1532

December 15, 1967

AEROSPACE SAFETY ADVISORY PANEL
IMPLEMENTATION RECOMMENDATIONS

National Aeronautics and Space Administration

AEROSPACE SAFETY ADVISORY PANEL
IMPLEMENTATION RECOMMENDATIONS

PREPARED BY:

Dr. Preston T. Farish, Industrial Operations
System Safety Technical Manager
National Aeronautics and Space Administration
Marshall Space Flight Center

R. Emerson Harris, Supervisor of Systems Safety
The Boeing Company
Huntsville, Alabama

Richard L. Reeb, Manager of Safety/Human Engineering
MOL Subdivision
McDonnell-Douglas Company
Huntington Beach, California

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

INTRODUCTION

Public Law 90-67 appropriating the 1967-68 NASA funding included the provision that an Aerospace Safety Advisory Panel be established. It is the function of this Panel to advise the Administrator with respect to the adequacy of the NASA methods used to:

1. Identify and report hazards or potential hazards
2. Eliminate or reduce these hazards to acceptable risk levels
3. Prevent a compromise of safety
4. Control deviations to safety management systems, hardware and procedures

It is recognized that the activation of the Panel will tend to serve as a management discipline for NASA in reviewing, strengthening, and consolidating its management structure and technical activities in safety. It also must be recognized that if this Panel is to be effective and accomplish the intent of the Congress, it must be an objective, unbiased body. The Panel must function in an environment of independence, as free as possible from all external influences. Further, the Panel must develop a means of understanding the information available to it, and arriving at realistic conclusions with respect to the hazards in proposed or existing systems, operations, and the adequacy of safety standards as well as the control of deviations to those standards.

Safety must be an integral part of the overall technical and management processes associated with the design, development and operation of complex aerospace systems. To be effective, the safety program must be technically acceptable to engineering, responsive to system schedules, sensitive to program needs, and never unduly restrictive. Further, it must be addressed to the personnel, the facilities, and the operational system itself.

The NASA method of performing the safety function is organized under three general headings as defined in NASA Management Instruction 1156.14, December 7, 1967, Aerospace Safety Advisory Panel. These include industrial safety, system safety, and public safety.

Industrial safety functions to provide a safe environment in which the manufacturing, testing, and operationspersonnel can safely work; system safety addresses its efforts to the identification, and elimination, or control, of hazards that have been inadvertently

designed or built into the operational system; public safety is oriented to the protection of personnel and property that are not related to NASA activities.

This report has been organized into four sections in order to describe typical activities of the Panel and its supporting Technical Safety Staff. These sections include:

1. Review
2. Initial assessment and recommendations
3. Panel activities
4. Safety data display system

SECTION I

THE REVIEW

The initial review of existing NASA safety organizations, and their respective functions, serves two purposes: It provides information required to make the initial assessment, and it familiarizes Panel members with safety activities presently performed at all operating and management levels.

This initial review should be accomplished in three increments, beginning with the Office of Manned Space Flight, since this NASA element is responsible for the man-rated systems. Review of the OART and OSSA organizations should follow immediately thereafter. The attention of the Panel should be addressed to:

1. Organization
2. Planning
3. Control
4. Hazard identification and correction
5. Safety reporting systems

Prior to beginning the review, the Panel must develop satisfactory methods for recording the required information. Many techniques are available, such as check lists, or narrative descriptions. Each technique has its unique advantages and disadvantages.

The Organization

The review of each management-level safety organization should provide answers to the following questions:

1. What are the objectives of the organization?
2. Have adequate resources been provided?
3. Will the present organization achieve the objectives?
4. Is there a proper division of work?
5. Is authority clearly defined?
6. Is responsibility fixed?
7. Is supervision provided at all levels?
8. Is the effort balanced and coordinated?
9. Is the organization flexible?
10. Is the organization generating conflicting decisions?
11. Does the organization provide adequate reports in response to directives?
12. Is the safety organization adequately staffed with qualified personnel to meet the objectives?

Safety Planning

The review of the safety planning activities should provide answers to the following questions:

1. Does the plan describe safety program goals?
2. Does the plan define specific safety tasks or program elements?
3. Where are the safety tasks to be accomplished?
4. When will the tasks be completed (schedule of tasks keyed to the major program milestones)?
5. Who will implement the plan and who will accomplish the tasks?
6. How will the tasks be accomplished (method)?
7. How will the activities performed be reported?
8. How does the plan from each area and management-level support the other plans for accomplishment of the overall program goals?

Safety Controls

The review of the controls falls into the areas of safety standards and criteria, conformance with or deviations from controls, and correction of deviations. Regarding controls, the Panel should determine whether:

1. Safety standards and criteria have been established and documented
2. Standards have been uniformly applied
3. Standards include adequate safety requirements
4. Management has a method of evaluating conformance
5. Deviations have been authorized
6. Unauthorized deviations have been corrected

Hazard Identification

The identification of hazards encompasses both surveillance and monitoring, as well as safety analyses.

Surveillance and monitoring normally consist of an on-site review of the manufacturing, testing, handling, storage, transportation, and operation facilities, as well as determination of conformance with safety standards and requirements.

Safety analysis is a detailed study of the design and hardware performed on a total system basis. It is this analysis which serves as the fundamental system safety baseline against which hardware changes, procedure changes and the personnel influences can be measured to demonstrate an improvement or loss in total safety.

A review of the technical safety activity at all levels should determine that:

1. Safety surveillance and monitoring is provided for all NASA activities
2. Results of these efforts are reported to management
3. Management responds to the hazard reports in an appropriate manner
4. Methods have been developed and imposed for safety analyses to be performed
5. Analytical method used is adequate
6. Effort is consistent among the various programs
7. Hazards identified by safety analysis are reported in a suitable medium
8. Corrective action recommendations influence the design
9. Closed-loop hazard identification and corrective action systems are used

Interfaces with Safety Related Disciplines

The technical safety effort is closely related to, and to a large extent dependent upon, the normal functional activities of the quality, reliability, configuration management, human engineering, maintainability, and system engineering organizations. Accordingly, a strong working relationship between the safety organization and these disciplines is prerequisite to an effective safety program.

The initial safety review should provide answers to the following questions as a verification that these interfaces have been established:

Configuration Management

1. Has a safety-configuration management functional interface been established?

2. What system exists to notify the safety organization that a change is being initiated?

3. Have criteria been developed as a basis for the designation of a safety change as such?

4. Is safety approval required on changes which impact safety, prior to Contract Change Board approval?

5. How does the safety organization take exception to Contract Change Board action?

6. To what level does the safety organization participate in drawing procedure-to-hardware validations and decisions?

HUMAN ENGINEERING

1. Has a safety-human engineering functional interface been established?

2. What data are exchanged and how are they verified?

3. How does the safety organization influence human engineering considerations?

4. How does information feedback to the safety organization?

5. How does human engineering participate in personnel certification activities?

MAINTAINABILITY

1. Has a safety-maintainability functional interface been established?

2. How does safety influence the preparation of maintenance concepts, procedures, and analyses?

3. How does information feed back to the safety organization?

4. Are repair time calculations provided to the safety organization for use in performing the safety analyses?

QUALITY

1. Has a safety-quality functional interface been established?

2. How does quality verify and report on nonconformance of the hardware with the safety requirement in the released drawings?

3. How do safety and quality work together to witness the qualification and acceptance testing of critical hardware?

4. How do quality and safety participate in the analysis of failed components?

5. How does safety obtain closeout verification of Unsatisfactory Condition Reports and failure analyses?

RELIABILITY

1. Has a safety-reliability functional interface been established?

2. How are reliability analyses (failure mode and effects analyses, and criticality analyses) provided to the safety organization?

3. Are mean time between failure (MTBF) calculations made available to the safety organization for use in performing the safety analyses?

4. Is operational data used to verify and adjust MTBF calculations?

5. How are safety analyses provided to the reliability organization to show the application made of the reliability analyses and data?

SYSTEMS ENGINEERING

1. Has a safety-system engineering functional interface been established?

2. How does safety participate in design reviews? (Preliminary Design Reviews, Critical Design Reviews, etc.)

3. How do safety recommendations influence the system engineering effort?

4. How does safety participate in mission planning and operational decisions such as go - no go decisions?

5. How does safety participate in postoperational studies and analyses?

SECTION II

THE INTERNAL ASSESSMENT AND RECOMMENDATIONS

Assessments should be undertaken with caution. Each fact uncovered should be evaluated both singly and in context with other facts. An objective determination must then be made as to whether each task actually enhances safety.

While this report contains recommended methods and techniques for performing a safety assessment, mature judgement is a vital ingredient for a successful evaluation. Furthermore, it must be recognized during the assessment and evaluation that the safety program should be truly dynamic in nature and responsive to the separate needs of each NASA system, as well as the unique operations performed at various NASA field centers. The effectiveness of the safety effort should be measured in terms of system impact, such as hazards identified and corrected, rather than quantities of documentation prepared and distributed.

Safety data and analyses developed for one system should be made available to all other NASA organizations for maximum utilization on other systems. The safety program must be postured to support sound engineering decisions in the area of safety, and thus obviate intuitive decisions.

Having developed the information previously described, the Panel should be prepared to perform the assessment.

A matrix exists which describes the optimum safety program technically oriented to finding hazards by use of the latest safety analysis techniques and correcting them before they become accidents. This matrix, shown in Figure 1, identifies the safety activities that should be performed at the various NASA levels and contractor activities during each phase of system development. This serves as a baseline against which the NASA safety activities may be inventoried. The adequacy of each task performed must ultimately become a matter of judgment by the Panel.

Data acquired during the Section I activity should be evaluated with the tasks being accomplished identified. These tasks are then compared with the Figure 1 matrix and a list of program omissions is prepared.

* NPD 7121.1 OCT. 28, 1965	PHASE A* ADVANCE STUDIES	
NASA HEADQUARTERS SAFETY OFFICE	1. Develop new NASA safety policies, guidelines and goals as required. 2. Monitor safety program activities and planning for conformance with policy and guidelines.	1. Develop and responsive t 2. Monitor safe policies and 3. Review accic
MSF, OSSA, OART, OTDA SAFETY OFFICES	1. Develop program-oriented safety policies and guidelines as required. 2. Monitor safety activities and report progress as required. 3. Participate in safety planning and approve safety plans. 4. Establish safety goals.	1. Refine progr 2. Monitor safe 3. Participate i 4. Approve Pha 5. Update safety
HEADQUARTERS PROGRAM SAFETY ORGANIZATION	1. Develop functional safety requirements and implementing directives. 2. Perform planning activities. 3. Approve Center safety planning. 4. Identify safety program elements. 5. Monitor Center safety activities. 6. Report progress and activities. 7. Refine planning for Phase B.	1. Refine funct 2. Update plans 3. Review Cent 4. Approve Cen 5. Identify addi 6. Monitor Cen 7. Report progr 8. Review data
CENTER SAFETY ORGANIZATION	1. Prepare planning and identify safety goals. 2. Approve contractor safety plans. 3. Develop initial safety efforts and requirements. 4. Participate in contractor safety development and contracting activities. 5. Develop interfaces with reliability, quality, maintainability, and human engineering. 6. Monitor contractor activities and report. 7. Perform data review.	1. Update safety 2. Refine safety 3. Identify safe 4. Update safety 5. Develop crite 6. Participate in 7. Review facili safety activiti 8. Development 9. Support inte 10. Provide for d 11. Report progr
CONTRACTORS SAFETY ORGANIZATIONS	1. Prepare safety plan (Phase A). 2. Gather and develop safety criteria. 3. Review related safety data from prior programs for applicability. 4. Develop working relationships with reliability, maintainability, and human engineering. 5. Perform safety analyses of design and mission concepts to support trade-off studies. 6. Update safety plan for Phase B.	1. Refine and d 2. Review facili industrial sa 3. Perform safe 4. Review safety 5. Update plann

PHASE B* PROJECT DEFINITION	PHASE C* DESIGN
1. Develop and refine safety policies and guidelines as required to keep them responsive to program needs. 2. Monitor safety program activities and planning for conformance with published policies and guidelines. 3. Review accident reports from developmental testing.	1. Develop and refine safety policies and guidelines as required to k responsive to program needs. 2. Monitor safety program activities and planning for conformance published policies and guidelines. 3. Review accident reports. 4. Develop public safety policy.
1. Refine program-oriented safety policies and guidelines as required. 2. Monitor safety activities and report progress as required. 3. Participate in safety planning. 4. Approve Phase B safety plans. 5. Update safety goals as required.	1. Refine program-oriented safety policies and guidelines as requir 2. Monitor safety activities and report progress as required. 3. Participate in safety planning. 4. Approve Phase C safety plans. 5. Update safety goals as required. 6. Develop public safety policy. 7. Assist in development of safety analysis goals.
1. Refine functional safety requirements and directives. 2. Update plans for Phase C. 3. Review Center safety criteria. 4. Approve Center safety plans for Phase C. 5. Identify additional safety program elements. 6. Monitor Center safety activities. 7. Report progress and activities. 8. Review data utilization.	1. Refine functional safety requirements and directives. 2. Update plans for Phase D. 3. Perform public safety planning. 4. Identify additional safety program elements. 5. Establish safety analysis goals. (undesired events and probabiliti 6. Review Center safety criteria and data utilization. 7. Monitor Center safety activities and functional relationships. 8. Report progress activities and anomalies. 9. Establish inter-center safety interfaces. 10. Review safety data, analyses and anomalies identified, and data e 11. Review state-of-the-art technical safety methods.
1. Update safety plan for Phase C. 2. Refine safety requirements. 3. Identify safety program elements. 4. Update safety goals. 5. Develop criteria documentation. 6. Participate in contractor safety development and contracting. 7. Review facilities and developmental requirements for changes in industrial safety activities and facilities. 8. Development inter-contractor interfaces. 9. Support inter-Center interfaces. 10. Provide for data exchange and utilization. 11. Report progress, activities and hazards.	1. Refine safety requirements and update planning to Phase D. 2. Expand and refine safety criteria 3. Support public safety contingency planning. 4. Update safety goals and identify safety analysis goals. (undesired their probabilities). 5. Identify additional safety program elements. 6. Participate in contracting for safety effort and approve contractor 7. Maintain all established functional interfaces. 8. Review facilities against changes in test requirements. 9. Monitor contractor safety activities. 10. Support design reviews with safety analyses. 11. Review data exchange and utilization. 12. Report progress, activities and hazards.
1. Refine and document safety criteria. 2. Review facilities and unique developmental requirements for changes in industrial safety activities. 3. Perform safety analyses to support system definition and trade-off studies. 4. Review safety data. 5. Update planning for Phase C.	1. Update planning for Phase D. 2. Refine safety criteria. 3. Start safety analysis (logic diagrams) for hazard identification and 4. Report hazards identified and correction implemented. 5. Review test procedures and approve qualification and acceptance t 6. Interface with reliability, maintainability, quality. 7. Review operational requirements. 8. Review test procedures, maintenance procedures. 9. Develop training and personnel certification requirements. 10. Review manufacturing planning. 11. Review shipping, handling, and storage requirements. 12. Support design reviews. 13. Perform accident and failure component analyses.

Figure 1. SAFETY ACTIVITY MATRIX

	PHASE C* DESIGN	PHASE DEVELOPMENT AN
d to keep them ance with published	1. Develop and refine safety policies and guidelines as required to keep them responsive to program needs. 2. Monitor safety program activities and planning for conformance with published policies and guidelines. 3. Review accident reports. 4. Develop public safety policy.	1. Develop and refine safety policies and guide responsive to program needs. 2. Monitor safety program activities and plann policies and guidelines. 3. Review accident reports. 4. Update public safety policy.
equired.	1. Refine program-oriented safety policies and guidelines as required. 2. Monitor safety activities and report progress as required. 3. Participate in safety planning. 4. Approve Phase C safety plans. 5. Update safety goals as required. 6. Develop public safety policy. 7. Assist in development of safety analysis goals.	1. Refine safety program policies and guidelin 2. Monitor safety activities and report progres 3. Approve Phase D safety plans. 4. Update planning as required. 5. Update safety goals as required. 6. Update public safety policy. 7. Monitor integration of safety analyses.
	1. Refine functional safety requirements and directives. 2. Update plans for Phase D. 3. Perform public safety planning. 4. Identify additional safety program elements. 5. Establish safety analysis goals. (undesired events and probabilities) 6. Review Center safety criteria and data utilization. 7. Monitor Center safety activities and functional relationships. 8. Report progress activities and anomalies. 9. Establish inter-center safety interfaces. 10. Review safety data, analyses and anomalies identified, and data exchange. 11. Review state-of-the-art technical safety methods.	1. Refine functional safety requirements and c 2. Review activities against plans. 3. Update public safety planning. 4. Integrate Center safety analyses into a total safety baseline and update as required. 5. Monitor use of safety analysis data to suppo safety goals are being met. 6. Review safety program at Centers for confor 7. Report safety program progress, activities, 8. Review state of the art advancements in tecl 9. Review performance of safety program elem
g. es in industrial	1. Refine safety requirements and update planning to Phase D. 2. Expand and refine safety criteria 3. Support public safety contingency planning. 4. Update safety goals and identify safety analysis goals. (undesired events and their probabilities) 5. Identify additional safety program elements. 6. Participate in contracting for safety effort and approve contractor safety plans. 7. Maintain all established functional interfaces. 8. Review facilities against changes in test requirements. 9. Monitor contractor safety activities. 10. Support design reviews with safety analyses. 11. Review data exchange and utilization. 12. Report progress, activities and hazards.	1. Refine safety requirements, planning and c 2. Update safety analysis goals and program el 3. Update public safety contingency planning. 4. Maintain inter-contractor and inter-Center 5. Integrate contractor safety analyses into a t safety baseline. 6. Develop requirements for end-to-end check 7. Participate in contracting effort and approv 8. Review hardware and procedure analyses ac 9. Support all major program reviews using th 10. Monitor contractor functional safety activiti 11. Report progress activities and hazards.
or changes in ade-off studies.	1. Update planning for Phase D. 2. Refine safety criteria. 3. Start safety analysis (logic diagrams) for hazard identification and correction. 4. Report hazards identified and correction implemented. 5. Review test procedures and approve qualification and acceptance test procedures. 6. Interface with reliability, maintainability, quality. 7. Review operational requirements. 8. Review test procedures, maintenance procedures. 9. Develop training and personnel certification requirements. 10. Review manufacturing planning. 11. Review shipping, handling, and storage requirements. 12. Support design reviews. 13. Perform accident and failure component analyses.	1. Refine safety analysis (logic diagrams) and hazard identification and corrective action i 2. Review hardware and procedures changes a safety baseline is not violated. 3. Participate in change board activities on sa 4. Support inter-contractor and inter-Center 5. Support accident investigation and perform 6. Monitor manufacturing, test, calibration, storage, and operational activities. 7. Support all major program reviews. 8. Update all analytical efforts as required. 9. Report progress, activities and hazards tog and responsibility.

PHASE C* DESIGN	PHASE D* DEVELOPMENT AND OPERATION
and refine safety policies and guidelines as required to keep them ve to program needs. safety program activities and planning for conformance with d policies and guidelines. ccident reports. ublic safety policy.	1. Develop and refine safety policies and guidelines as required to keep them responsive to program needs. 2. Monitor safety program activities and planning for conformance with published policies and guidelines. 3. Review accident reports. 4. Update public safety policy.
ogram-oriented safety policies and guidelines as required. safety activities and report progress as required. e in safety planning. Phase C safety plans. fety goals as required. ublic safety policy. development of safety analysis goals.	1. Refine safety program policies and guidelines. 2. Monitor safety activities and report progress. 3. Approve Phase D safety plans. 4. Update planning as required. 5. Update safety goals as required. 6. Update public safety policy. 7. Monitor integration of safety analyses.
nctional safety requirements and directives. ns for Phase D. ublic safety planning. dditional safety program elements. safety analysis goals. (undesired events and probabilities) nter safety criteria and data utilization. enter safety activities and functional relationships. gress activities and anomalies. inter-center safety interfaces. fety data, analyses and anomalies identified, and data exchange. te-of-the-art technical safety methods.	1. Refine functional safety requirements and directives. 2. Review activities against plans. 3. Update public safety planning. 4. Integrate Center safety analyses into a total program analysis to establish safety baseline and update as required. 5. Monitor use of safety analysis data to support program reviews and to assure safety goals are being met. 6. Review safety program at Centers for conformance with requirements and schedule. 7. Report safety program progress, activities, hazard correction activities. 8. Review state of the art advancements in technical safety methods. 9. Review performance of safety program elements by Centers.
ety requirements and update planning to Phase D. d refine safety criteria ublic safety contingency planning. ety goals and identify safety analysis goals. (undesired events and abilities) ldditional safety program elements. in contracting for safety effort and approve contractor safety plans. ll established functional interfaces. ilities against changes in test requirements. ntractor safety activities. sign reviews with safety analyses. a exchange and utilization. gress, activities and hazards.	1. Refine safety requirements, planning and criteria. 2. Update safety analysis goals and program elements. 3. Update public safety contingency planning. 4. Maintain inter-contractor and inter-Center interfaces. 5. Integrate contractor safety analyses into a total system safety analysis as a safety baseline. 6. Develop requirements for end-to-end checks and system validation. 7. Participate in contracting effort and approve contractor plans. 8. Review hardware and procedure analyses activities against this baseline. 9. Support all major program reviews using the safety analysis baseline analyses. 10. Monitor contractor functional safety activities. 11. Report progress activities and hazards.
ning for Phase D. ty criteria. analysis (logic diagrams) for hazard identification and correction. ards identified and correction implemented. procedures and approve qualification and acceptance test procedures. ith reliability, maintainability, quality. ational requirements. procedures, maintenance procedures. ning and personnel certification requirements. ufacturing planning. ping, handling, and storage requirements. ign reviews. ident and failure component analyses.	1. Refine safety analysis (logic diagrams) and support analysis integration for hazard identification and corrective action implementation and reporting. 2. Review hardware and procedures changes against safety analysis to assure safety baseline is not violated. 3. Participate in change board activities on safety changes. 4. Support inter-contractor and inter-Center interfaces. 5. Support accident investigation and perform diagnostic analyses. 6. Monitor manufacturing, test, calibration, checkout, handling, shipping, storage, and operational activities. 7. Support all major program reviews. 8. Update all analytical efforts as required. 9. Report progress, activities and hazards together with correction, schedule and responsibility.

The information obtained in the initial review is then analyzed to identify any inadequacies or inconsistencies in the following:

1. Organizational structure
2. Planning and activities
3. Management control
4. Hazard identification techniques
5. Establishment of safety standards

The identification of both the program omissions and the specific inadequacies or inconsistencies provides the basis for the development of recommendations. These recommendations should be addressed not only to the omissions and inadequacies, but also should include any areas that are receiving excessive emphasis and are redundant.

Once the recommendations have been completed for all management levels of the NASA safety organization, the effort of the Panel and its Safety Technical Staff turns to the sustaining activities.

SECTION III

PANEL ACTIVITIES

The Panel activities fall into two areas which include the initial review and the sustaining activities.

Implementation of the Initial Review

NASA Management Instruction 1156.14, Aerospace Safety Advisory Panel, includes the requirement for a Safety Technical Staff of full-time NASA employees to support the Panel. The initial action required in support of the Panel is the selection and assessment of personnel to the Safety Technical Staff. Members of this staff are to be fully responsive to the requirements of, and direction from, the Panel.

The Director of the Safety Technical Staff should serve as Executive Secretary and chief technical advisor to the Panel and is responsive to specific instructions from the Panel and from the NASA Administrator.

The Staff should consist of four members, with one member appointed as the Director, and should be appointed prior to beginning the initial review.

Safety Technical Staff Implementation

Immediately upon formulation, the staff should begin preparation for the first increment of the review.

Forms are prepared for recording the data developed, visits are scheduled in accordance with Panel directions and travel arrangements are completed. One staff member should accompany each Panel team during completion of the Manned Space Flight safety review and support the preparation of the review report.

Upon completion of the Manned Space Flight review, one member of the staff should be assigned to begin the sustaining effort for the Manned Space Flight organization.

The Panel and the remaining three staff members then redirect their attention to the Office of Space Science and Applications organization and repeat the review process.

When the Office of Space Science and Applications review report and recommendations have been completed, a second staff member is assigned to begin the sustaining effort for this organization.

The third staff member is assigned the Office of Advance Research and Technology organization, and the review process is again completed.

This provides a Safety Technical Staff organization as shown in Figure 2. The Staff Director serves as Executive Secretary to the Panel, interfaces with the NASA Safety Director in matters of safety policy and

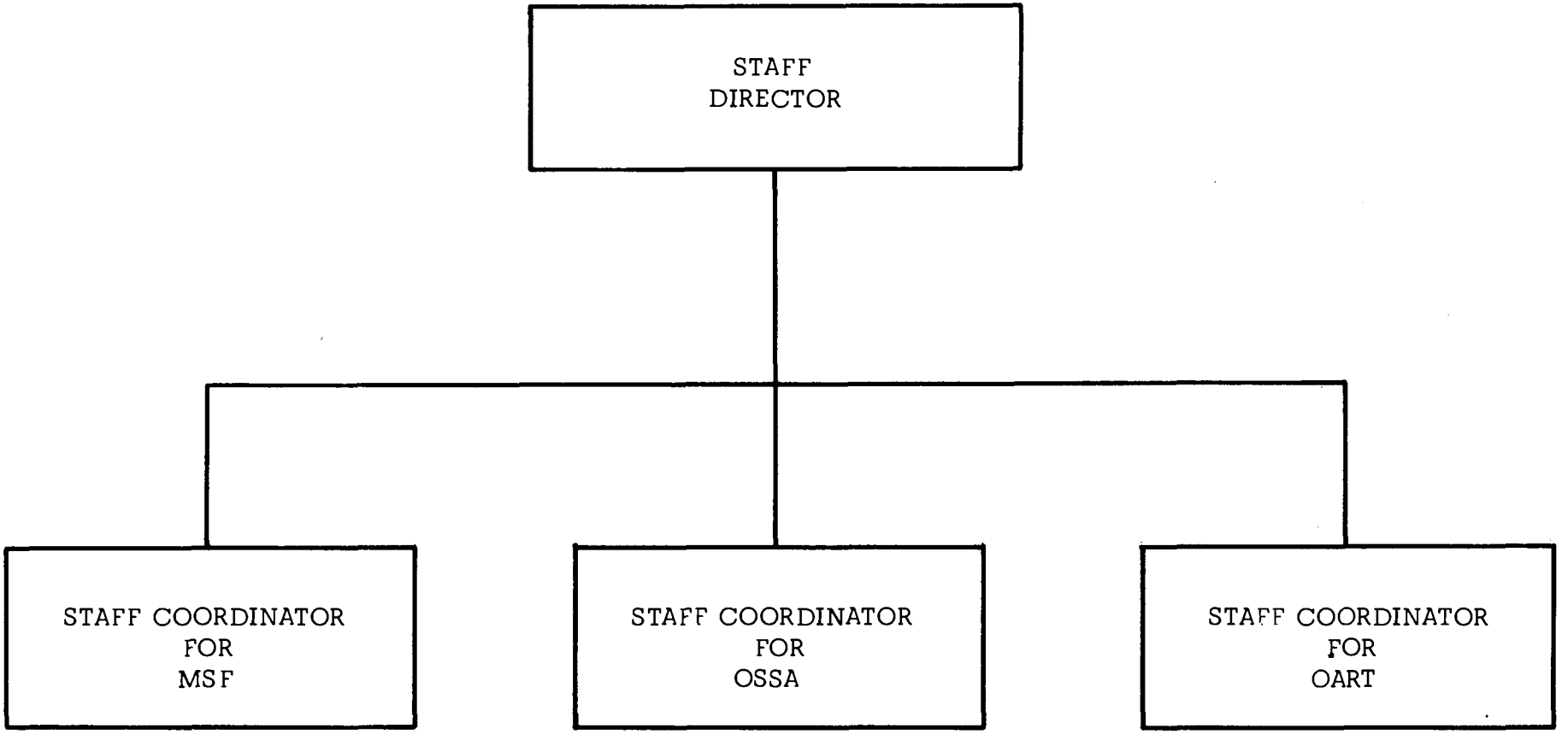


Figure 2. Safety Technical Staff Organization

guidelines, and functions as the focal point for the effort of the three functional staff members, assuring their efforts are integrated to the fullest extent possible.

Sustaining Activities of the Staff

Each staff member begins his sustaining activities by developing requirements and formats for data submittal by the functional organization.

As illustrated in Figure 3, the activities of the Safety Technical Staff include the identification of system hazards and potential hazards. This is based on a review of safety analyses and data developed at the functional safety levels, and, the effective display of this data to provide current, comprehensive visibility as to the safety of the system. The safety is covered in terms of hazards identified, corrective action implemented, the responsibility for, and the effectiveness of, the corrective action.

Consistent with this activity, each staff member performs continuing assessments of the NASA safety program management relative to the adequacy of:

1. Organization
2. Planning
3. Control
4. Hazard identification
5. Corrective action
6. Safety reporting system

Performance of these activities is a full-time task with monitoring programs and analyzing data playing a large role. Safety visibility evolves from an objective reduction of safety analyses and data by the Safety Technical Staff members. These data are originated at the contractor level where the basic technical safety program elements are being performed. It is at this level that the well-trained, competent safety engineers, using modern techniques, perform the safety analyses that will serve as the foundation of the Panel's visibility.

Data reporting relationships are from the bottom to the top with safety decisions and corrective action implementation accomplished at the lowest possible level. Thus, the information presented for Panel consideration is in terms of:

Problems or hazards that cannot be resolved at any of the functional levels, together with potential program impact relative to risks, costs and schedules.

Hazards identified that are being resolved, the organization or person responsible for the resolution, and the schedule for completion of the action.

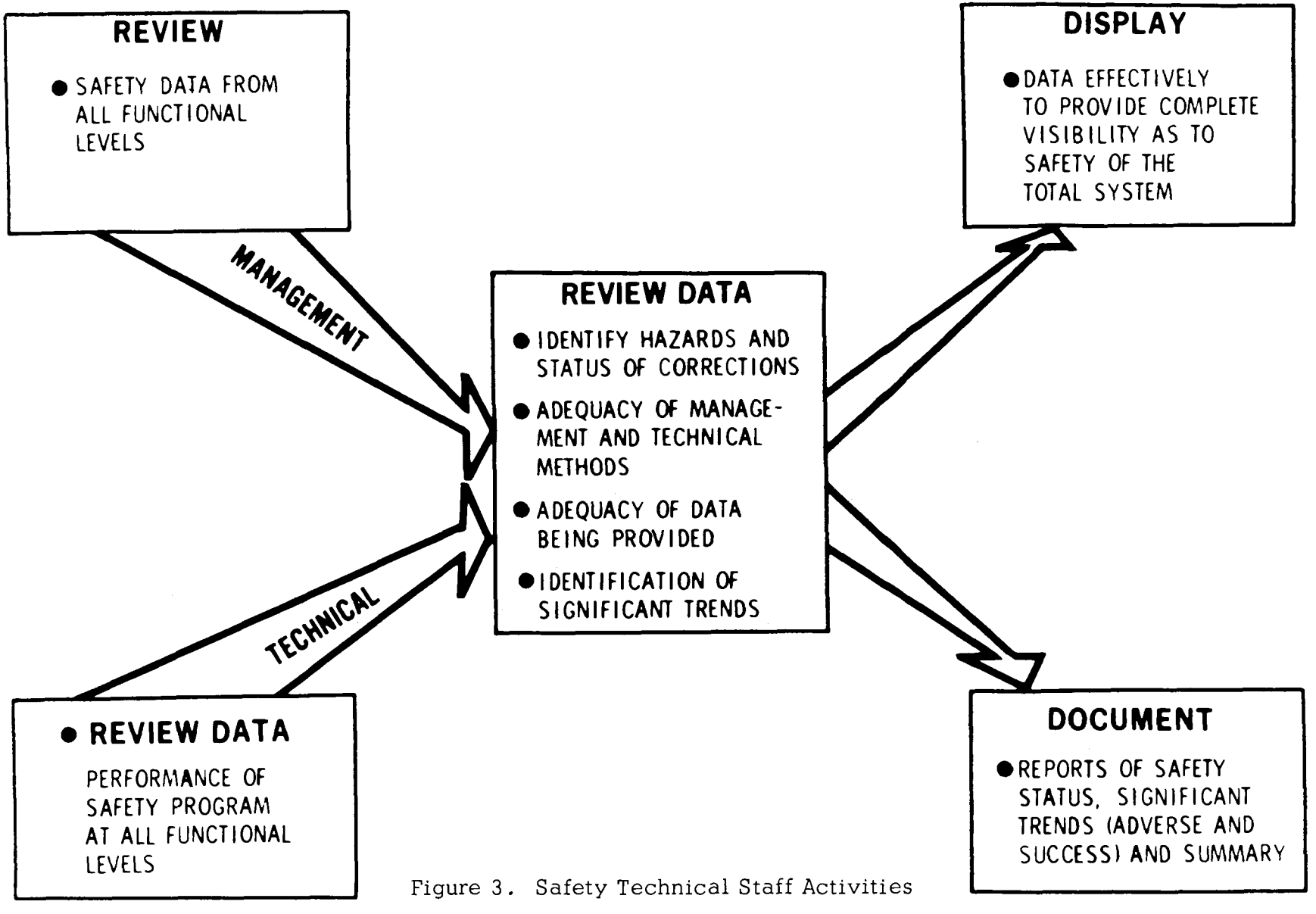


Figure 3. Safety Technical Staff Activities

The Safety Technical Staff's assessment of the safety program management adequacy will be founded on the objectivity, quality and quantity of the safety data, the efficiency of corrective action efforts, as well as actual safety program review activities. The Safety Technical Staff displays the results of its evaluations such that the Panel can clearly see the overall program hazards, assign priorities to them based upon program impact, and recommend appropriate corrective action.

Safety Data Acquisition

The relationship between safety visibility and data quality is self-evident in that the use of poor data results in restricted visibility and leads to erroneous or invalid conclusions. The quality and objectivity of the safety visibility developed by the Safety Technical Staff is completely dependent upon the proper selection of the basic data. This can best be outlined by Figure 4, which plots safety visibility against data quantity. This illustration indicates that there is a specific quantum of data which is inconclusive in nature and would yield very little visibility. Above this point, as data is acquired and correlated, visibility increases sharply to an optimum point. Finally, there is a point at which increased data yields but little additional visibility to support the decision-making process.

Safety data must originate at the contractor functional safety level in conjunction with performance of the basic safety program elements and reported on a closed loop manner as shown in Figure 5. Also shown in some detail are the safety activities that should be accomplished during the design, manufacture, test and operations phases. Figure 6 shows safety inter-relationships and data flow. Boxes I and II indicate the contractor/center working relationship. Reports, analyses, and identified hazards flow from the contractor to the Center; and requirements, program monitoring and corrective action flow from the Center to the Contractors. Thus, basic decisions and corrective actions are made at the lowest possible level in the area of design responsibility. This chart also shows safety data flowing from the Centers to the Safety Technical Staff. These data taps are located at the strategic control points of the NASA safety organization where the most effective data acquisition can be accomplished. Boxes II and III describe typical Center-Headquarters Program Office working relationship in that reports, analyses and corrective action recommendations flow from the Center to the functional Headquarters Office, while requirements, monitoring and corrective actions flow to the Centers. Decisions affecting one or more Centers, which cannot be made at the Center level, are developed at the Headquarters Program Office level. Data also flows from this Safety Office to the Safety Technical Staff.

This process allows data to be obtained from the functional levels with a minimum of handling, which is mandatory if the Panel is to function in the independent manner intended by the Congress.

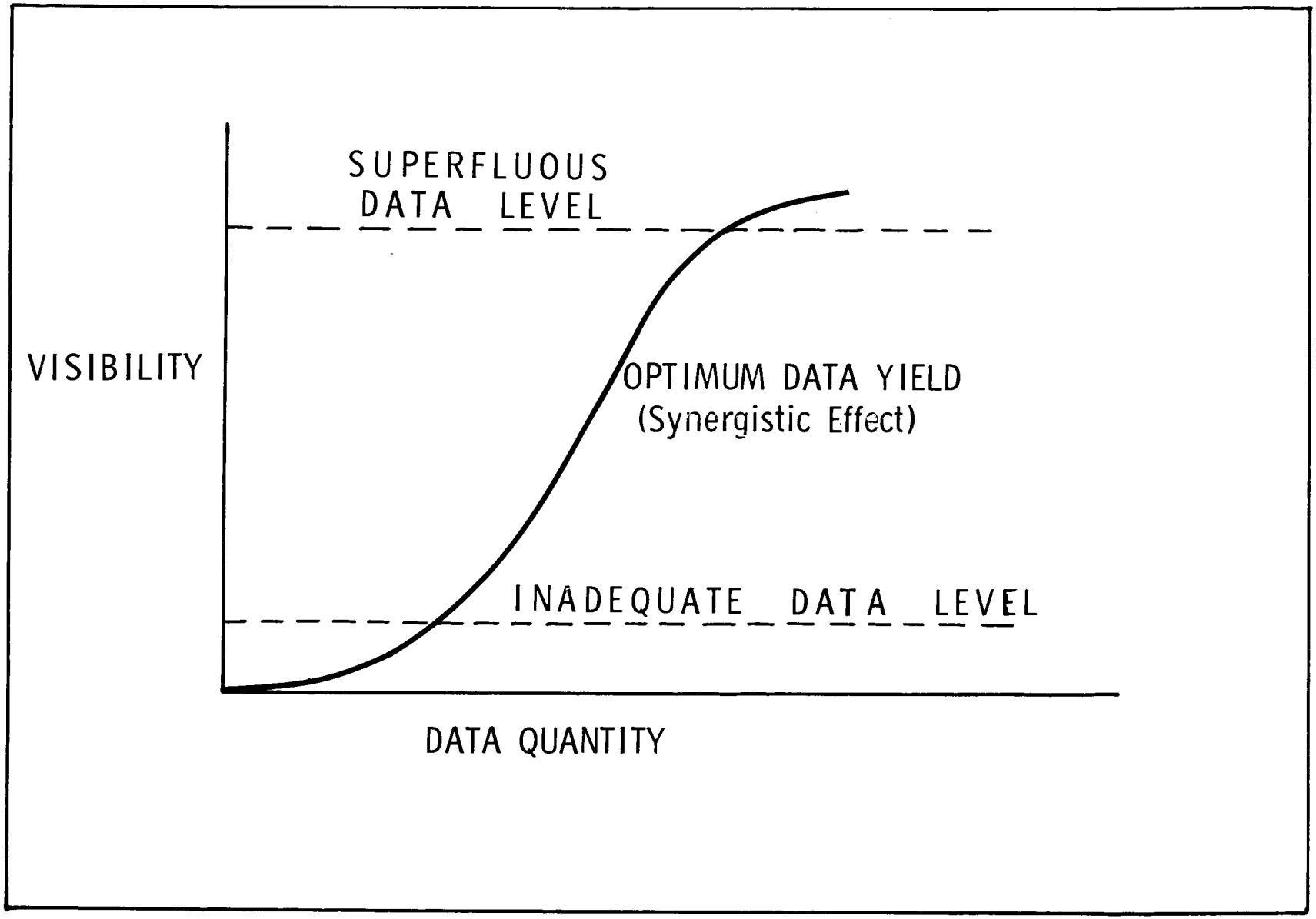


Figure 4. Safety Data Acquisition

DESIGN

1. SAFETY PLANNING PREPARED
2. SUPPORT TRADE-OFF STUDIES
3. FACILITIES DESIGN
4. SAFETY ANALYSES
   - DESIGN
   - PROCEDURES
   - HARDWARE
5. IDENTIFY SAFETY FEATURES
6. IDENTIFY CRITICAL
   - SYSTEMS
   - SUBSYSTEMS
   - COMPONENTS
   - OPERATIONS
   - TESTS
   - MATERIALS
7. REVIEW MISSION CONTINGENCY, RECOVERY & RESCUE PLANS
8. DETERMINE
   - HAZARDS
   - ANOMALIES
9. DESIGN REVIEW SUPPORT
10. RECOMMEND CORRECTIVE ACTION
11. REPORT
    - HAZARDS
    - CORRECTIVE ACTION
    - EFFECTIVENESS
12. SAFETY DATA MANAGEMENT
13. SAFETY ASSURANCE

MANUFACTURING

1. SAFETY INPUT TO MANUFACTURING PLANS
2. IDENTIFICATION OF CRITICAL OR HAZARDOUS MANUFACTURING ACTIVITIES
3. IDENTIFICATION OF HAZARDOUS MATERIALS OR PROCESSES AND SPECIAL HANDLING REQUIREMENTS
4. CONCUR IN CONTINGENCY AND RECOVERY PLANS
5. CERTIFICATION OF PERSONNEL PERFORMING CRITICAL MANUFACTURING TASKS
6. SAFETY EVALUATION OF CHECKOUT AND CALIBRATION TECHNIQUES AND EQUIPMENT
7. HARDWARE AND PROCESS INSPECTIONS
8. FAILURE OR ACCIDENT REPORTS
9. SAFETY ASSURANCE

TEST

1. SAFETY INPUT TO TEST PLANNING
2. IDENTIFICATION OF CRITICAL OR HAZARDOUS TESTS
3. ANALYSIS OF SPECIAL HANDLING OR EQUIPMENT REQUIREMENTS
4. CONCUR IN CONTINGENCY AND RECOVERY PLANS
5. CERTIFICATION OF TEST CONDUCTING PERSONNEL
6. SAFETY ANALYSIS OF FAILED COMPONENTS AND TEST PROCEDURES
7. FAILURE OR ACCIDENT REPORTING
8. MONITOR TEST OPERATIONS
9. SAFETY ASSURANCE

OPERATIONS

1. SAFETY INPUTS TO OPERATIONS PLANNING
2. IDENTIFICATION OF CRITICAL OR HAZARDOUS OPERATIONS
3. COORDINATE RANGE SAFETY REQUIREMENTS
4. ANALYZE PROCEDURES
   - OPERATION
   - CHECKOUT-VALIDATION
5. CONCUR IN CONTINGENCY AND RECOVERY PLANS
6. CERTIFICATION OF OPERATION AND MAINTENANCE PERSONNEL
7. PARTICIPATE IN GO-NOGO-ABORT DECISIONS
8. FAILURE OR ACCIDENT REPORTS

Figure 5. Joint Center - Contractor Safety Activities During Major Program Phases

SAFETY INTERW

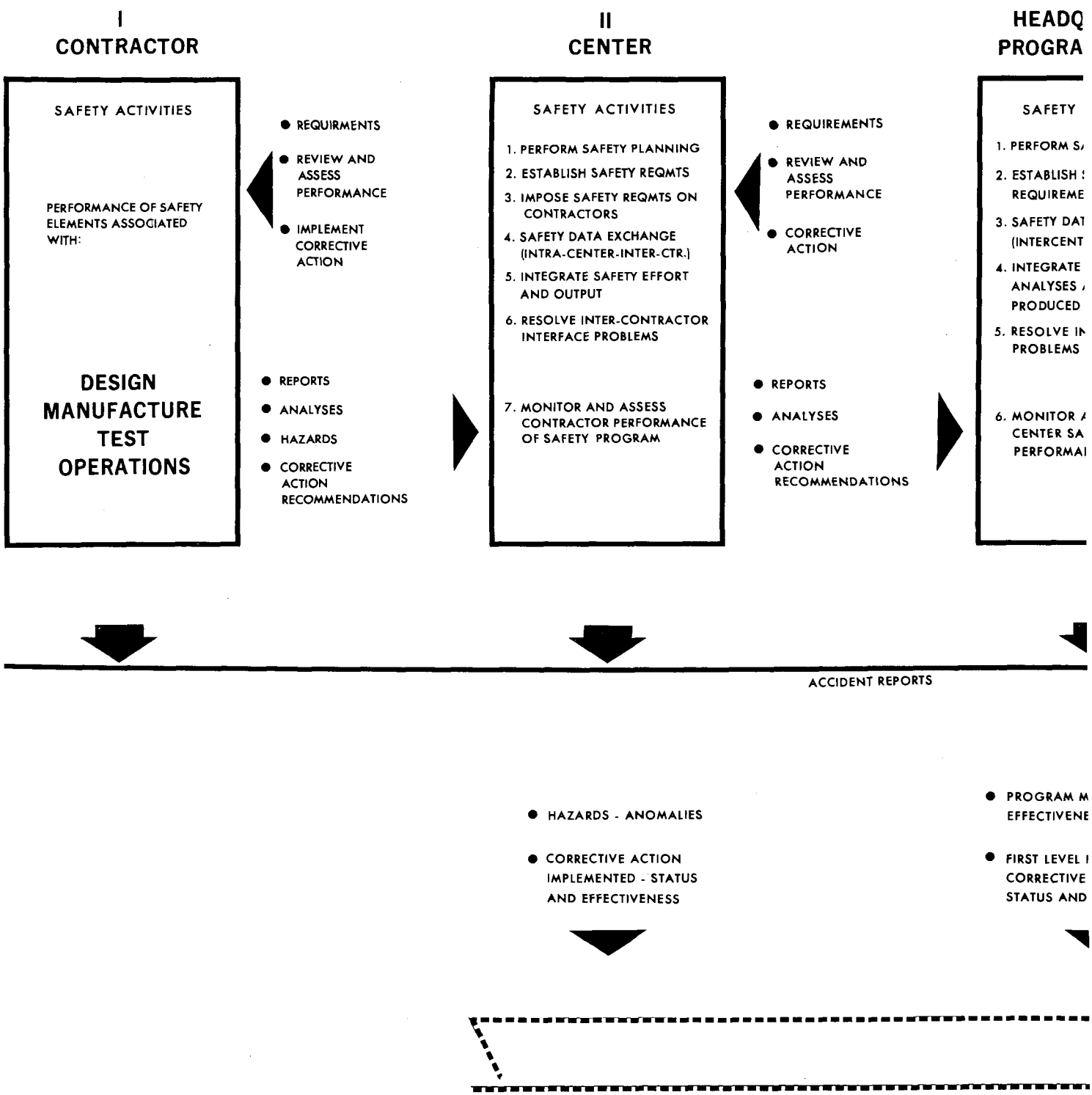


Figure 6. SAFETY

FETY INTERWORKING RELATIONSHIP AND SAFETY DATA FLO

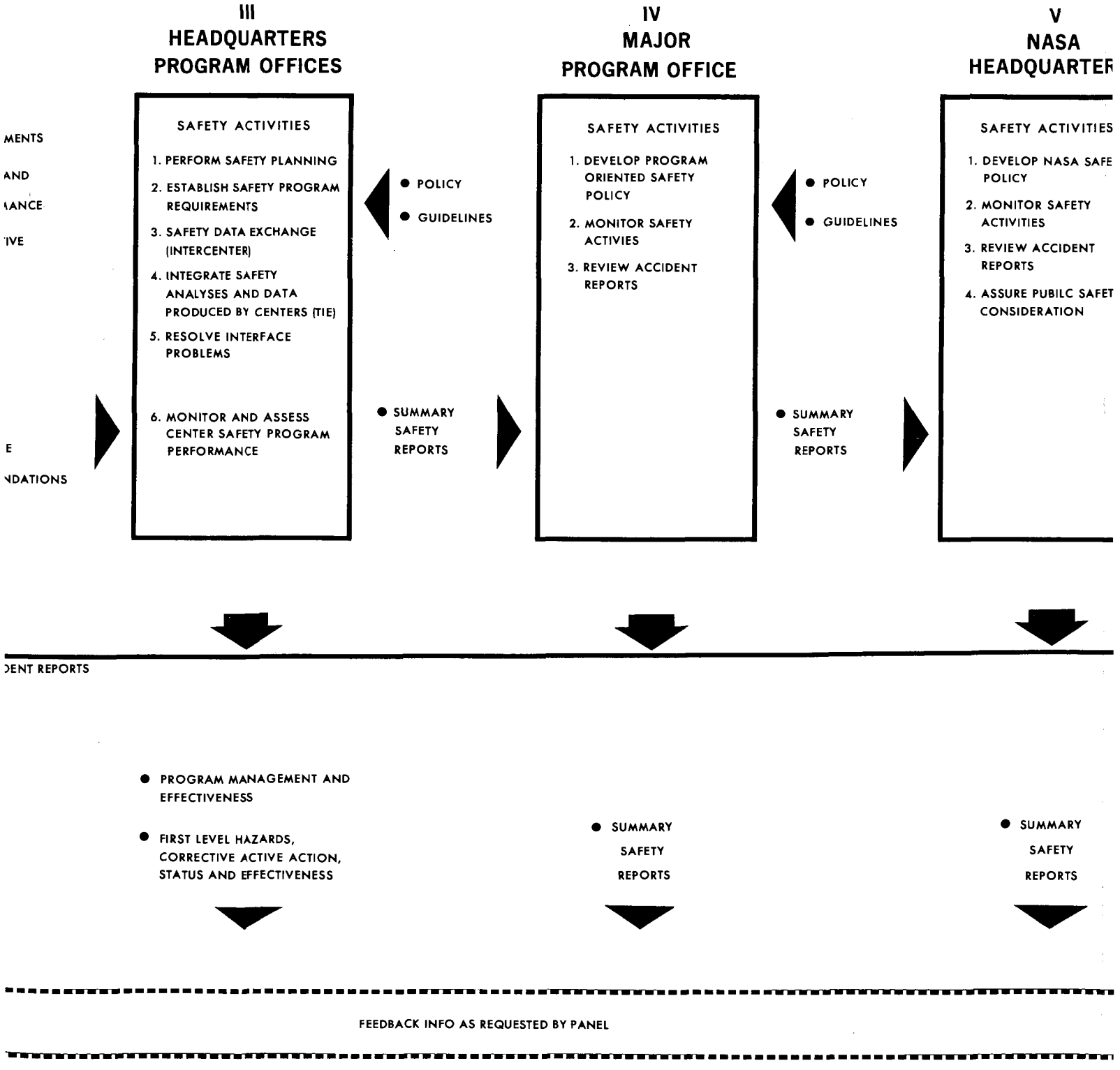
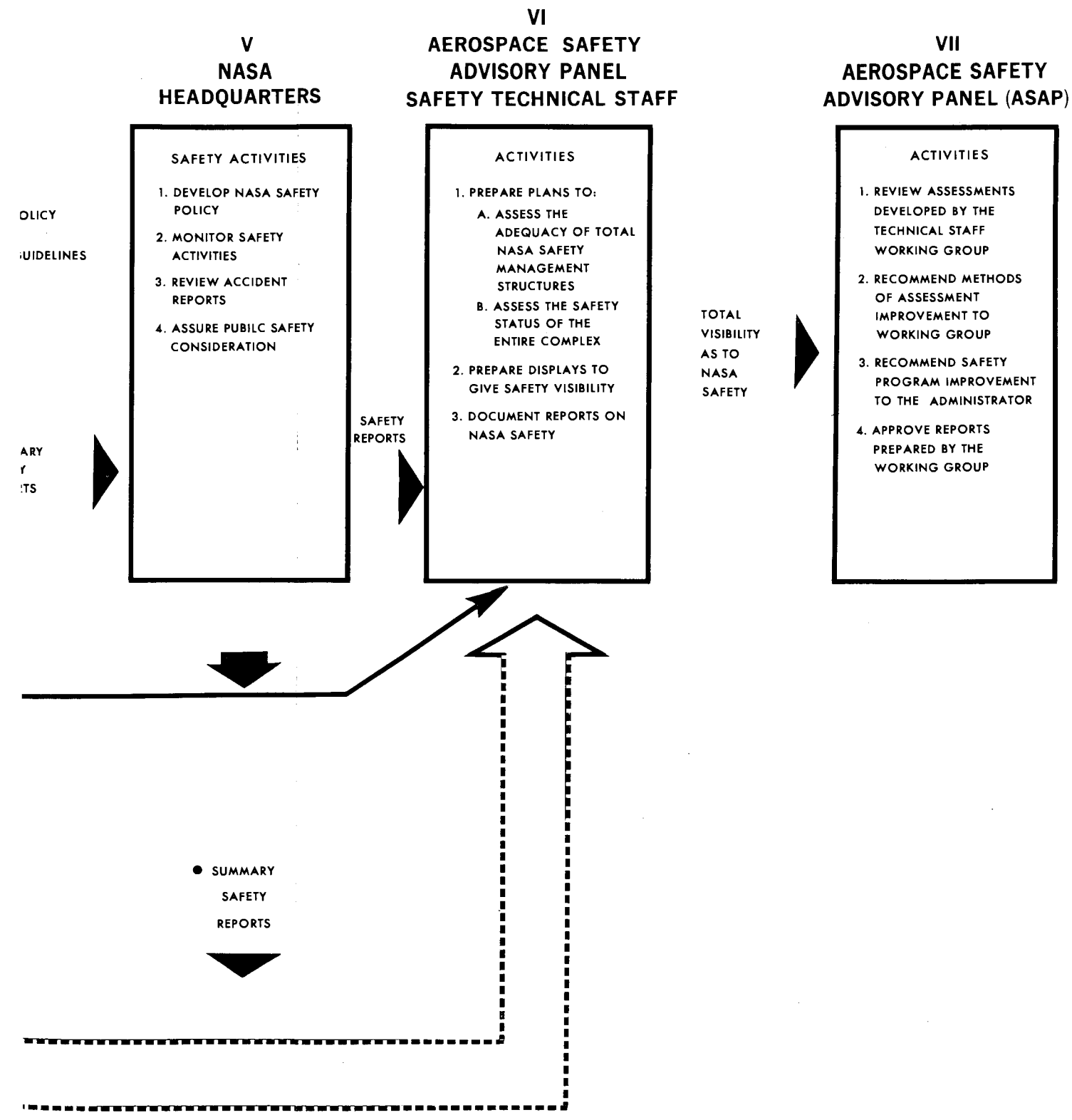


Figure 6. SAFETY INTERWORKING RELATIONSHIP AND SAFETY DATA FLOW

18C

FETY DATA FLOW



OW

Figure 7 is an example of the typical data content that would be required by the Safety Technical Staff. The form would describe hazards identified both in hardware and software.

Figure 8 shows the types of safety data that should be provided as a basis for identifying hazards and reporting their resolution, as well as the means of clarifying the actual risks being incurred.

It should be noted that most of the Hazard Identification Reports will result from the safety analyses, although this does not preclude the origination of reports from the other functional safety activities.

Using the principle of safety evaluation by exception, only the system hazards are identified and reported. These Hazard Identifica- Reports may be accompanied by segments of the safety analyses by which they have been identified, if required by the Panel.

Figure 9 includes the elements of the Safety Analyses and shows that each aspect of the development and operation of the system is included and considered.

Figure 10 is a typical sequence of events chart that describes how the planning, implementation, analyses, corrective action and reporting activities would inter-relate in the Manned Space Flight organization, beginning with the Safety Technical Staff and extending to the contractor level.

The development of the planning and technical methods to be used for the functional safety program is a NASA responsibility. The Aerospace Safety Advisory Panel is responsible for assessing the adequacy of these activities and methods.

Safety Data Processing

Each staff member must develop requirements to be imposed on his safety director counterpart for data processing. This should include such activities as:

1. Hazard reporting and risk identification
   a. Supporting analyses
   b. Corrective action schedule
   c. Program impact information (cost and schedules)
   d. Corrective action responsibility
   e. Closeout or resolution

2. Accident reporting
   a. Where and when
   b. Estimate and description of damage
   c. Personnel injuries
   d. Possible causes
   e. Conditions (operating, weather, etc.)
   f. Operation being performed

NOTE: This is a serially numbered report. It should be logged out by Contractor and logged in by Center Safety Office. Close out will be shown by having both reports in Center Safety file.

HAZARD IDENTIFICATION REPORT	REPORT NO. IDENTIFICATION
USE REPORTING OF HAZARDS IDENTIFIED BY SAFETY ANALYSIS, SAFETY REVIEW, SAFETY SURVEILLANCE OR OTHER ENGINEERING ANALYSIS	REFERENCE

CLASSIFICATION OF HAZARD:

_____Catastrophic (cause system loss or death)
_____Critical (damage system or injury to personnel - require immediate corrective action)
_____Marginal (may degrade system performance but can be counteracted or controlled)

1. This report will be submitted to the Center Safety Office at any time a hazard has been identified and validated or corrected by the contractor. A copy of the analysis which identified the hazard will be kept on file at the Contractor Safety Office for review by the Center Safety Office.

2. This report will include the following information:

   (a) Description of the item analyzed (flight hardware, associated ground equipment, facility, procedure or personnel qualification)
   (b) Description of the hazard
   (c) Probability of occurrence
   (d) System exposure to the hazard
   (e) Corrective action recommendations
   (f) Estimated schedule for correction
   (g) Office responsible for corrective action

3. When used for close out of a corrective action this report will also include:

   (a) Date corrective action effective
   (b) Changes made to designs, contracts, shelf stores, drawings, Change Board results; etc.
   (c) Cost of corrective action
   (d) Office primarily responsible for closeout

_____ Originated by:

_____ Signature of Responsible Safety Manager

Phone _____ _____
Area Code Number

NASA FORM

Figure 7. Typical Safety Data

SYSTEMS SAFETY DATA FLOW

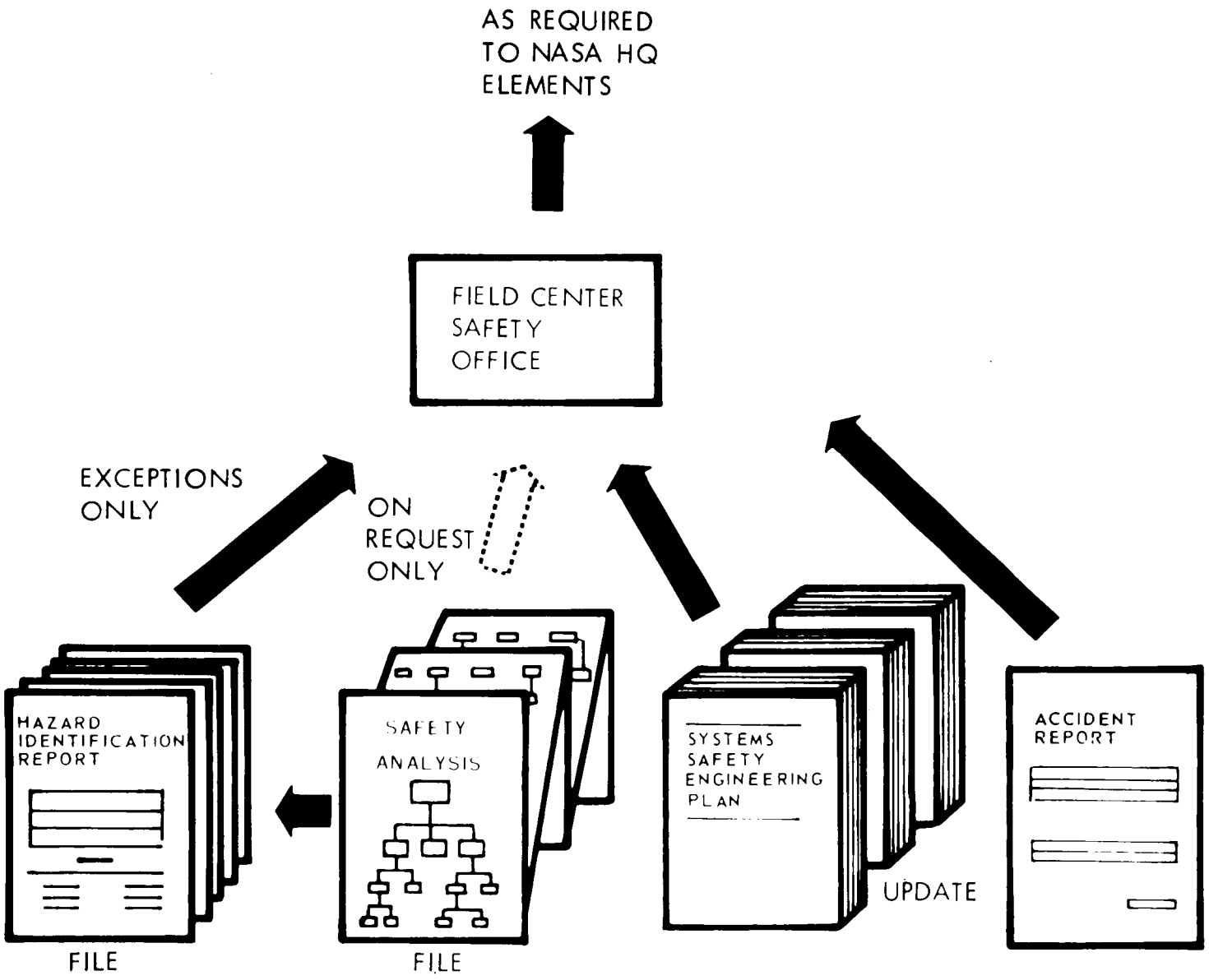


Figure 8. Systems Safety Data Flow

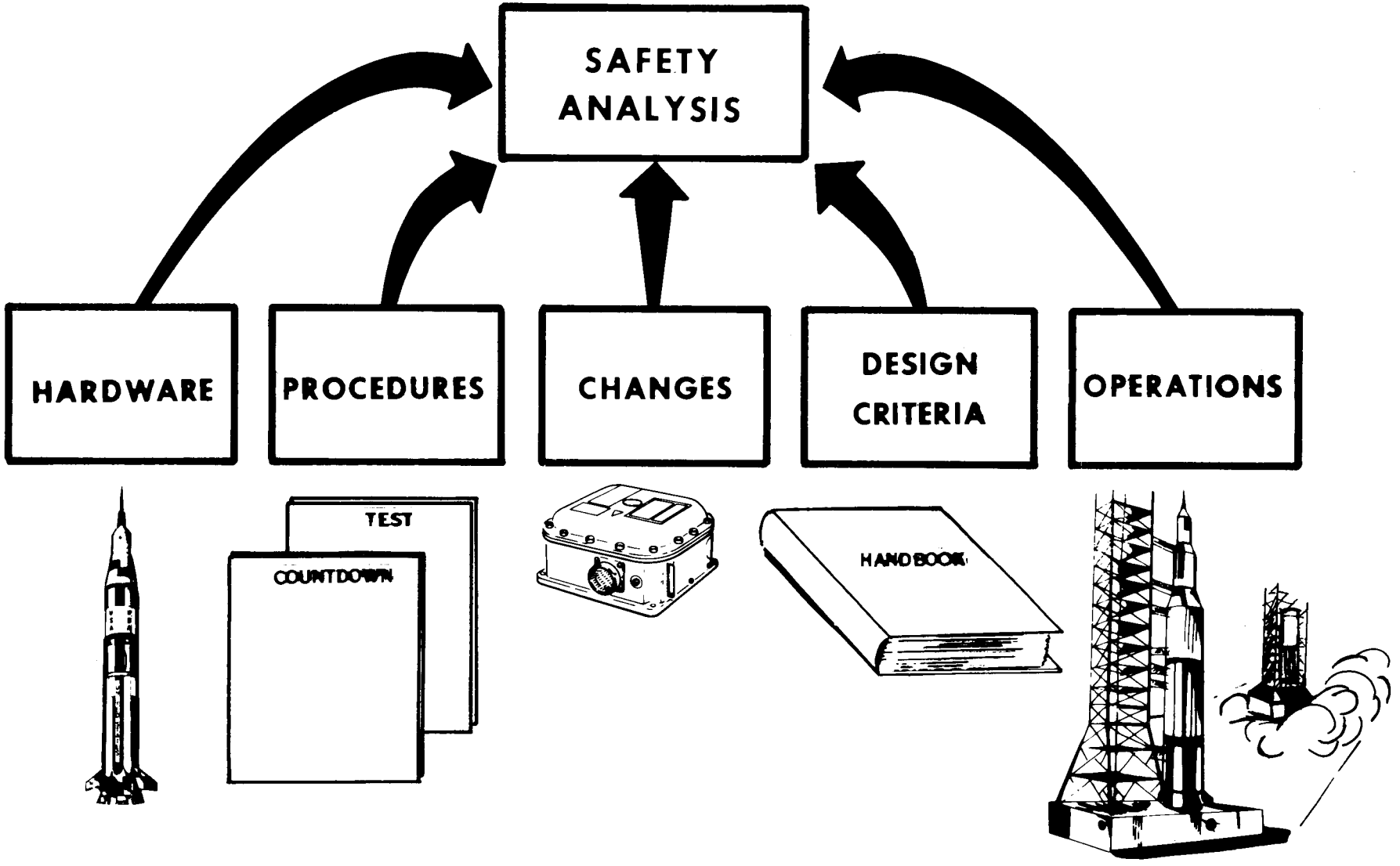


Figure 9. Elements of Safety Analysis

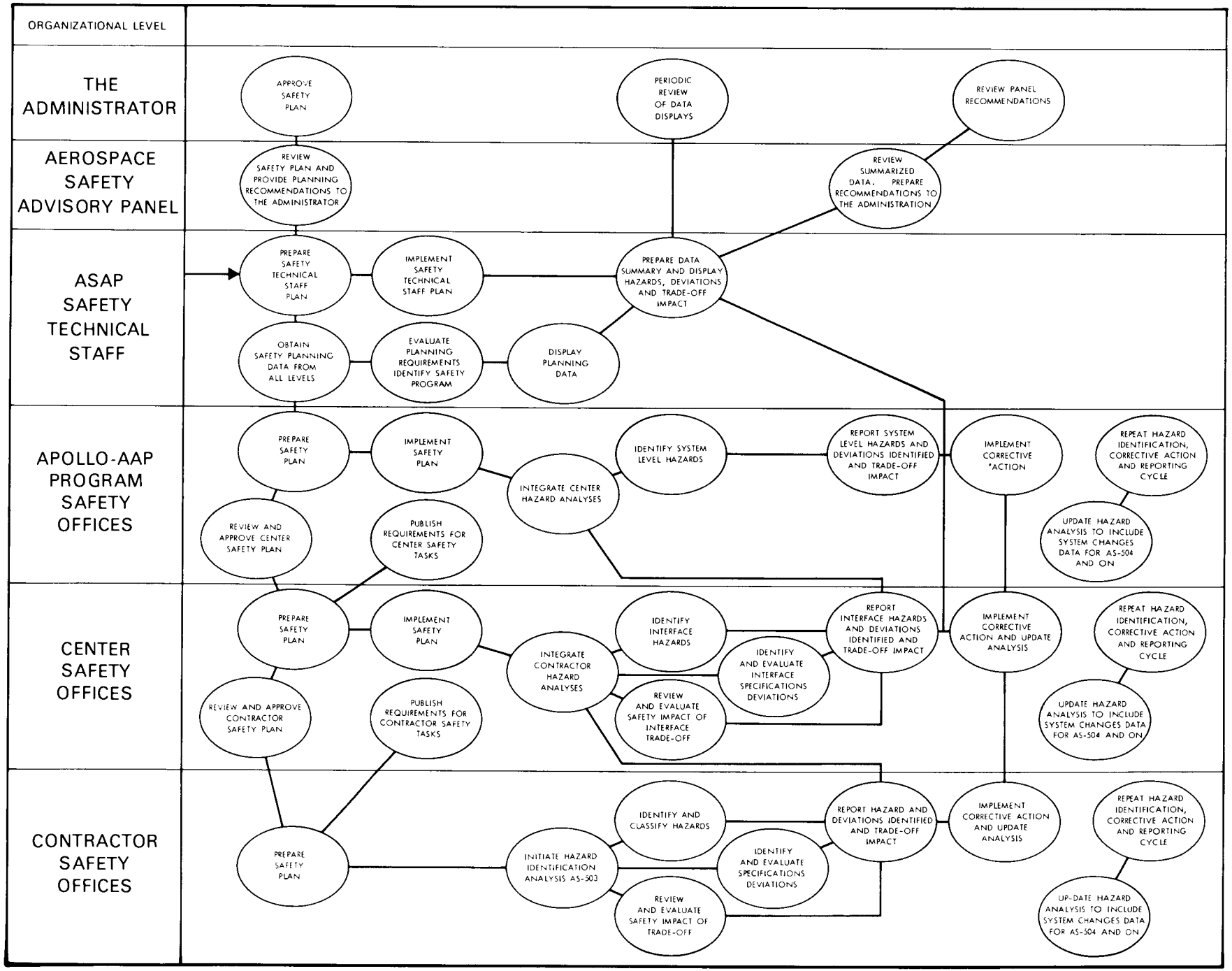


Figure 10. Safety Activity Interrelationship

3. Status of recommendations for changes proposed by the Panel and approved by the Administrator, together with reports on the effectiveness of the change

4. Data retention and retrieval support

5. Support in the performance of trend analyses which consists of a periodic review of acquired data to identify significant adverse trends and success paths

   Adverse trends - analysis of the correlated data indicates that a particular design feature or sequence of operations are frequently or repeatedly identified as system hazards

   Success paths - Analysis of the correlated data indicates that certain management or technical methods, a design feature or sequence of operations that is consistently hazard free

These recommendations for safety data submittal and evaluation have been structured in simplest yet most effective way possible. Each staff member must develop his own techniques for random, on-site reviews to assure the validity and objective of the data he receives.

Further, the staff member must assure this data is processed and compiled into a format that will provide both the Panel and the Administrator with accurate and timely visibility of the safety program.

SECTION IV

SAFETY DATA PRESENTATION

Presentation of the safety data developed during the initial review and subsequent sustaining program must serve three purposes:

1. The data must make available to the Administrator comprehensive, timely information that provides visibility of the safety of the system in terms of:

    a. Hazards identified
    b. Status of hazard resolution action
    c. Program risks vs program impact (i.e., risk levels/cost and schedule)
    d. Status of recommendations for correction by the Panel and approved by the Administrator
    e. Other information as may be required by the Administrator

2. The data must be presented to the Panel during its periodic meetings so that there can be an immediate determination of what the program inadequacies are and the corrective action that needs to be recommended. This presentation of data could be in the following format:

    a. Identification of recommendations resulting from preceding meeting
    b. Status of all recommendations prepared to date with regard to implementation
    c. Feedback information as to the effectiveness of recommendations implemented previously
    d. Identification of current program inadquacies
    e. Background data sufficient to lead to decisions for new recommendations

3. The data must be compiled into periodic (semi-annual) reports for retention purposes

This system may be supplemented by engineering drawings, analyses, documents, specifications and reports as may be required to project total safety visibility.

Certain refinement of these techniques should be developed to satisfy special situations as they arise.