, and ramp accessways.

Figure A-8. Element: Facilities (Block 9)

- Hazardous Materials Storage
- Escape Routes
- Structural Durability
- Traction (floors)
- Environmental Control
- Fire/Ignition Sources
- Electrical Damage/Shock
- Explosion/Implosion/Overpressure
- Corrosion
- Warning Devices
- Toxicity/Environmental Control Systems
- Heights/Guard Rails/Stairs
- Earthquake/Flood Vulnerability
- Elevators
- Temporary Facilities
- Range Targets
- Airfield Lighting
- Emergency Lighting
- Runway Condition
- Runway Barrier Condition
- FOD Potential
- First Aid/Washdown
- Missile Silo/Launch Facility
- Controlled Access to Hazardous Areas
- Fire Alarms/Extinguishers/Hazards (Halon, water deluge)

A-4. Amelioration (Block 10).

Amelioration is not a system element but is necessary for consideration. Amelioration deals primarily with minimizing the effects of the mishap and avoiding possible follow-on mishaps. Amelioration helps minimize loss. It assumes that credible mishaps will occur, and evaluates the possible

actions, which can reduce the severity of these mishaps. The US Army's effort to improve the crashworthiness of helicopters is an excellent example of a successful amelioration program. The Army recognized that crash landings cannot be totally avoided, so they set out to incorporate all reasonable means to improve the survivability of helicopter occupants during a survivable crash. Losses can continue to occur beyond the conclusion of the initial mishap, so post-mishap actions are also considered, as shown in Figure A-9.

Figure A-9. Element: Amelioration (Block 10)

- Emergency Actions
- Control of Energy Source Inputs
- Control of Unwanted Energy Flow
- Target Evacuation (personnel, equipment)
- Rescue -
  Medical Services (first aid, transportation, treatment)
- Rehabilitation (equipment, personnel)
- Public Relations (relatives, neighbors)
- Crashworthiness (structural, restraints, delethalization)
- Energy Absorption
- Post Crash Fire/Egress

A-5. Preliminary Hazard List (Block 11).

Having defined mission and system elements (Block 1) and listed potential hazard/mishap causes (Blocks 2-9), the analyst is ready to perform a risk assessment of each of the hazards. Those conditions that could possibly exist and contribute as causal factors in a mishap should be listed as requiring evaluation. A worksheet might be devised and filled in to describe these possible hazards. The analyst can then provide a completed copy of these assessment worksheets to someone more familiar with the particular operations being analyzed and have this individual comment as to the validity of the concern. Depending upon the agencies involved, system safety groups, materiel safety task groups, safety review groups or similar activities may review and evaluate each item.

A-6. Interface Hazard Analysis (Block 12).

To this point, the effort has primarily consisted of gathering data on each individual element involved in the mission. The interface hazard analysis considers interplay among the various elements and their effect upon each other. This analysis requires a detailed understanding of both the physical and functional interfaces among aerospace vehicles, subsys-tems, facilities, and equipment. Additionally, and very importantly, the interfaces between each of these items and the human must be analyzed. Concurrent with all of these interface analyses, the analyst must consider the medium or environment in which the operation or function is to be performed. The environment, whether natural or artificial, may impact the hardware, facilities, and people.

a. Physical interface problems include the actual mating or fitting together of elements such as the way a pilot may fit into a cockpit or the way a missile is mounted on a launcher. Another example of a physical interface may be the suitability of a runway for certain aircraft particularly in terms of length. Clearance between vehicles or clearance between vehicles and facilities or equipment would also be classified under physical interface. A final example of physical interfacing would be load carrying capability such as a load of bombs being too heavy for transportation or loading equipment.

b. Functional interface analysis includes situations where one element inputs to another such as electrical or pressure functions. Failure of the first element may result in no input or erroneous input to a second element and lead to a mishap. In some cases, undesired inputs may cause a mishap such as electromagnetic radiation from an aircraft radar causing electrical squibs on ordnance items to fire.

c. The environmental interface may not be an actual interface in the true sense of the word but is classified as such because of the criticality of environment in so called "acts of God" and other environment-related mishaps. Certainly the aerospace vehicle, equipment, facility and people must be compatible with the environment in which they are located or under which they are operating. These mission elements should be able to withstand and function safely under all expected meteorological conditions and induced or artificial environments. A motor vehicle should operate safely on icy roads, buildings should be able to withstand high winds, an aircraft should be able to withstand a lightning strike, a mechanic should be able to safely function in cold weather, a pilot should be able to reach and operate necessary controls under conditions of acceleration and electrical contacts should not be affected by humidity-caused corrosion. In many operations, the need for an environmental interface analysis may not be apparent but in the end may prove to be the most "eye-opening" analysis of them all.

A-7. Inputs (Blocks 13-21).

Existing material on the weapon system being operated and the type of mission being performed is most useful in assessing the overall risk of an operation. This input material is extremely valuable in helping to determine the hazard severity or loss (Block 22), mishap rate or frequency (Block 23), and exposure (Block 24). The contents of each input are covered in the following Tables.

Figure A-10. Element: Deficiency/Service Reports (Input 13)

- End Item
- Deficient Item Works With ...
- Deficient Item Interfaces With ...
- Functions/Materiel Affected
- Mission Degradation/Constraints
- Extent of Equipment Damage/Severity
- Potential for Personnel Injury
- Maintenance Feedback

Figure A-11. Element: Mishap Records/Experience (Input 14)

- Experience with System/Subsystem Being Used
- Logistics/Operations Factors
- Mishap Causes
- Recommendations for Preventing Recurrence
- Extent of Damage/Injuries
  Lessons Learned

Figure A-12. Element: Previous Hazard Analyses (Input 15)

- Development and Modification Analyses
  - Preliminary Hazard Analysis
  - Subsystem Hazard Analysis

    - System Hazard Analysis
    - Operating and Support Hazard Analysis
- Analysis Methods
    - Fault Hazard Analysis
    - Fault Tree
    - Sneak Circuit Analysis
    - Failure Modes, Effects and Criti cality Analysis

Figure A-13. Element: Previous Similar Operations (Input 16)

- Degree of Similarity
    - Operations
    - Systems
    - Weather/Climate/Terrain
- Mishap/Incident Experience (Malfunction/ Failure/Damage)
- Potential for Mishap
- Adequacy of Training
- Adequacy of Contingencies
- Supervisory Requirements
- Adequacy of Communications
- Maintainability/Reliability Experience
- Scheduling Pressure
- Human Factors Experience
- Commander's Evaluation/Assessment

Figure A-14. Element: System Constraints (Input 17)

- Structural Limits vs. Operating Hours
- Engine Operational Limits
    - Cycles
    - Overtemps
    - RPMs
- Flight Envelopes
- Ejection Envelopes
- IFR/VFR Constraints
- G-Limits
- Takeoff Refusal/Abort Speeds
- Maximum Range/Combat Radius of Aircraft
- Range of Missile
- Terrain Considerations
- Minimum Equipment Requirements

Figure A-15. Element: Operating Requirements (Input 18)

- Operations/Logistics/Test Plans
- Safety Annexes/Range Safety
- Emergency Procedures/Search and Rescue
- Mission Planning/Briefing/Debriefing
- Contingency Plans
- Security/Sabotage Prevention
- Special Mission Requirements
    - Combat Turnaround/Hot Refueling
    - Special Cargo
- Special Tech Data
- Interface Communications
- Special Support
- Mission Combat Realism
- Formation Flying
- Missile Launch Envelope
- Special Training
- Uniqueness of Mission
- Protective Devices/Clothing
- Joint Service Operations
- Operations with Allies
    - Language
    - Equipment Interoperability

Figure A-16. Element: Operations and Maintenance Records (Input 19)

- Maintenance Data Collection Systems
- System Operating/Flight Hours
- Frequency of Maintenance Actions
- Number of Launches/Aborts
- Number of Firings (guns/missiles)
- Miles Driven
- Population
- Number of Items
- Amount of Activity (man-hours per flight-hour, supply actions per sortie, etc.)
- Number of Tests
- Fleet Size
- Remaining Useful Life (years/flying hours)

Figure A-17. Element: Safety Review Minutes (Input 20)

- System Safety Groups
- System Safety Working Groups
- Materiel Safety Task Groups
- Product Improvement Working Groups

Figure A-18. Element: Miscellaneous (Input 21)

- Durability and Damage Tolerance Assessment
- Aircraft Structural Integrity Program
- Analytical Condition Inspection
- Design Handbooks/Mil Primes
- Programmed Depot Maintenance
- Reliability Centered Maintenance
- Lessons Learned Database

A-8. Determination of Quantitative Risk (Blocks 22-25).

With the mission and system element assessment (Blocks 1 through 10), hazard lists (Blocks 11 and 12) and input data (Blocks 13-21) now available, the analyst is ready to determine the expected risk (expected loss), in either quantitative or qualitative terms. A commonly accepted quantitative method is to multiply factors that represent future losses expected per mishap (loss rate), mishaps expected per time or event (mishap rate) and expected remaining life (exposure) expressed in time or event. The result is risk (or total expected loss) if the deficiency is not corrected, or total risk for the planned operation being analyzed. This method requires historical data of Blocks 13 through 21 on which to base the predictions. Figure A-19 and A-20 provides some guidance. If sufficient data does not exist, a qualitative approach should be used.

Figure A-19. Determine Loss (L) per Mishap (Block 22)

DIRECT LOSSES

- Lives
  - Operators
  - Maintainers
  - Public/Other
- Equipment/Material (replacement or repair)
  - Vehicle (aircraft, missile, satellite)
  - Subsystems (ECM pods, laser designators)
  - Ordnance
  - Cargo
  - Expendables (fuel, etc.)
  - Property (public and private)

INDIRECT LOSSES

- Operational System
  - Recovery/Salvage Operations
  - Investigation Costs
  - Environmental Damage (plant/animal life)
  - Litigations/Liability
  - Burial/Medical and Disability Costs -- Training of Replacement Personnel
  - Lost Time Injury Costs
  - Insurance/Death Benefits
  - Loss of Skills and Experience
  - Loss of Mission Capability
- Redesign Costs
  - Engineering Change Proposals
  - Modifications once system is deployed
- Other Losses/Impact
  - Possible cancellation of program
  - Program schedule delays
  - Loss of fleet mission capability through grounding during inspection and repair/modification
- System performance limitations because of mishap potential
- Loss of confidence in system by operators, maintainers and public

Figure A-20. Determining Quantitative Risk (Block 25)

R = L x M x E

Where:

R = Risk
L = Loss Rate (L) from Block 22
M = Mishap Rate (M) from Block 23
E = Exposure (E) from Block 24

Example:

L = 1 aircraft per Class A mishap
M = 0.3 Class A mishaps per 100,000 flight hours
E = 500,000 flight hours
R = 1 X 0.3 X 500,000 = expected loss of 1.5 aircraft

A-9. Determination of Qualitative Risk (Block 26).

As we have already said, there is sometimes insufficient data upon which to base a quantitative estimate of risk. In other cases, a quantitative estimate may not be the most desirable. It is often difficult to "sell" a number that represents the result of a quantitative risk analysis. Numbers like 1×10^{-5} or once in four million events are often difficult for management to comprehend. The commander/program manager may not "believe" the number or the analyst, himself, may have little confidence in his number. What the commander/program manager may desire is a qualitative assessment that essentially lists the key problems, some unique concerns that may not be obvious, criticality of the problems and concerns and the likelihood of their occurrence. Supplied with this information, the commander/program manager and staff can arrive at a course of action on whether to accept or reject the risk. Oftentimes the staff's years of experience serve as an "institutional memory" of lessons learned and may be the most valuable tool in the whole risk analysis effort. Nevertheless, the better the hazard analyses and the more complete the input data, the more effective will be the output of this institutional memory. Some sample methods of qualitative analysis follow.

Figure A-21. Determining Qualitative Risk (Block 25)

- No attempt to assign an absolute number
- Inputs largely from past experience
  - Blocks 13-21 (documented)
  - Personal experience (undocumented)
- Tools
  - Intuition
  - Deductive Analysis—what things would happen to cause this particular mishap?
  - Inductive Analysis—given this malfunction or failure, what mishap might result?
  - Trends (could also be quantitative)

a. Mishap Risk Assessment Value Analysis. Perhaps the most commonly used safety analytical technique is the mishap risk assessment value. This technique should not be used if sufficient mishap data exists pertaining to the mission or identified deficiency to conduct a quantitative risk assessment. It can be used if a deficiency is identified before the deficiency causes a mishap, and should be used for an initial assessment of risk after a deficiency has been identified or a mishap has occurred. It provides a means to subjectively quantify risk based on a qualitative evaluation of the severity and probability of occurrence of hazards associated with the identified deficiency. This involves assigning arbitrary, dimensionless values to each classification of severity and probability, then multiplying the two numbers to obtain the risk assessment value. For purposes of conducting a risk analysis of an Air Force operation involving the elements previously mentioned, one could compute the value using the frequency and severity of mishaps associated with each element, sum up these values and evaluate whether or not this total is acceptable. Refer to Chapter 3 of this handbook or MIL-STD-882 for a discussion and examples of this technique.

b. Sensitivity Analysis. One of the more straightforward, and probably more meaningful, methods of qualitatively assessing risk is the

sensitivity analysis. Here, an assessment is made to ascertain how much each mission element contributes to the probability of a mishap occurring, the degree of mishap severity and the relative weight or importance a commander/program manager attaches to each of these elements in a given situation. In this type of analysis, the analyst can change a few key parameters and test the impact, or sensitivity, on the final outcome. If the impact is minimal, (i.e., the outcome changes very little, if at all) the analyst and his commander/-program manager can treat the results with a higher degree of confidence.

(1) The analyst analyzes each element and assesses the probability of a mishap occurring primarily because of this element or totals the number of different hazards that may result primarily from this element. Based on this assessment, a number is assigned to reflect this probability (zero through 5 as an example). The analyst may later test the "sensitivity" by adjusting the probabilities to see what the overall effect may be.

(2) Mishap severity is assessed in a similar manner. AFI 91-204 should be consulted for the definition of Class A, B, and C mishaps.

Figure A-22. Sensitivity Analysis Values

Mishap Probability

0 - Not applicable or mishap impossible (no hazards)

1 - Remote or very unlikely under any condition (very few, if any, hazards)
2 - Unlikely under normal conditions (few hazards)
3 - 50-50 chance of occurring under normal conditions (average number of hazards)
4 - Above average chance of occurring or above average number of hazards
5 - Very likely to happen or many hazards

Mishap Severity

0 - No damage, injury or loss
1 - No damage, injury or loss, but sets up conditions for potential loss
2 - Minimal damage, injury or loss
3 - Significant loss (Class C mishap or hazard with potential for major loss
4 - Class B mishap
5 - Class A mishap

Relative Weight (Subjective)

0 - Irrelevant or no importance
1 - Minimal importance
2 - Important enough to warrant attention
3 - Major concern—warrants constant attention

(3) The relative weight, or importance, is one of the distinguishing features of a sensitivity analysis. Here the commander/program manager has the opportunity to reflect his/her concerns. For example, the commander may feel that people are the key to the success of a particular operation and may have some concerns as to their qualification levels, morale, stress or other factors. In the commander's mind, this may be an extremely important element and the relative weight column would receive a multiple of three.

(4) The probability, severity, and weight can then be multiplied to produce subtotal values for each element. Some elements may not apply, reducing the total accordingly. For example, weapon/armament may not apply in assessing risk associated with a radar system or ground vehicle operation. Some pre-established ground rules should be set. As an example, it might be stated that any class A mishap severity (rating of 5) with a probability of 3 or greater is unacceptable or any single element value of 50 or greater (right hand column of Figure A-23) is unacceptable. Another guideline may state that any maximum table value (lower right hand corner) of greater than 200 is unacceptable or at least must be reviewed by the commander/program manager or a safety review board.

(5) There are a number of ways to perform sensitivity analyses. Most commonly they are in the tabular form (see Figure A-23). Problem areas, such as an unacceptably high probability of a mishap, can readily be spotted and action taken to reduce this probability and, in turn, lower the mishap potential. That is to say, high numbers or trouble spots are readily spotted and supervisors can apply their efforts in areas where there is the highest potential payoff.

c. Risk Exposure Analysis. The previous example of an analytical technique, the sensitivity analysis, takes into consideration the commander/program manager's concern by applying appropriate weights to the mission elements to reflect these concerns. Along a similar vein, the analyst may substitute an exposure factor in place of the subjective weight factor and perform a similar computation. Anticipated exposure rates may be projected from many sources such as the operations plan, reports of similar operations and maintenance records.

Figure A-23. Sensitivity Analysis Format

	Mishap	Mishap	Relative	Element

Mission Element	Probability	Severity	Weight	Value
Vehicle/Subsystem	0 thru 5	0 thru 5	0 thru 3	Maximum of 75 (multiply first three columns)
Personnel	"	"	"	"
Procedures	"	"	"	"
Support Equipment	"	"	"	"
Payload/Armament	"	"	"	"
Facilities	"	"	"	"
Environment	"	"	"	"
				+_____

Maximum of 525

A-10. Safety Assessment (Block 27)

a. With the mission now analyzed and the risk factors well understood, it is time to convene a safety review board or something similar. The purpose of such a review is to elicit the thoughts and opinions of the unit's institutional memory—those of experienced pilots, operations officers, maintenance supervisors, engineers, system safety personnel and others. The key outputs of this board are the verification of the analyst's findings, addition or deletion of safety concerns and recommendations for action.

b. The next step along the way is to brief the commander/program manager. This briefing should be concise, summarizing what was involved in the safety analysis with emphasis on the critical findings. Recommendations of the safety review board should also be briefed to assist the commander/program manager and staff in arriving at a decision.

A-11. Decision Time (Blocks 28-40)

The remainder of the risk management procedure covers the action required, given the overall safety level of the system or operation. This process starts at Block 28. One choice may be to do nothing. That is, accept the risk and proceed with the operation or live with the deficiency (Block 29). Another possible option is to completely cancel the operation because of the high risk and obvious lack of means to reduce this risk to an acceptable level (Block 30).

a. In between these two options lies a range of actions that could be taken to eliminate or reduce the level of risk. These actions include:

(1) Revising Mission Requirements (Block 31). The operations planners may not have been aware of the hazards involved in the operation. Certain operations described in the operations plan may not be as essential as originally thought and modifying these operations could significantly reduce the risk. In air operations, weapons delivery tactics may pose a hazard. Turnaround time requirements for refueling and reloading munitions could be unrealistic and lead to safety problems. Excessive workloads required of maintenance personnel might lead to fatigue and possible human error. Air operations in a "crowded sky" environment may significantly increase risk. Whatever the mission requirement, if it is causing safety problems, it should be considered for revision or possible elimination versus its essentiality to overall mission success.

(2) Consideration of an Alternate System (Block 32). An action that may not be feasible for most operations, but nevertheless should be considered, is selection of an alternate weapon system or subsystem. A mission selected for an F-4 aircraft may be done more safely by an F-15 because of performance characteristics. Or perhaps a chase mission should be performed by a T-38 instead of an F-15, if only because the potential loss (L) would be so much less in terms of dollar resources in the case of the T-38. In this case, degraded performance by the T-38 in comparison to the F-15 may be acceptable. Instead of a system change, we may want to consider an alternate subsystem. For example, a certain electronic countermeasures (ECM) pod may cause an unacceptable degree of electromagnetic interference with other electronic systems critical to safety of flight. Using a different ECM system may be the solution to the problem.

(3) Redesign or Modification (Block 33). This option may not be too viable for the short term in that a redesign requiring hardware modification is usually expensive and time consuming. Nevertheless, depending on the long-term benefits, this is an action that must be considered. At times, we may be concerned with a very minor change to the hardware that can be accomplished by the operational unit. In some cases, it might be acceptable to operate with the known deficiency in the short term with action taken to provide a long-term solution, for example, a safety modification in accordance with AFR 57-4.

(4) Revising Procedures/Personnel Qualifications (Block 34). Normally, revising the operational or support procedures may be the lowest cost alternative, especially when compared to expensive hardware procurement or modification. Also, revising procedures usually will not eliminate a hazard but should significantly reduce the likelihood of a mishap or the severity of the effects. A number of functions fall under the category of procedure revision, ranging from increased or improved training to the posting of caution or warning signs. This category also includes increasing supervisor, operator and technician qualification procedures to improve safety. Requiring protective clothing and protective equipment and rehearsal of emergency procedures are other actions that may serve to reduce the severity of a mishap. Another consideration is to upgrade the qualification requirements of the operators, maintenance personnel, and supervisors.

(5) Revising Maintenance Requirements (Block 35). This might involve using preferred part substitutes and instituting or changing time change requirements. Increased inspection and other technical order changes might be sufficient.

b. Determining Cost of Alternatives (Block 36). Each alternative should be evaluated not only for its dollar cost but also for its impact or "cost" to mission performance. The dollar costs are usually straightforward, but the impact on the mission may be measured in terms of degraded weapons delivery accuracy, reduced number of sorties, reduced speed with which the operation is accomplished or a number of other mission parameters. A great deal of judgment may be involved in trading off the cost versus benefits of the various alternatives. Extending the mission turnaround time of a fighter aircraft from 20 minutes to 30 minutes may improve safety but have an unacceptable impact on mission accomplishment. On the other hand, changing ECM pods as described earlier may only slightly degrade one's ability to jam an enemy's radar but greatly reduce hazardous EMI effects on radios, radar and electro-optical devices. The basic question to be asked is, "what is the cost of safety worth?" If a case can be made for a $200,000 training program having the potential of saving two $15 million aircraft and two pilots over a 5-year period, the decision is easy to make—spend the money for training now! However, a $10 million modification having the potential to save one $8 million aircraft over a similar 5-year period may not be justified. Oftentimes we overlook the total benefits derived from safety efforts. The partial list of the cost of mishaps provided back in Table E-19 will help in determining the benefits of mishap prevention. The list of direct losses deals primarily with losses incurred in mishaps involving operational systems. Should the operation involve a developmental system where safe design may help to reduce life cycle cost, then some of the indirect costs should be added to the list. Some of those costs could be attributed to a failure on the part of the developing agency to properly apply system safety engineering principles during the design of a system. This type of failure could also lead to problems with liability.

c. Choosing a Solution (Blocks 37-39). Having looked at a number of alternatives and traded off their associated costs versus the benefits they offer, the decision-makers must now choose among several courses of action. Once again, cancellation of the entire operation may be an acceptable solution (Block 37). Modifying the operation in some way, either with an alternate weapon system/subsystem, revised procedures, better qualified personnel, or modified weapon system/subsystem may be cost effective and be chosen as the solution (Block 38). Or the decision-maker may decide that the costs of changing things are too high or the benefits too minimal when compared to the relatively low risk and accept this risk without any modifications (Block 39).

d. Any solution involving risk assumption should be subsequently validated to determine if the decision was a correct one (Block 40). Figure A-22 defines some validation criteria.

Figure A-22. Validation of Risk Assumption Decision (Block 40)

- Validation occurs after modification has obtained sufficient field experience
- Validation could be initiated by
  - Routine actions (review of field data at predetermined milestone)
  - Incident-generated actions
    --- Mishap/HAP
    --- Discovery of adverse trend
- Validation requires
  - Record of risk assumption decision
  - Preservation of the record
  - Access to the record
- Validation is required to
  - Improve existing risk assessment techniques
  - Identify need for new risk assess ment technique
  - Identify faulty techniques which have been used in other risk assessments and resulted in invalid risk assumption decisions

A-12. Final Comments.

Regardless of the final decision, the increase in knowledge to the operating unit or responsible agency gained by performing a risk analysis as outlined herein can only serve to make the managers, supervisors, operators and support personnel more aware of the operational hazards involved and of some means to combat them. But this will only happen if a dedicated effort is made to inform the troops—from top to bottom—of the hazards involved. These people can help to reduce the risk but must first be armed with the necessary information. As emphasized throughout this guide, the procedure outlined here is not an absolute method—only an approach suggested by the Air Force Safety Center. Any suggestion for improving the guide or other comments are solicited and welcomed. Hopefully, the operating units or major commands will forward "real-world" risk analyses to AFSC as information copies to be used in refining this procedure. Comments, suggestions, copies of risk analyses, or other correspondence should be forwarded to HQ AFSC.

Additional guidance and tools can be found in AFPAM 91-215, Operational Risk Management (ORM)