NASA TECHNICAL MEMORANDUM

NASA TM X- 53612

May 23, 1967

NASA TM X- 53612

THE SYSTEMS SAFETY PROGRAM FOR A TOTAL SPACE LAUNCH VEHICLE GENERAL REQUIREMENTS

By Preston T. Farish, Ph.D.
Industrial Operations

NASA

George C. Marshall
Space Flight Center,
Huntsville, Alabama

TECHNICAL MEMORANDUM X-53623

THE SYSTEMS SAFETY PROGRAM FOR A TOTAL SPACE LAUNCH VEHICLE GENERAL REQUIREMENTS

By

Preston T. Farish, Ph.D.

George C. Marshall Space Flight Center
Huntsville, Alabama

ABSTRACT

This report sets forth the requirements for a Systems Safety Program for a total space launch vehicle system. It defines the elements of such a program necessary to assure maximum safety and establishes the requirements for the accomplishment of those elements. The principles described herein shall be applied through all phases of the space launch vehicle system development including system definition, design, manufacture handling, storage, transportation, test, checkout and operation.

NASA-GEORGE C. MARSHALL SPACE FLIGHT CENTER

NASA-GEORGE C. MARSHALL SPACE FLIGHT CENTER

TECHNICAL MEMORANDUM X-53623

THE SYSTEMS SAFETY PROGRAM FOR A TOTAL SPACE LAUNCH VEHICLE GENERAL REQUIREMENTS

By

Preston T. Farish, Ph.D.

INDUSTRIAL OPERATIONS

TABLE OF CONTENTS

TABLE OF CONTENTS (CONCLUDED)

LIST OF ILLUSTRATIONS

TECHNICAL MEMORANDUM X-53623

THE SYSTEMS SAFETY PROGRAM FOR A TOTAL SPACE LAUNCH VEHICLE GENERAL REQUIREMENTS

SUMMARY

This report sets forth the requirements for a Systems Safety Program for a total space launch vehicle system. It defines the elements of such a program necessary to assure maximum safety and establishes the requirements for the accomplishment of those elements. The principles described herein shall be applied through all phases of the space launch vehicle system development including system definition, design, manufacture handling, storage, transportation, test, checkout and operation.

INTRODUCTION

The Systems Safety Program for a space launch vehicle system is not intended as an inhibiting activity. It is, conversely, an enabling activity which employs sound scientific engineering and management practices to support all phases of the product development, resulting in the safest possible system for accomplishment of the mission. The Systems Safety Program has as its objectives the provision of the greatest possible management visibility concerning total system safety, the provision of preventive and/or corrective actions that can be used to ensure astronaut safety and mission success, the assurance that safety considerations are made a basic part of the total space launch vehicle system.

DEFINITIONS

Safety - is the freedom from those conditions which can cause injury or death to personnel and damage to, or loss of, equipment, property, or the mission.

System - As applied to this specification is defined as the total launch vehicle system including ground support equipment.

Systems Safety - is a systems engineering oriented discipline which functions to provide the greatest possible freedom from the occurrence of abnormal, or out-of-sequence, events that could, by their occurrence, cause the loss of the crew, the system, or the mission.

THE SYSTEMS SAFETY PLAN (SSP)

Each prime contractor or producer of a major system shall prepare a systems safety plan that is in consonance with the phase of development of his respective system. This plan shall include an identification of the applicable major system safety program elements described herein. It shall include a detailed description of the management and technical methods that will be used to accomplish these program elements and how they will function, together with a schedule for their completion, keyed to major program milestones. The SSP shall include but is not limited to the following:

I. Introduction and Scope

II. Objectives

III. Management Techniques

- A. The Systems Safety Organizational Structure
- B. The reporting lines
- C. The responsibility and authority
- D. The contractor interfaces
- E. The functional relationships with other disciplines such as Reliability and Maintainability and with the manufacture and testing organizations
- F. Data management - retention, distribution and effective use
- G. Unique management methods and the advantages
- H. Subcontractor systems safety management
- I. Training and development of technical competence
- J. Resource applications
- K. Progress reporting

IV. Technical Methods

A. Trade-off study participation

B. Analysis Techniques

C. Criteria development

D. Support of design reviews

E. Procedures review, including manufacturing, handling, storage, transportation, checkout, test and operation

F. Accident - Incident investigation support including planning

G. Hardware change assessment

H. Component failure analyses (UCR's)

V. Schedules

Showing accomplishment of safety program elements keyed to major program milestones or such schedule requirements as may be imposed by NASA to support systems safety integration.

Approval of the SSP

Each contractor's SSP shall be submitted to the NASA Center Technical Manager for Systems Safety for approval, and when approved shall constitute the contractor's systems safety work statement. All changes to the SSP also shall require approval by the Technical Manager for Systems Safety. The approved plan shall be used by the procuring activity to measure the contractor performance in systems safety.

Integrating SSP

An SSP shall be prepared by the integrating contractor in the case of a system being developed by two or more prime contractors with a separate integration effort. This SSP shall describe the major integration program elements, the management and technical methods to be used and the schedule of completion. This SSP also requires approval by the NASA Center Technical Manager for systems safety.

Systems Safety Program Elements

The Systems Safety Program Elements, listed in chronological order without regard for phase definition are as follows.

1. Trade Studies for System Definition. The Contractor's Systems Safety organization shall participate in trade studies leading to system definition. Analyses shall be performed as required to ensure that hazards are not inadvertently incorporated into the system during definition.

2. Systems Safety Criteria Development. The Contractor's Systems Safety organization shall review data and experience gathered from all similar systems as a basis for safety criteria furnished in support of the design activities.

3. Systems Safety Analysis. The contractor will perform a system safety analysis of his system using the technique described in the appendix of this specification or equivalent. In the event that the contractor's product is one or more subsystems of a total system, he will support the integration of his analysis into a total system safety analysis as performed by the integrating contractor in accordance with schedules established by the Center's Technical Manager for Systems Safety.

The analyses will be updated in accordance with established schedules to include each subsequent system in the series.

Analysis applications. The contractor's systems safety organization will support all design and flight readiness reviews of the system as required by the NASA Center Technical Manager for systems safety using the completed safety analyses as a means of demonstrating the safety of the system.

4. Procedures Review. The systems safety organization will review all manufacturing, handling, transportation, storage, maintenance, testing, and operating procedures to ensure that they do not set up out-of-sequence events or otherwise create hazards to the system by their use. Criteria will be established as a basis for identifying test or operations that are hazardous. Those tests or operations that are hazardous will be given special attention including the development of back out or emergency planning and procedures.

5. Activities During Manufacturing. The systems safety organization will coordinate with manufacturing and with Quality Control at frequent intervals to provide system safety support to those efforts.

6. Hardware Change Review. The systems safety organization will review and/or analyze all proposed changes to the system prior to incorporation to ensure that safety levels established for the system are not compromised by changes.

7. Activities During Testing. The systems safety organization will provide close support to the test activities, including participation in the test program, to ensure that the safety of the system is considered in all decisions made during the performance of the tests.

8. Analysis of Failed Components. All components failing during test or system checkout, as reported in the UCR system, will be analyzed to determine the potential impact of that failure on the safety of the operational system.

Other Activities

1. Technical Interchange. The contractor will support the interchange of system safety information, analyses and data with other contractors and the cognizant NASA Center through meetings and other means as set forth by the Technical Manager for Systems Safety.

2. Accident-Incident Investigations. The systems safety organization will complete a plan for participation in accident-incident investigations. This plan will designate key personnel and describe their activities during the investigation. It will include provisions for the performance of diagnostic analyses as required to identify the causes of the event.

3. Training. The contractor will provide his personnel with training both in the systems he is developing and in the systems safety discipline such that he develops a high level of skill and technical compentence.

Relationships With Industrial Safety

The contractor will review his system safety organizations activities and responsibilities at frequent intervals in conjunction with the industrial safety activities to ensure that there are no voids in the interface between the two organizations and that the full spectrum of safety is receiving the proper effort.

Systems Safety Plan Approval

1. Contractor Submittal. The contractor's system safety plan will be submitted to the Center's Technical Manager for Systems Safety (one original and six copies) five weeks following implementation of this specification.

2. Plan Approval. The Center's Technical Manager for Systems Safety will review this plan and return it to the contractor within three weeks as approved or approved subject to required revisions or disapproved subject to required revisions.

APPENDIX

FAULT TREE 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, treating cascading faults, and interfunctional relationships. The analysis should be sufficiently flexible to measure the impact of both large and small system changes.

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

Development of fault tree analysis techniques began in 1962 at Bell Telephone Laboratories (BTL). BTL performed a ballistic missile system safety study using a method of mathematical analysis applicable to probability combinations in a fault tree format.

This technique is now expanding throughout the aerospace industry because it possesses many unique capabilities:

a - It allows the quantitative measurement of the safety of any given system.

b - It can be used to assess the safety impact of any change to that system.

c - It can locate and identify all of the critical paths and the possible failures which yield a given set of failure symptoms.

d - It can accommodate Interfunctional Relationships and cascading faults.

The following steps are required in fault tree analysis:

1 - Define the undesired event.

2 - Acquire understanding of the system.

3 - Construct the fault tree.

4 - Collect quantitative data.

5 - Symbolize the fault tree algebraically.

6 - Solve the algebraic equations to determine the level of safety.

Step 1 - Define The Undesired Event

The objective of a fault tree 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.

Definition of the most undesired event is not always as simple as it might appear from a superficial view of the system. The undesired event may not be the final result of a malfunction or incorrect procedure, but rather the final single action that inevitably leads to catastrophe. Consider the rotary lawn mower for example. The possibility of injury to the operator might appear to be the most undesired event to a lawnmower manufacturer. On the other hand, because of possible lawsuits, he should also be concerned with the possibility of his product throwing a blade or some other object and injuring a passerby.

It is impossible to construct a fault tree 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, fault tree 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 calculation of exposure to operational environments requires the systems analyst to consider two variables: duration of operation and the stress levels. The length of projected missions will have a direct bearing on exposure to known hazards and, therefore, may be assigned a specific numerical value in fault tree construction. The stress level will vary with each segment of the mission, i.e., countdown liftoff, boost, orbit, etc.

The construction of a fault tree 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 fault tree construction.

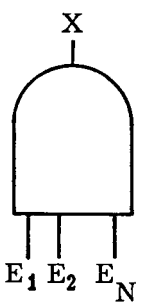
The principal objective of the system safety analyst is to determine how the system, considering the crew as an integral part, could fail and cause the undesired event. The myriad details the engineer can develop to determine all the probable ways a system can fail depends on his understanding of the 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 Fault Tree analysis can be developed cooperatively only by a group of engineers having all of these required skills.

Step 3 - Construct The Fault Tree

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

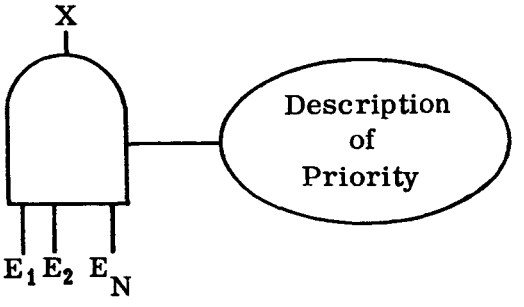
The development of a particular fault tree is accomplished in an orderly manner and begins with definition of the end system fault condition or undesired event for which a determination of probability of occurrence must be made. Once definition of the end fault event is made, the system is analyzed and 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 fault events is further analyzed to determine the logical relationships of system fault events which may cause them. In this manner, a "tree" of logical relationships among fault events is developed. The development is continued until all fault events on the tree are defined in terms of basic, identifiable faults which may be assigned known probability values. The connections between the events are depicted in the fault trees 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:



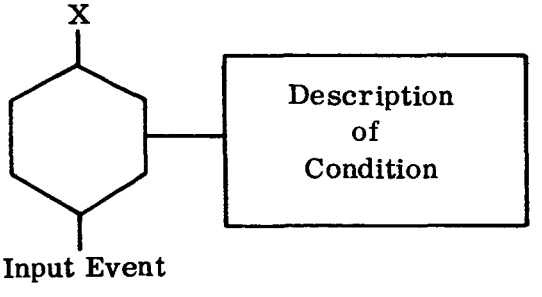
This symbol is understood to represent the logic operation whereby a "true" output exists at X when inputs E_1 through E_n are simultaneously present in their "true" state. Otherwise X is in a "false" stage.

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.

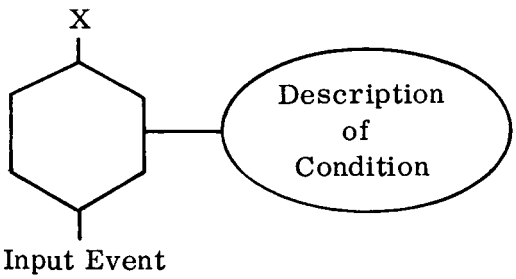


INHIBIT Gates. The INHIBIT Gates describe a causal relationship between one fault and another. The input event directly produces the output event if the indicated condition is satisfied. The conditional input defines a state of the system that permits the fault sequence to occur, and may be either normal to the system or the result of equipment failures. It is represented by an oval if it describes a specific failure 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 fault sequence. If the input event occurs and the condition is satisfied, a "true" output will be generated at X.

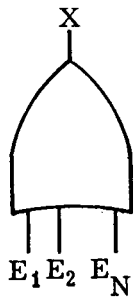


RANDOM INHIBIT Gate. The RANDOM INHIBIT Gate is functionally the same as the INHIBIT Gate. However, in this case the conditional input is a variable.



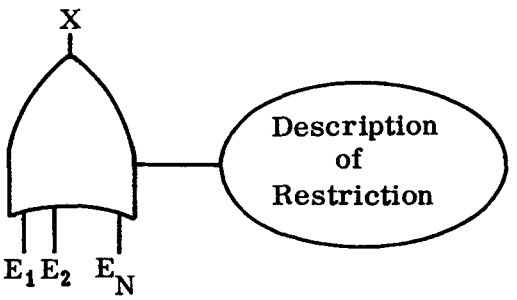
All of the above gates are basically AND Gates. The following two gates are OR Gates.

OR Gate.



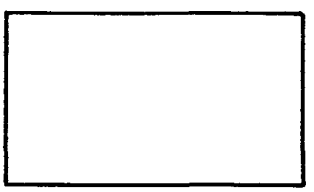
This symbol represents the logic operation whereby a "true" output exists at X when any one or more of the inputs E_1 and E_n are present in their "true" state. The output X is "false" only when all inputs E_1 through E_n are "false" simultaneously. No order requirements exist at OR Gates.

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.

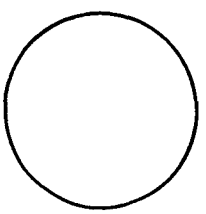


Other Symbols. In addition to the gates, several other symbols are used in the construction of fault trees.

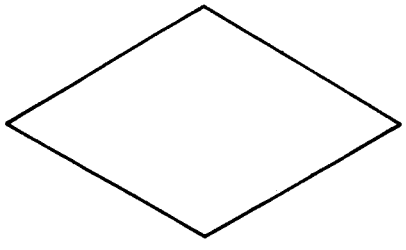
The rectangle identifies an event, usually a malfunction, that results from the combination of fault events through the logic gates. The rectangle is also used to describe conditional inputs to INHIBIT gates. In this use it indicates a condition that is presumed to exist for the life of the system.



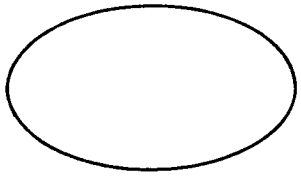
The circle describes a basic fault event that requires no further development. This category includes component failures whose frequency and mode of failure are derived through laboratory testing.



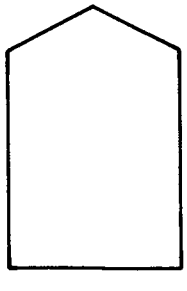
The diamond describes a fault event that is considered basic in a given fault tree; however, the causes of the event have not been developed usually because the event is of insufficient consequence.



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.

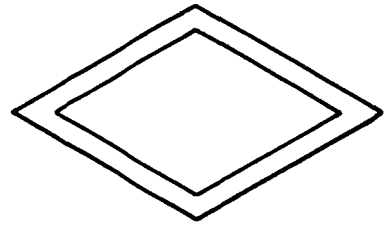


The house indicates an event that is normally expected to occur.



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 fault tree.



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 Fault Tree. A typical fault tree for a simple system is illustrated in Figure A-1. Fault trees representing more complex systems are much larger and more involved, but the relationships are the same. The numbers and letters on the tree are only to facilitate discussion and do not represent actual designations.

The basic fault 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 fault tree 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 Fault Tree Algebraically

Examining the sample tree in Figure A-1, it is seen that the event Q_1 (represented by a true output from gate 1) is equivalent to the "true" state of 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 ($\cdot$) and the logical OR by the symbol (+). Each gate can then be represented as follows:

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

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

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

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

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

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

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

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

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

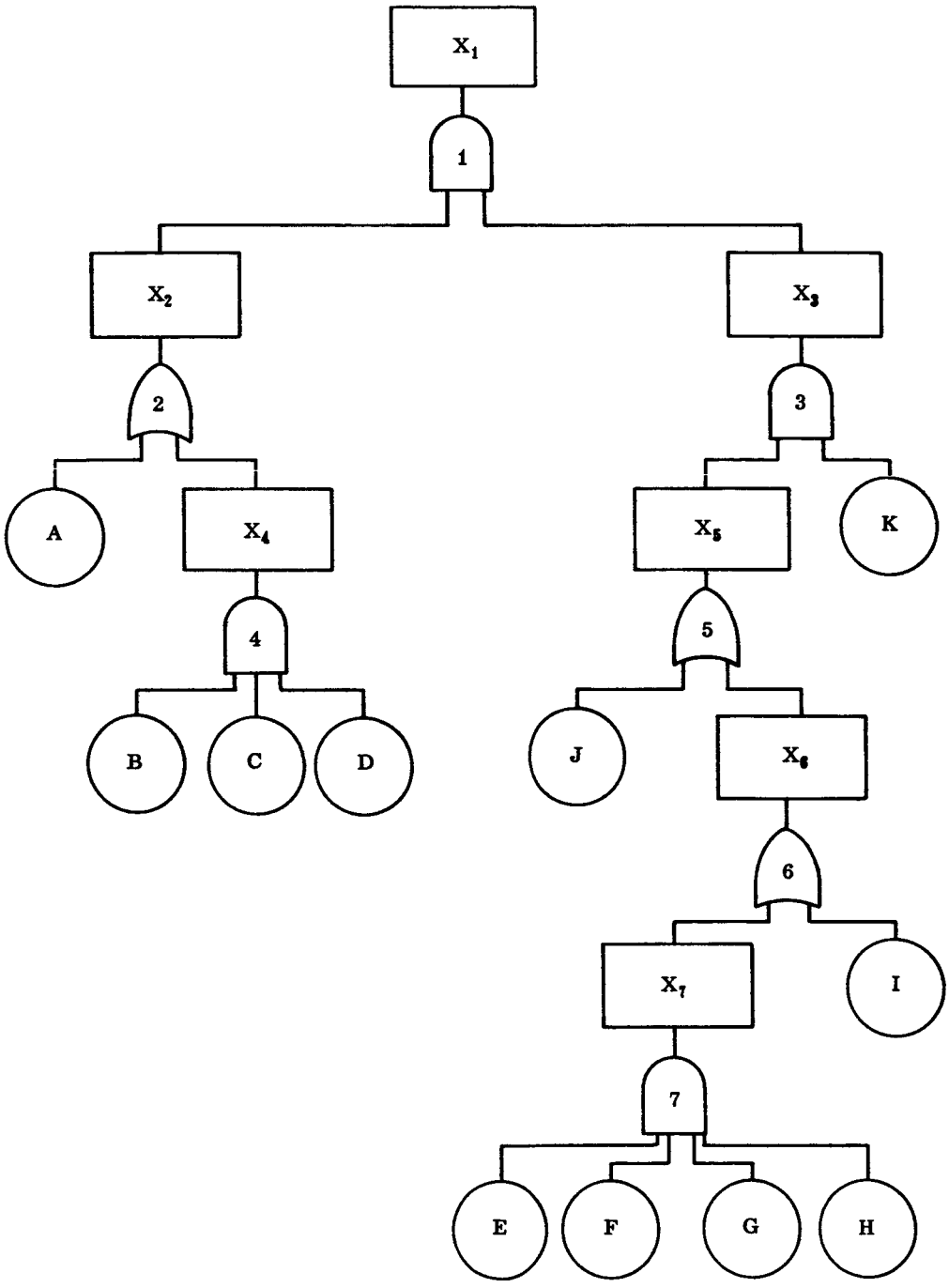


Figure A-1. Typical Fault Tree

This equation is a Boolean representation of the fault tree. 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 A-2 shows how interfunctional relatiships 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:

$$Q_1 = (C + D)\ (V + W + XYZ) + B(V + W + X) + A(V + W + Z) +$$

$$+ E(W + Y).$$

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 fault trees 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 is given the output of each gate as a function of the gate inputs and the computer not only develops the equation but removes the redundancies and calculates the probabilities.

The computer method offers many other advantages in cases where simulation is required or where "Repair" is considered. The simulation is conducted by generating random life length and repair times, according to the

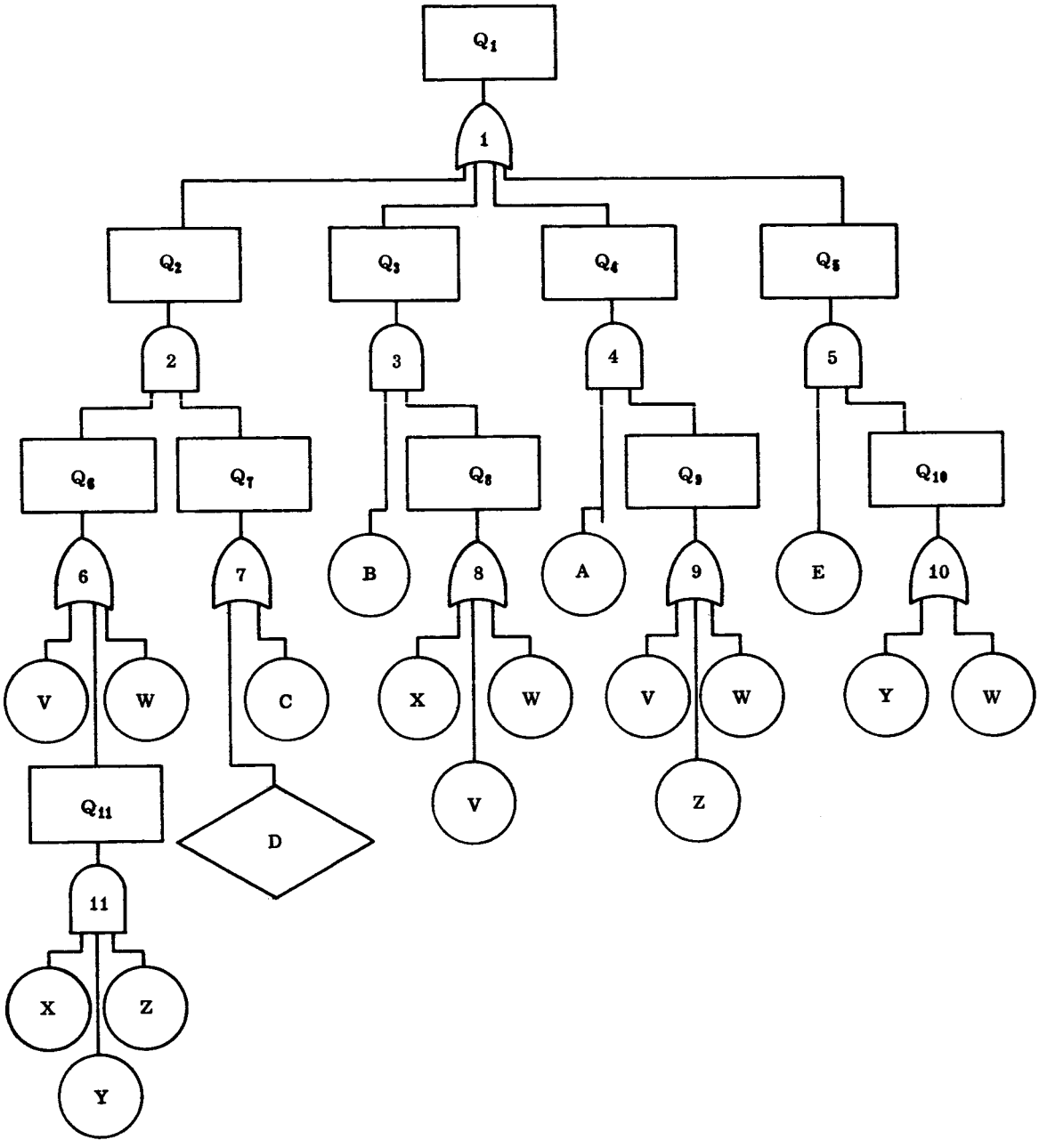


Figure A-2. Interfunctional Relationships

probability distribution given for each input. This is done by pseudo-random number generations on the computer. These random numbers provide data for a computer analog of the fault-tree. At the occurrence of a failure of any input the fault tree logic stored in the machine is checked to see if the undesired or the time period of interest, T, has elapsed. At this time, all of the inputs are recycles to an "up" state and a new trial begins. After a predetermined number of trials have been considered, an estimate is computed for the probability of the undesired event occurring within that time period from the formula:

$$\hat{P} = \frac{n}{N}$$

where n = number of times the undesired event has occurred out of N trials.

It can be seen that after all of the above steps have been accomplished, a quantitative measure of the safety of the system can be established; the contribution of each event to the "unsafe" condition can be determined; and the safety impact of any change to that system can be assessed. Therefore the "promise" of a suggested change toward increasing the overall safety of the system can be assessed.

George C. Marshall Space Flight Center
National Aeronautics and Space Administration
Huntsville, Alabama, June 28, 1967

APPROVAL

THE SYSTEMS SAFETY PROGRAM FOR A TOTAL SPACE LAUNCH VEHICLE GENERAL REQUIREMENTS

By Preston T. Farish, Ph.D.

The information in this report has been reviewed for security classification. Review of any information concerning Department of Defense or Atomic Energy Commission programs has been made by the MSFC Security Classification Officer. This report, in its entirety, has been determined to be unclassified.

This document has also been reviewed and approved for technical accuracy.

W. A. Mrazek
Assistant Director for Engineering
Industrial Operations