MM 1700.2
MARCH 12, 1968

X.15

GEORGE C. MARSHALL SPACE FLIGHT CENTER

system safety plan

INDUSTRIAL OPERATIONS

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

NASA

MSFC - Form 454 (Rev October 1967)

This plan describing the System Safety activities to be conducted by Industrial Operations, Marshall Space Flight Center, is hereby adopted and will be implemented by all program offices in an expeditious and practicable manner.

Edmund F. O'Connor
Director, Industrial Operations

PREFACE

This system safety plan provides guidelines for the implementation of the program-oriented system safety effort for all Marshall Space Flight Center programs managed by Industrial Operations. It includes the identification of responsive organizational elements that will develop the effort leading to detection and identification of hazardous situations. Organizational elements include an Industrial Operations System Safety Office, a system safety activity within each program office, and an identifiable system safety activity within each prime contractor's organization that is responsive to the program offices. Provisions are included for a system safety overview serving to identify to all levels of management the hazards that are detected and corrective action recommendations.

Considerable effort has been expended at this Center to achieve success for the Saturn program, and to a great extent system safety is inherent in the design, development, and operation of these systems. The function of this plan is to recognize in a consistent manner this system safety effort as a discipline and as such to penetrate to a greater depth the system safety problem and to make every reasonable effort to assure the uniform application of system safety methods. Maximum use of available test data and analytical material will be made in the accomplishment of the system safety objectives.

TABLE OF CONTENTS

SYSTEM SAFETY PLAN
INDUSTRIAL OPERATIONS
MARSHALL SPACE FLIGHT CENTER

SECTION 1: INTRODUCTION

1.1 PURPOSE

The purpose of this document is to set forth the Marshall Space Flight Center Industrial Operations plan containing guidelines to be followed in organizing the system safety functions to be performed by the Industrial Operations System Safety Office, the program office system safety activities and the coordinated methods for the accomplishment of these functions.

1.2 SCOPE

This plan presents the major considerations for implementing and assessing a total system safety program for all development programs for which Industrial Operations, Marshall Space Flight Center, is responsible.

1.3 SYSTEM SAFETY DEFINITION

A discipline oriented toward the total system that functions to identify and control all hazards or out-of-sequence events which, should they occur within the total launch vehicle system during design, manufacture, handling, transportation, storage, test or operation activities, would cause loss of the system, the mission or the crew.

1.4 AUTHORITY

Apollo Directive 31, September 6, 1967, subject: Apollo System Safety Program Requirements.

1.5 RESPONSIBILITY

The Center Safety Office reporting to the Center Director has the overall responsibility for determining general policies and guidelines as relates to system safety, industrial safety and public safety. The Industrial Operations System Safety Office will function under the general policies and guidelines of the Center Safety Office. The System Safety Office, Industrial Operations, will respond to directives originating in the Program Offices, MSF. The participation and involvement of Research and Development Operations in the formulation of system safety requirements, their implementation and surveillance will be assured through existing program channels and agreements. Within Industrial Operations the system safety functions will be accomplished with minor organizational adjustments as described in Section 8.

SECTION 2: SYSTEM SAFETY REQUIREMENTS

2.1 GENERAL

The objective of system safety is to minimize the occurrence of failures and malfunctions by providing the greatest possible freedom from abnormal or out-of-sequence events that could cause the loss of the crew, the launch vehicle, or the mission.

System Safety Elements will be applied to all areas requiring system safety analysis within every phase of development and operation of the vehicle and related equipment.

2.2 SYSTEM SAFETY ELEMENTS

The basic elements of system safety analysis comprise the areas of Design Criteria, Procedures, Engineering Changes, System Logic Analyses, and Operational Safety. Maximum use of available development data and analytical material will be made in the incorporation of these elements. Application of these elements as a part of the decision making processes should provide maximum program safety visibility.

2.2.1 DESIGN CRITERIA

The system safety criteria established for each program by the cognizant program office will be identified, listed and submitted to the Industrial Operations System Safety Office as it becomes available. (Reference TMX 53563, System Safety Handbook). These criteria will be used as:

a. A basis for a program review to determine uniformity of application.

b. A criteria source for all new programs and studies.

c. A contributing part of the system safety baseline.

2. 2. 2 PROCEDURES

Procedures for operations, test, checkout, handling, launch and others pertaining to the launch vehicle will be reviewed as developed to assure that they are adequate with respect to system safety and that no procedure-to-procedure or procedure-to-hardware conflicts exist. Procedures will be selected for review based on the following selection criteria:

a. System areas where the application, removal or existence of energy (electrical, chemical, kinetic, potential, thermal) can create a hazard due to personnel error or procedure inadequacy.

b. System areas where the loss of control or monitoring capability will create a hazard to personnel or hardware.

c. Tests or operations which create environmental conditions hazardous to personnel or hardware.

d. Functions involving critical operations limits which, when exceeded, will create a hazard to personnel or hardware.

Procedures, software, interfaces and special requirements will be reviewed to determine if they include the following: (Reference TMX 53664, System Safety Criteria for Use in Preparation of Reviews of Procedures.)

a. Procedures-to-requirements correlation

b. Procedures-to-hardware correlation

c. Hazardous step and/or warning adequacy

d. Sequence critical identification

e. Failsafe/backout capability

f. Emergency procedure adequacy

g. Redline/critical-dates display

h. Interlock/automatic abort provisions

i. Time, cycle, retest limitations

j. Measures to offset human error

k. Interface control existence for all critical elements

l. Open work closeout procedure/test procedure update capability.

m. Other requirements as may be determined

Procedures governing hazardous activities such as high pressure, high temperature, hazardous materials handling, or close-space crew-proximity will be identified and subjected to a detailed safety review prior to use.

2.2.3 ENGINEERING CHANGES

Engineering change proposals will be reviewed at the program system safety level against the logic diagrams or equivalent analyses to determine the effect of the engineering changes on the safety of the system. Any changes in risk level inherent in an engineering change should be identified to the Change Board as one of the parameters on which the Change Board bases its decision as to the desirability of incorporating this change. This will assure that the safety of the system is not degraded.

2.2.4 SYSTEM LOGIC ANALYSES

2.2.4.1 SCOPE OF ANALYSES

A system safety design analysis will be conducted as directed by the Program Director to assure that hazards inadvertently designed into the system are identified and removed or that risk levels are clearly understood by NASA management. The results of the analytical method employed will be in a format that is suitable for integration into a total systems analysis. The following will be accomplished:

a. The analyses will consist of a "top down" or equivalent logical identification of hazardous situations and the hazard

categories that might cause these situations. Undesired events will be prioritized and a determination of those undesired events will be made for which a logic diagram is to be constructed. Analyses will be performed for each of the selected undesired events with special attention devoted to inter-functional relationships and cascading faults.

b. Analyses will be conducted where practicable of vehicle and GSE functional systems and subsystems.

2.2.4.2 TECHNIQUE AND METHODS

The preferred technique and methods of system logic diagramming are discussed in Appendix B.

2.2.5 OPERATIONAL SAFETY

Operations is that aspect of the total system safety effort that interrelates the results of analytical studies and test results with procedures and personnel/hardware interfaces. Areas of concern are those that control and describe the functions necessary for manufacture, test, checkout, transport, storage, launch, and mission accomplishment. These functions are briefly described as follows:

a. The conceptual and design activities will be surveyed to assure that safety criteria are correctly applied and are suitable for use. There will be participation in trade studies to assure safety is not compromised. High risk or hazardous systems will be identified and work-arounds (such as alternative designs, procedural changes, warning systems, etc.) developed where feasible.

b. Critical manufacturing areas will be identified, and each area will be evaluated by a study of manufacturing planning documentation. Manufacturing planning personnel will be informed of hardware and manufacturing processes that are critical to system safety. The manufacturing activities will be surveyed to assure that system safety inputs are followed and to identify any additional system safety requirements as they develop.

c. The transportation activities will be surveyed to assure that all equipment is handled properly and not subjected to undue stress or environmental conditions. Provisions will be made to assure that the proper environment is maintained, packaging is properly accomplished, and complies with applicable safety specifications, and labels are affixed to the outside of packages listing all special handling and storage instructions.

d. Checkout procedures will be reviewed prior to use to assure correlation with hardware configuration and calibration requirements to verify adequacy and accuracy, and to identify hazards and emergencies that

could arise. Redline values will be reviewed prior to checkout to assure that there are no anomalies between requirements and hardware capabilities. End-to-end checks will be conducted to determine incompatibilities and non-conformities, so that proper actions can be taken to minimize the risk during checkout and operations. End-to-end checks are performed after the required configuration baseline has been established and verified, and the procedures have been checked against the mission rules, specifications and criteria, and test requirements documents.

e. Storage activities will be monitored to assure that required environments and actual environments are compatible with system requirements and that all induced environments which may be hazardous in nature, have been adequately controlled. The system revalidation procedures, following removal from storage, will be reviewed with special attention devoted to all components with critical shelf life.

f. All test activities will be surveyed for compliance with system safety test criteria. Particular attention will be paid to all hazardous tests (e.g., those approaching or exceeding design limits) for documented warnings and recovery and backout procedures. Failed components will be analyzed for potential impact on the safety of the system. Diagnostic analyses based on the logic diagram analyses (2.2.4) or equivalent analytical methods will be used as required to support accident/incident investigations.

g. System safety personnel should participate in the analysis of cause and effect of all test failures and accidents/incidents related to flight and post flight operations. After investigation of failures and/or accidents a copy of the report of the pertinent details will be made through the channels of the system safety organization. These reports will be submitted on standardized forms to be provided by OMSF.

h. Personnel certification requirements relative to test and checkout functions shall be analyzed to determine both team certification and individual personnel certification. Personnel certifications will be monitored and specialized personnel training requirements will be initiated when required.

i. The potential mission operations hazards may be minimized by change in system design, operational procedures, mission rules, contingency action plans, etc.

2.3 SYSTEMS ENGINEERING

An interface between System Safety and Systems Engineering will be established to ensure the effective exchange of information. Such information will include top level drawings, descriptive documents, and functional flow diagrams as developed by Systems Engineering. System safety will make maximum use of this Systems Engineering documentation to assure the safety of the system.

2.4 QUALITY ASSURANCE

A functional interface shall be established with the quality assurance organization. Peculiar system safety requirements should be supplied to the quality assurance organization on a timely basis.

2.5 RELIABILITY

A system safety-reliability interface shall be established. System safety shall make maximum use of data from reliability analyses (failure mode and effect, and criticality) and Mean Time Between Failure (MTBF) calculations to be made available to support performance of the logic diagram analyses.

2.6 HUMAN ENGINEERING

A system safety-human engineering functional interface shall be established to assure the safety of the man-machine interface.

2.7 MAINTAINABILITY

A functional interface shall be established with the maintainability organization. System Safety shall provide inputs to the development of maintenance concepts, procedures, and analyses.

2.8 CONFIGURATION MANAGEMENT

A system safety-configuration management interface shall be established and a method shall be developed to notify the safety organization of any changes affecting the system safety baseline. Criteria shall be developed as a basis for designating the change as a safety change and cognizant system safety activity recommendations shall be made on changes which impact safety, prior to submittal to the Configuration Control Board.

2.9 INDUSTRIAL SAFETY

A system safety-industrial safety interface should be established to assure that no voids exist between the functions of the two organizations. While system safety is program oriented and industrial safety is facilities oriented, there are many areas of mutual interest such as during the testing and manufacturing activities. These are typical of interfaces that must be defined.

SECTION 3: CONTRACTORS' SYSTEM SAFETY ACTIVITIES

3.1 GENERAL

The following guidelines should be used by each Marshall Space Flight Center prime contractor to establish a system safety function within his organizational structure. This contractor system safety function will be responsible for assuring that system safety is implemented in all phases of program activities.

Specific requirements include at least the following:

a. The preparation of and submittal to the appropriate program office a system safety plan as required, responsive to and consistent with this document and any other requirements which may be imposed by the program office.

b. Assurance that subcontractors and suppliers comply as applicable with this document.

c. Provisions for supporting reviews of his conformance to system safety requirements and the performance of his subcontractors and suppliers for the purpose of determining the effectiveness of the system safety programs.

d. Identification and evaluation of hardware interfaces between design contractors and operating stage and GSE contractors with respect to system safety objectives.

3.2 SYSTEM SAFETY PLAN

The contractors system safety plan will identify his methods for applying the system safety program elements described in paragraph 2.2 as directed by the program manager. It will include a detailed description of the management and technical methods that will be used in the implementation of system safety in these areas including a schedule for completion keyed to major program milestones. It is suggested that the system safety plan include the following: (Reference TMX 53612, The System Safety Program for a Total Space Launch Vehicle General Requirements).

a. A description of the contractors' system safety organization with responsibilities including functional relationships.

b. Organizational reporting lines showing authority and relationships of system safety to other functions, e.g., engineering, quality, test, reliability, etc.

c. Safety criteria for design of equipment to minimize hazards.

d. Considerations for crew safety, range safety, pad safety, and mission operations.

e. Component, subsystem and system safety analyses.

f. Review of design changes to identify possible hazards.

g. Analyses of maintainability concepts for existence of safety hazards.

h. Analysis of test equipment for possible hazards.

i. System safety review of procedures for inclusion of system safety considerations, e.g., test, operation, storage, transportation, and accident investigation plans.

j. Training and certification of personnel in critical job categories.

k. Failure report screening for system safety impact.

l. Participation in design activities.

m. System safety training.

n. System safety audits.

o. Milestone schedule for accomplishment of the system safety program.

p. Support for the NASA-contractor system safety network.

SECTION 4: DATA MANAGEMENT

The program office system safety activity will formulate recommendations for system safety data to be submitted by contractors. The recommendations will include the title of each system safety document to be submitted, the number of copies to be submitted, the frequency of submittal, the distribution, and a description of the purpose and content of the document. Each document so recommended will fall within Documentation Category 11, Safety (Code SA), as defined in Apollo Documentation Administration Instruction, NPC 500-6. Upon approval by the cognizant project manager, action will be initiated to acquire the data. If formal data management is in force in a contract, the required system safety data will be itemized on a Data Requirements List (DRL) and described in supporting Data Requirement Descriptions (DRD's).

The program offices' system safety activities will furnish system safety data to other NASA centers in accordance with the provisions of current inter-center agreements.

The Industrial Operations System Safety Office will make the fullest practicable use of available center data management techniques in the storage, control, and distribution of system safety data.

SECTION 5: PROGRAM PECULIAR REQUIREMENTS

5.1 GENERAL

It is the purpose of the plan to provide safety program requirements that are applicable to all of the Industrial Operations programs. There are certain requirements which are unique to each program. These are listed as follows:

5.2 SATURN IB PROGRAM

The system safety program developed by the SIVB and IU contractors will satisfy the requirements of both the Saturn IB and Saturn V program, in other than a few unique instances. Accordingly, the only additional requirements would be the SIB stage and the ground support equipment for which Marshall Space Flight Center is responsible. The vehicle systems integration contractor will assist the program office system safety effort as required.

5.3 SATURN V PROGRAM

The system safety program developed by the SIVB and IU contractors will satisfy both the Saturn IB and Saturn V program requirements. The additional requirements will include the SII and SIC stages and their related ground support equipment for which Marshall Space Flight Center has responsibility.

Integration of the Saturn V system safety program as performed by the System Evaluation & Integration contractor shall serve a dual purpose. It shall satisfy the Saturn V program requirements as defined herein and as contained in Apollo Program Directive 31, and it shall support the integration of the total Apollo system safety program as being performed under the Apollo Safety Director.

5.4 APOLLO APPLICATIONS PROGRAM

The system safety effort as performed by the Apollo Applications Program in response to this plan shall be structured to make maximum use of the safety data and analyses originated by the Saturn program. This safety effort shall be structured to assure that experimental AAP systems and subsystems have been fully analyzed as described herein. This is to determine that the AAP hardware will not create unacceptable risks or hazards for the Apollo/Saturn System by its incorporation into that system.

5.5 ENGINES

The Engine system safety program performed in association with this plan shall satisfy the overall safety program requirements of both the SIB and the Saturn V systems.

SECTION 6: IMPLEMENTATION

6.1 GENERAL

The provisions of this plan will be imposed within each Marshall Space Flight Center program at the earliest possible time. A copy of each contractor's system safety plan or equivalent will be submitted to the Industrial Operations System Safety Office prior to approval by the program office.

6.2 REVIEWS KEYED TO PROGRAM MILESTONES

The Industrial Operations System Safety Office and the program office system safety activities will participate in milestone reviews, provide system safety status information, and will assure that system safety interfaces are maintained with other disciplines, such as engineering, quality, reliability, and test. Milestone reviews are conducted at critical points in the program development cycle to assure the requirements of this plan are being accomplished adequately. The program office will assure inclusion of system safety considerations that are consistent with this document in each review. These program milestone reviews are:

a. Preliminary Design Review (PDR)

b. Critical Design Review (CDR)

c. First Article Configuration Inspection (FACI)

d. Certification of Flight Worthiness (COFW)

e. Design Certification Review (DCR)

f. Pre-Flight Review (PFR)

g. Flight Readiness Review (FRR)

7.0 REPORTING AND REVIEW

The Industrial Operations System Safety activities shall utilize standard programmatic reporting and review procedures for reporting all safety progress and activities.

SECTION 8: ORGANIZATION

8.1 STRUCTURE AND REPORTING LINES FOR INDUSTRIAL OPERATIONS

This plan provides for the incorporation of appropriate system safety activities into the existing organizational structure of Industrial Operations, and is consistent with guidelines and criteria established by the Marshall Space Flight Center Safety Office.

Functional elements should be identified and reporting lines established as indicated in Figure 1.

8.1.1 INDUSTRIAL OPERATIONS SYSTEM SAFETY OFFICE

A staff office for system safety will be established within Industrial Operations, Marshall Space Flight Center, and will report to the Assistant Director for Engineering, Industrial Operations. The role of this office is to provide policies and guidelines and to coordinate the system safety activities performed by each of the program offices into an effective integrated safety program within the framework of guidelines and policies established by the Marshall Space Flight Center Safety Office.

8.1.2 PROGRAM OFFICE

A system safety engineering activity will be established within each existing program office and in any future program offices established within Industrial Operations, Marshall Space Flight Center. The role of this activity is to implement the functional system safety plans and requirements in accordance with program needs.

8.1.3 MISSION OPERATIONS OFFICE

A system safety engineering activity will be established in the Mission Operations Office.

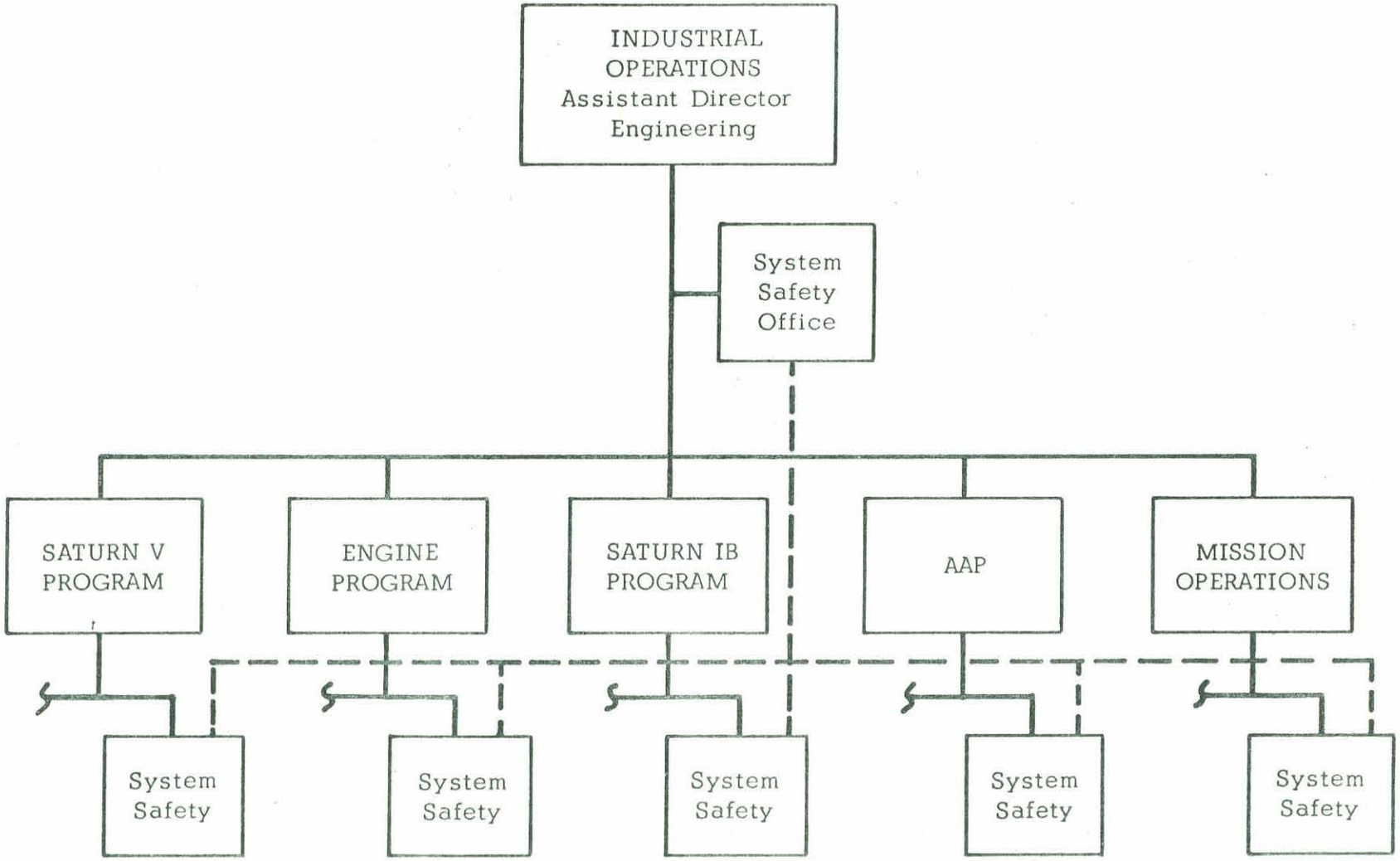


Figure 1. INDUSTRIAL OPERATIONS SYSTEM SAFETY FUNCTIONAL RELATIONSHIP

8.2 RESPONSIBILITIES AND FUNCTIONS

The responsibilities and functions of various organizations of Marshall Space Flight Center concerned with system safety are as described in the following paragraphs.

8.2.1 INDUSTRIAL OPERATIONS SYSTEM SAFETY OFFICE

The Industrial Operations System Safety Office, operating under the delegated authority of the Assistant Director for Engineering, is responsible for the development of system safety requirements and techniques in support of the respective program oriented system safety functions within the framework of guidelines and policies established by the Marshall Space Flight Center Safety Office. In pursuance of this responsibility this office will:

a. Provide guidelines for developing a system safety activity in Industrial Operations programs that is effective during all applicable phases of a system development and operation. A suggested flow diagram showing relationships of phased program planning with system safety is given in Appendix A.

b. Integrate the system safety functions performed by each program office into an effective total Industrial Operations system safety effort.

c. Maintain liaison among associated Marshall Space Flight Center contractors and others through Technical Interchange Meetings.

d. Provide uniform techniques and methods to comply with the system safety requirements described in Section 3 of this plan.

e. Participate in design reviews, certification reviews, and flight readiness reviews, in addition to other special safety reviews as required by the Director of Industrial Operations.

f. Participate as a member of the Marshall Space Flight Center Safety Board as required for the purpose of representing the Director, Industrial Operations in center-wide system safety plans and functions and coordinating Industrial Operations system safety activities.

8.2.2 PROGRAM OFFICES

The program office system safety activity will utilize the guidelines and provisions of this plan as applicable. In pursuance of the

responsibilities in planning, organizing, and implementing a system safety effort, the program office system safety activity will for the program manager:

a. Require each prime contractor to establish an identifiable system safety activity.

b. Require each prime contractor as appropriate to prepare and submit to the program office a system safety plan that describes the system safety effort to be performed and the approach to be used for its accomplishment. The system safety effort is to be keyed to major program milestones (paragraph 6. 2) and should consider the policies and procedures contained in this system safety plan.

c. Establish requirements as appropriate for the contractors to apply the system safety program elements identified in Section 2.

d. Maintain functional relationships with related disciplines including Configuration Management, Reliability, Maintainability, Quality Assurance, System Engineering, and Mission Operations.

e. Provide system safety data to the Industrial Operations System Safety Office and to other program offices.

f. Incorporate system safety activities into program management review functions.

g. Maintain interfaces with the Research and Development Operations and obtain support as required.

8. 2. 3 MISSION OPERATIONS OFFICE

The Mission Operations Office system safety activity will be consistent with system safety guidelines and criteria, and the provisions of this plan. The activity will:

a. Perform an overview function for the mission operational safety analyses and requirements relative to each program.

b. Maintain cognizance of safety problems identified in system design and as associated with launch and flight operations requirements.

c. Coordinate and staff range safety requirements in accordance with established policy.

d. Maintain close relationship with Research & Development Operations laboratories, Industrial Operations program offices and operations offices of other centers in mission operational safety effort.

APPENDIX A

PHASED PROGRAM PLANNING

Over the past year, considerable attention has been devoted to the improvement of the agency's program/project management and, particularly, the planning and approval processes related thereto. Phased program planning is an effort to develop an incremental or phased approach to program/project management which, based on limited applications in several major areas, has demonstrated many potential benefits. Phased Project Planning is not an end itself but represents a major step in evolving a management pattern of maximum effectiveness in the application of agency resources to its tasks.

The conceptual framework of these phases is as follows:

(1) Phase A effort involves the analysis of a proposed technical agency objective or mission in terms of alternate approaches or concepts, and the conduct of that research and technology development requisite to support that analysis and to assist in determining whether the proposed technical objective or mission is valid.

(2) Phase B effort involves detailed study, analysis and preliminary design directed toward the selection of a single project approach from among the alternate approaches resulting from Phase A activities.

(3) Phase C effort includes the detailed definition of the final project concept, including the system design and the bread-boarding of critical systems and subsystems, as necessary to provide reasonable assurance that the technical milestone schedules and resource estimates for the next phase can be met, and that definitive contracts can be negotiated for Phase D.

(4) Phase D effort includes final hardware design and development, fabrication, test, and project operations.

Phased program planning as related to system safety activities is illustrated in Figure A-1.

*NPD 7121.1 OCT. 28, 1963	PHASE A* ADVANCED STUDIES	PHASE B* PROJECT DEFINITION	PHASE C* DESIGN	PHASE D* DEVELOPMENT AND OPERATION				
				MANUFACTURING	TESTING	HANDLING & SHIPPING	STORAGE	OPERATION
SYSTEM SAFETY DESIGN CRITERIA	START DEVELOPMENT OF SAFETY CRITERIA TO BE USED.	DEVELOP AND DOCUMENT SYSTEM SAFETY CRITERIA.	IMPOSE SYSTEM SAFETY DESIGN CRITERIA FOR SAFE TEST, HANDLING, STORAGE, OF THE SYSTEM.	AUDIT/SURVEY MANUFACTURING ACTIVITIES TO SAFETY ASSURE CRITERIA IS MET.	AUDIT/SURVEY TEST ACTIVITIES TO ASSURE SAFETY CRITERIA IS MET.	AUDIT/SURVEY SHIPPING ACTIVITIES TO ASSURE SAFETY CRITERIA IS MET.	AUDIT/SURVEY STORAGE ACTIVITIES TO ASSURE SAFETY CRITERIA IS MET.	AUDIT/SURVEY OPERATION ACTIVITIES TO ASSURE SAFETY CRITERIA IS MET.
SYSTEM ANALYSES (DESIGN)	START SYSTEM ANALYSES TO SUPPORT TRADE OFFS AND MISSION CONCEPT DEVELOPMENT.	DEFINE SYSTEM ANALYSES TO SUPPORT SYSTEM DEFINITION AND MISSION DESIGN	DETAILED QUANTITATIVE SAFETY ANALYSES TO SUPPORT DESIGN REVIEWS AND DEVELOP SYSTEM SAFETY BASELINE.	REVIEW FAILURE OR DAMAGE OF SYSTEM	COMPONENT/SYSTEM FAILURE ANALYSES.	REVIEW DAMAGE TO SYSTEM	SYSTEM CHECKOUT AND REVALIDATION.	OPERATION FAILURE DIAGNOSTIC ANALYSES WILL BE PERFORMED ACCORDING TO EST'D CURRENT MSFC/KSC OPERATING AGREEMENTS. THE PROG. S/S ACTIVITY IS RESP'BLE FOR GETTING NOTICE OF SUCH FAILURES
HARDWARE CHANGE ANALYSES (ECP'S)	DEVELOP METHOD FOR ECP'S REVIEWS BY SYSTEM SAFETY	UPDATE ECP SYSTEM SAFETY REVIEW METHOD	PERFORM ANALYSES AND SYSTEM SAFETY TRADE STUDIES.	REVIEW SYSTEM CHANGES FOR IMPACT ON MANUFACTURING.	REVIEW SYSTEM CHANGES FOR IMPACT ON TESTING, TEST EQUIPMENT AND TEST PROCEDURES.	REVIEW SYSTEM CHANGES FOR IMPACT ON SHIPPING, HANDLING EQUIPMENT AND PROCEDURES.	REVIEW SYSTEM CHANGES FOR IMPACT ON STORAGE, ENVIRONMENT, SHELF LIFE AND REFURBISHMENT.	REVIEW SYSTEM CHANGES FOR IMPACT ON OPERATIONAL REQUIREMENTS.
OPERATIONS SYSTEM SAFETY ANALYSES	DEFINITION OF HAZARDOUS OPERATIONS.	DEVELOP METHOD OF OPERATIONS SYSTEM SAFETY ANALYSES	ANALYZE MANUFACTURING PLANNING, MAINTENANCE CONCEPTS, SHIPPING, STORAGE, HANDLING PROCEDURES AND FACILITIES. DEVELOP PERSONNEL CERTIFICATION REQUIREMENTS.	SURVEY MANUFACTURING ACTIVITIES AND REVIEW CERTIFICATE OF PERSONNEL PERFORMING CRITICAL ACTIVITIES.	AUDIT TEST ACTIVITIES AND REVIEW CERTIFICATION OF TEST PERSONNEL.	AUDIT HANDLING AND SHIPPING ACTIVITIES FOR SAFETY COMPLIANCE.	SURVEY STORAGE ACTIVITIES AND REQUIREMENTS FOR SAFETY COMPLIANCE.	MONITOR CERTIFICATION OF PERSONNEL PERFORMING OPERATIONS AND PREOPERATIONAL CHECKOUT, DETERMINE THE COMPATIBILITY OF HARDWARE/ PROCEDURE/ PERSONNEL
PROCEDURES ANALYSES	DEVELOP METHOD TO ASSURE PROCEDURE INCORPORATION OF SAFETY CONSIDERATION	DEVELOP SAFETY CRITERIA FOR USE IN PROCEDURE PREPARATION.	UPDATE SAFETY CRITERIA FOR USE IN PROCEDURES PREPARATION.	REVIEW MANUFACTURING PROCEDURES TO ASSURE THEY INCORPORATE THE SAFETY CRITERIA.	REVIEW TEST PROCEDURES TO ASSURE INCORPORATION OF THE SAFETY CRITERIA.	REVIEW HANDLING AND SHIPPING PROCEDURES TO ASSURE INCORPORATION OF SAFETY CRITERIA	REVIEW STORAGE PROCEDURES TO ASSURE INCORPORATION OF SAFETY CRITERIA.	REVIEW PROCEDURE TO ASSURE INCORPORATION OF SAFETY CRITERIA.

FIGURE A-1 PHASED PROGRAM PLANNING AS APPLIED TO SYSTEMS SAFETY

APPENDIX B

SYSTEM LOGIC ANALYSIS

The systems safety analysis, when completed, must be a useful tool and must be fully program effective. The technique employed should have sufficient versatility to encompass the complete system. It should provide management visibility as to the safety of the system in terms of a quantification of the safety; and it should identify critical fault paths, which treat cascading faults and interfunctional relationships. The analysis should be sufficiently flexible to measure the impact of both large and small system changes.

The system logic analysis technique is the most satisfactory method of system safety analysis developed to date which has this versatility and lends itself readily to computerizing.

The following steps are required in system logic analysis:

1. Define the undesired event.
2. Acquire understanding of the system.
3. Construct the system logic diagram.
4. Collect quantitative data.
5. Symbolize the system logic diagram. algebraically.
6. Solve the algebraic equations to determine the level of safety.

STEP 1 - DEFINE THE UNDESIRED EVENT

The objective of system logic analysis is to identify all hazardous potentials (failures, malfunctions, or human errors) within a system,

determine the level of safety of the system, and indicate those areas where additional effort would be most fruitful in improving the safety level.

The measurement of the level of safety for an operational product, requires initially the definition of the most undesired event, i. e., the event which must be kept from happening.

It is impossible to construct a system logic diagram with more than one "most undesired event"; yet it is possible to isolate several events that must be prevented from occurring. This situation makes it mandatory to establish terminology for the top event that will encompass the lesser events individually or collectively.

As will be shown, system logic analysis is a team effort. A tremendous amount of "brainstorming" and carefully considered inputs from many sources are required to make the analysis truly valid.

STEP 2: ACQUIRE UNDERSTANDING OF THE SYSTEM

The safety of any system must be measured from a specific time interval and type of activity. For this reason, the systems safety analyst must thoroughly understand the system and its intended use.

The construction of a system logic diagram for a given system or operational procedure necessitates that the analyst consider controlled premature termination of a specific event. For instance, an engine malfunction or failure may be compensated for by immediate abort action, still, the possibility of failure to react or incorrect reaction on the part of the astronaut must be considered. Conversely, a reasonable probability must be assigned for occurrence of the proper action.

The analyst must also consider the possibility of inability to initiate controlled termination during certain segments of the analysis. Once the Lunar Module has returned from the lunar surface, for example, the Apollo system is committed to follow its normal mission profile and any inflight failures must be accepted as additional events in the system logic analysis.

The principal objective of the system safety analyst is to determine how the system, considering the crew as an integral part, could fail and cause the undesired event. The myriad details the engineer can develop to determine all the probable ways a system can fail depends on his understanding of the system. A space vehicle has so many subsystems it is obvious that the systems safety analyst cannot possibly have a thorough working knowledge of each. Thus, in addition to his basic skill he must have broad experience with subsystems in general and must understand the basic concepts of the various system functions involved. Accordingly, a complete system safety analysis can be developed cooperatively only by a group of engineers having all of these required skills.

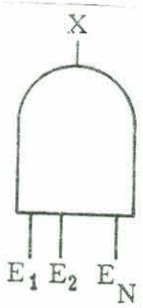
STEP 3: CONSTRUCT THE SYSTEM LOGIC DIAGRAM

A system logic diagram is a graphical representation of the sequential relationships of basic system events which can contribute to the occurrence of the end fault condition.

The development of a particular system logic diagram is accomplished in an orderly manner and begins with definition of the end system condition or undesired event for which a determination of probability of occurrence must be made. Once definition of the end event is made, the system is analyzed and all possible

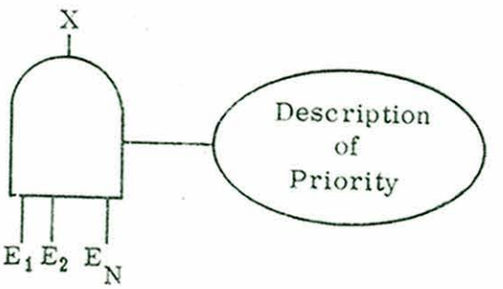
sequences of events are determined which, upon occurrence, result in the undesired event. Such analysis is entirely dependent upon a thorough knowledge of the system functions and equipment. Each of these contributing events is further analyzed to determine the logical relationships of system events which may cause them. In this manner, a "tree" of logical relationships among events on the tree are defined in terms of basic, identifiable events which may be assigned known probability values. The connections between the events are depicted in the system logic diagram as a progression of events through logic gates. Two basic logic gates are used in constructing a fault tree: The AND and the OR gate. These and several variations of them which are occasionally used are described in the following paragraphs.

AND Gate. The logical AND function is symbolized as follows:



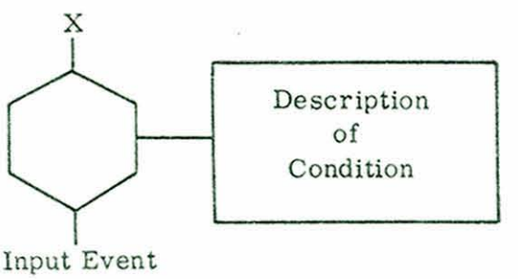
This symbol is understood to represent the logic operation whereby a "true" output exists at X when inputs E_1 through E_n are simultaneously present in their "true" state. Otherwise X is in a "false" stage.

PRIORITY AND Gate. The PRIORITY AND Gate performs the same function as an AND Gate with the additional stipulation that one event must precede the other.

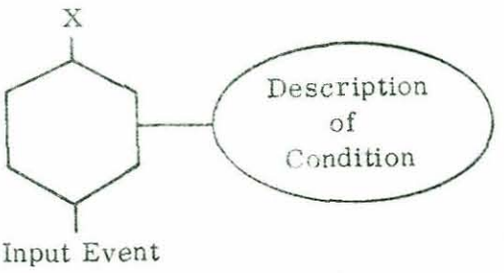


INHIBIT Gates. The INHIBIT Gates describe a causal relationship between one fault and another. The input event directly produces the output event if the indicated condition is satisfied. The conditional input defines a state of the system that permits the sequence to occur, and may be either normal to the system or the result of equipment failures. It is represented by an oval if it describes a specific mode, or a rectangle if it describes a condition which may exist for the life of the system.

INHIBIT Gate. The INHIBIT Gate provides a means of applying conditional probabilities to the sequence. If the input event occurs and the condition is satisfied, a "true" output will be generated at X.

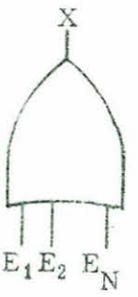


RANDOM INHIBIT Gate. The RANDOM INHIBIT Gate is functionally the same as the INHIBIT Gate. However, in this case the conditional input is a variable.



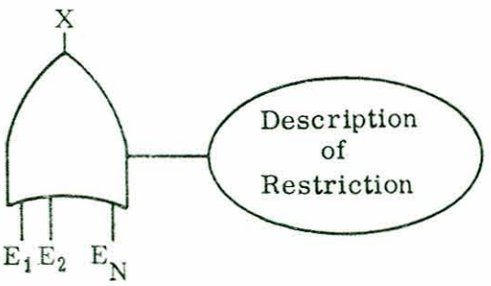
All of the above gates are basically AND Gates. The following two gates are OR Gates.

OR Gate.



This symbol represents the logic operation whereby a "true" output exists at X when any one or more of the inputs E_1 and E_n are present in their "true" state. The output X is "false" only when all inputs E_1 through E_n are "false" simultaneously. No order requirements exist at OR Gates.

EXCLUSIVE OR Gate. The EXCLUSIVE OR Gate performs the logical OR function but will not respond to the co-existence of two or more specified inputs.

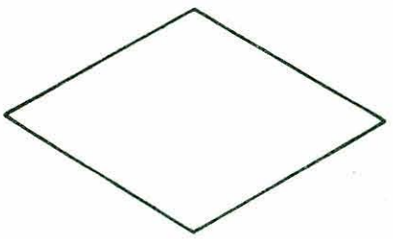


Other Symbols. In addition to the gates, several other symbols are used in the construction of system logic diagrams.

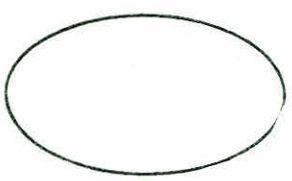
The rectangle identifies an event, usually a malfunction, that results from the combination of events through the logic gates. The rectangle is also used to describe conditional inputs to INHIBIT gates. In this use it indicates a condition that is presumed to exist for the life of the system.

The circle describes a primary event that requires no further development. This category includes component failures whose frequency and mode of failure are derived through laboratory testing.

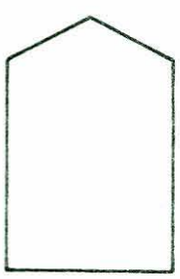
The diamond describes an event that is considered basic in a given system logic analysis; however, the causes of the event have not been developed usually because the event is of insufficient consequence.



The oval is used to record the conditional input to an inhibit gate. It defines the state of the system that permits an event sequence to occur, and may be either normal to the system or be the result of equipment failures.

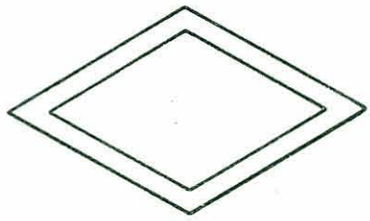


The house indicates an event that is normally expected to occur.



The triangles indicate transfer symbols. A line from the apex of the triangles indicates that data from another part of the tree is also to be input at this point. A line from the side of triangle denotes that this portion of the tree is also to be transferred to some other place in the tree.

The double diamond is used in the simplification of the fault tree for numerical evaluation. The event described results from causes that have been developed but are not shown on a particular version of the system logic diagram.



The term "event" represents that situation whereby an input to a gate or an output from a gate goes from an unfailed or "false" state to a state of failure or "true" condition. This event represents a system failure, whether it be a basic hardware fault or a gate output resulting from input events. The "event" will remain "true" until the conditions for its existence are no longer satisfied; i.e., either repair of a hardware failure is accomplished, thereby removing the failure from the system, or the input conditions required for a gate output are no longer satisfied due to some change in the system.

Typical System Logic Diagram. A typical system logic diagram for a simple system is illustrated in Figure A-1. System logic diagrams representing more complex systems are much larger and more involved, but the

relationships are the same. The numbers and letters on the logic diagrams are only to facilitate discussion and do not represent actual designations.

The basic events are represented by circles and are designated by the letters A through K. The logical relationships among the events are represented by AND and OR gates and are given number designations 1 through 7. The output events are represented by rectangles and are designated by X_1 through X_7.

The overall effect of this representation is to present a working model of the inter-relationships of basic system failure events as they contribute to a major system failure.

STEP 4 - COLLECT QUANTITATIVE DATA

After having constructed the system logic diagram in sufficient depth such that the inputs are specified in terms of component failure, the next step is to determine the probability of failure of each of the components. This type of data is available from such sources as the Failure Rate Data Program or the Reliability Group within one's organization.

STEP 5 - SYMBOLIZE THE SYSTEM LOGIC DIAGRAM ALGEBRAICALLY

Examining the sample tree in Figure B-1, it is seen that the event X_1 (represented by a true output from gate 1) is equivalent to the "true" state of

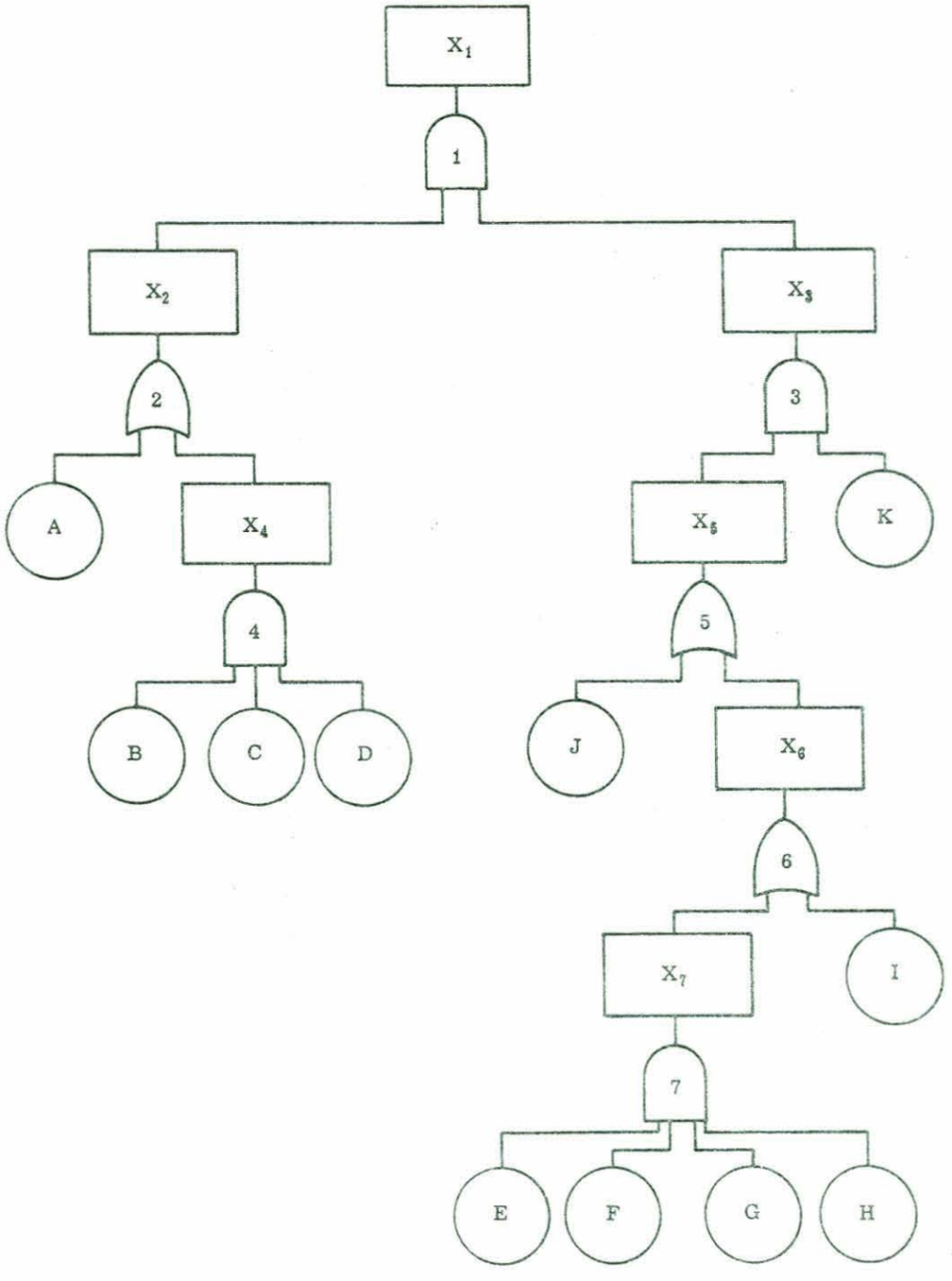


Figure B-1. Typical System Logic Diagram

both events X_2 and X_3. In similar fashion X_2 is equivalent to the true state of either event A or event X_4 or both. The logical AND is represented by the symbol (·) and the logical OR by the symbol (+). Each gate can then be represented as follows:

$X_1 = X_2 \cdot X_3$ $\qquad$ $X_3 = X_5 \cdot K$

$X_2 = A + X_4$ $\qquad$ $X_5 = J + X_6$

$X_4 = B \cdot C \cdot D$ $\qquad$ $X_6 = X_7 + I$

$X_7 = E \cdot F \cdot G \cdot H \cdot$

The total tree can then be represented by a single equation (by simple substitution) as follows:

$$X_1 = X_2 \cdot X_3 = (A + X_4) \cdot (X_5 \cdot K) = [A + (B \cdot C \cdot D)] \cdot [(J + X_6) \cdot K]$$

$$= \{A + B \cdot C \cdot D\} \cdot \{[J + (X_7 + I)] \cdot K\}$$

$$= \{A + BCD\} \cdot \{[J + (E \cdot F \cdot G \cdot H) + I] K\}$$

$$= [A + BCD] [K(I + J + EFGH)].$$

This equation is a Boolean representation of the system logic diagram. It is to be noted that the gates in the tree establish the relationships of the events in the end expression and that the output of the tree is expressed in terms of the basic input events.

Another sample tree, Figure B-2 shows how interfunctional relationships are handled. For example, failure event W has an effect on gates 6, 8, 9, and 10 or ultimately gates 2, 3, 4, and 5; thus it can be seen that event W and any one of four other events provide a straight path to Q. The equation which represents the tree (using the substitution technique described above is:

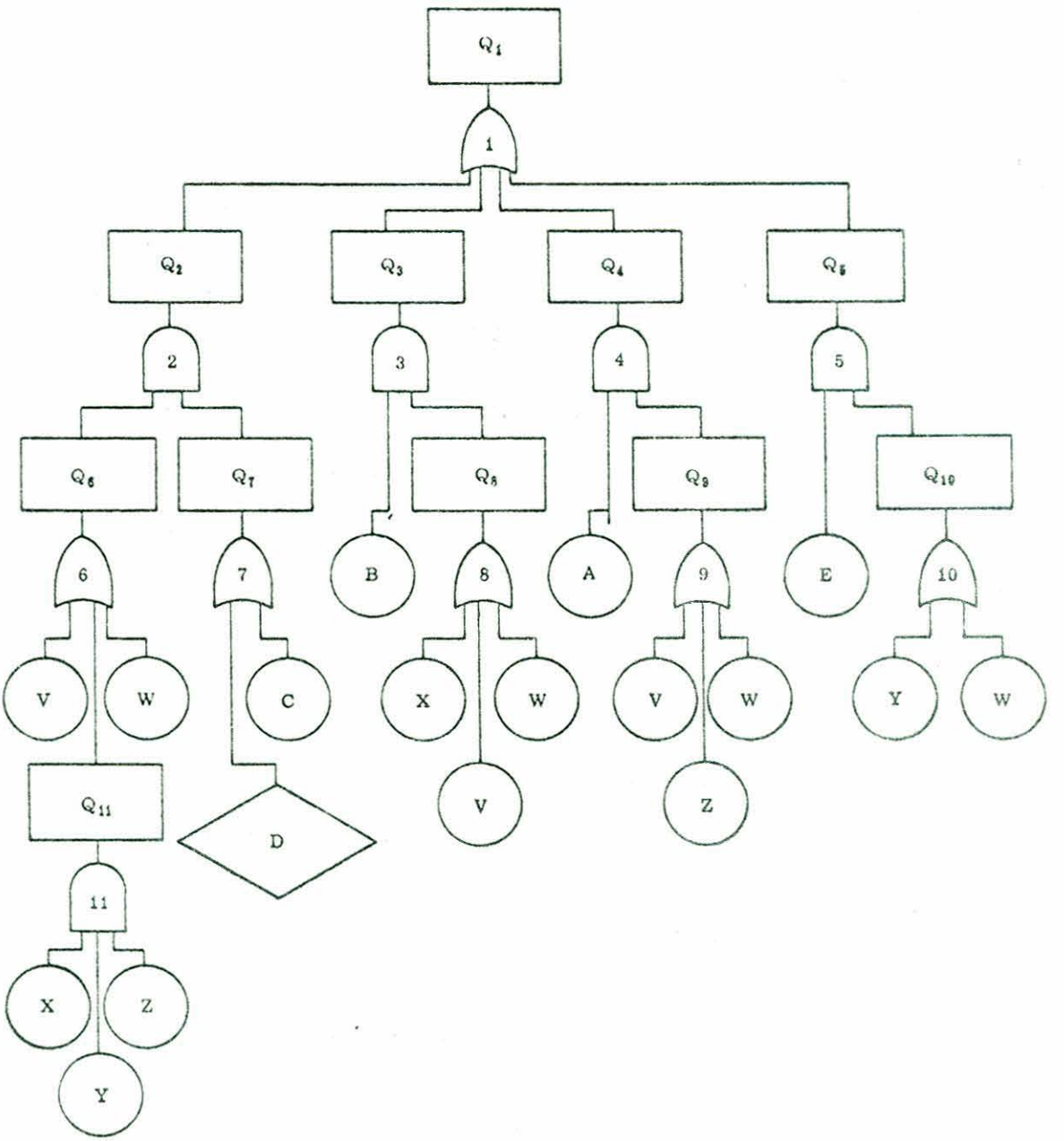


Figure B-2. Interfunctional Relationships

$$Q_1 = (C + D)(V + W + XYZ) + B(V + W + X) + A(V + W + Z) +$$
$$+ E(W + Y).$$

The probabilities of failure can now be utilized in the equation for the fault tree. By using normal relationships for the combination of probabilities and converting the equation from a Boolean expression to a normal algebraic expression, the equation will yield the probability of occurrence of each of the major branches to that probability. If the probability of occurrence of the undesired event is determined to be too high, the branch which is the major contributor can be identified and efforts to increase the safety can be applied to the most promising branch.

STEP 6 - SOLVE THE ALGEBRAIC EQUATIONS TO DETERMINE THE LEVEL OF SAFETY

In the simplest of system logic diagrams the solution of the equation consists of simply applying Boolean techniques to the equation originally derived from the fault tree to reduce the equation to the simplest possible form. The probabilities of the failures are then substituted into the equation and the equation is algebraically solved to yield the overall probability of the undesired event. Few trees are small and simple enough to solve in this manner and the solution is usually obtained by computer. The computer procedure is the same as the manual method except that the computer not

only develops the equation but removes the redundancies and calculates the probabilities.