SOCIETY OF AUTOMOTIVE ENGINEERS, INC.

ARP 926A
FAULT/FAILURE ANALYSIS PROCEDURE

SAE AEROSPACE RECOMMENDED PRACTICE

BY: SAE S-18 AD HOC COMMITTEE TO UPDATE ARP 926 — OF THE SAE GENERAL PROJECTS DIVISION

Society of Automotive Engineers, Inc.
400 COMMONWEALTH DRIVE, WARRENDALE, PA. 15096

AEROSPACE RECOMMENDED PRACTICE

ARP 926A

Issued 9-15-67
Revised 11-15-79

FAULT/FAILURE ANALYSIS PROCEDURE

CONTENTS

FIGURES

1. INTRODUCTION

1.1 Background: A fault and failure analysis (F/FA) is an evaluation procedure that analyzes and assesses the effects of and documents potential failures in a system or equipment item design. It determines by analysis the effect of failures on system operation, identifies failures critical to operational success for personnel safety, and ranks each potential failure according to the combined influence of its effect and its probability of occurring.

The use of F/FA in design has grown with the expansion of technology. In the past, failure mode and effect analysis (FMEA) has been considered and used in a possibly restricted way. Now, however, other analytical procedures should be described and their application explained.

This revision of Aerospace Recommended Practice (ARP) 926 takes into account current technology and explains various methods of F/FA and their application. It presents fault and failure analysis procedures in their broad scope as design analysis tools. From this perspective, specialized analyses such as the FMEA and fault-tree analysis are considered as individual types of analyses within the broad scope of F/FA methodology.

The basic concept of the F/FA is one of determining the failure sources within a design, the modes of failure for each of the sources, and the effect of each mode on the complete design or any portion of it. F/FA is a design analysis tool; thus, it relates to several technical disciplines. The emphasis in this document is on what the tool is and how it can be applied to accomplish various objectives. The user determines how and for what purpose he uses it within his own technical discipline, such as reliability, safety, maintainability, or other associated specialty.

The end objective of the F/FA will determine what type of specialized analysis must be performed and how comprehensive the analysis must be. Considerations which will establish the specific form of the analysis are (a) whether qualitative or quantitative results are required, (b) the extent of the failure effects assessment required, and (c) the amount of the design to be included. As illustrated in Fig. 1, a minimum F/FA would consist only of an assessment of qualitative effects of failure modes of one portion of a design.

This minimum type F/FA can be expanded to provide a more comprehensive assessment of failure effects in terms of severity, or further, in terms of criticality. Severity pertains to the effect of the failure mode on equipment operation or mission function, whereas criticality is a combination of its severity level and the rate or probability of it occurring. For example, a nuisance effect of a low-severity level, frequently-occurring failure mode might be highly critical as far as equipment availability is concerned. On the other hand, a high-severity failure mode that occurs rarely, if ever, might be classified noncritical under some circumstances.

Failure mode probabilities, effect severities, and criticalities may be assessed qualitatively (e.g., low, medium, or high) and thus minimize the extent and cost of the analysis. If the needs of a program require more definitive results, the F/FA can be conducted to provide quantitative assessments for the failure mode probabilities and the severity levels and criticality rankings. Other considerations can also be included such as the effects on personnel and equipment safety; mission completion success; or maintenance, logistic, and supply support. Once the specialized form of the F/FA to be conducted is established, it can be applied to any or all levels of a design.

1.2 Approaches: There are two primary approaches for accomplishing the analysis, identified by their orientation in starting the analysis. One is the function-oriented approach. "Functional F/FA" is sometimes referred to as the "top-down" or "system" approach, since this type of analysis is frequently initiated at the top, or system level, and then proceeds downward through the design. The Functional F/FA uses the design functional requirements for evaluating design performance. It proceeds from a starting point of functional failure mode identification at a level of design where the analysis is being performed. The other is the hardware-oriented approach, "Hardware F/FA," and is sometimes referred to as the "bottom-up" or "parts" approach, since this type of analysis is frequently initiated at the parts level and then proceeds upward through the design. The Hardware F/FA starting point is the identification of the hardware failure modes at the design level where the analysis is being performed.

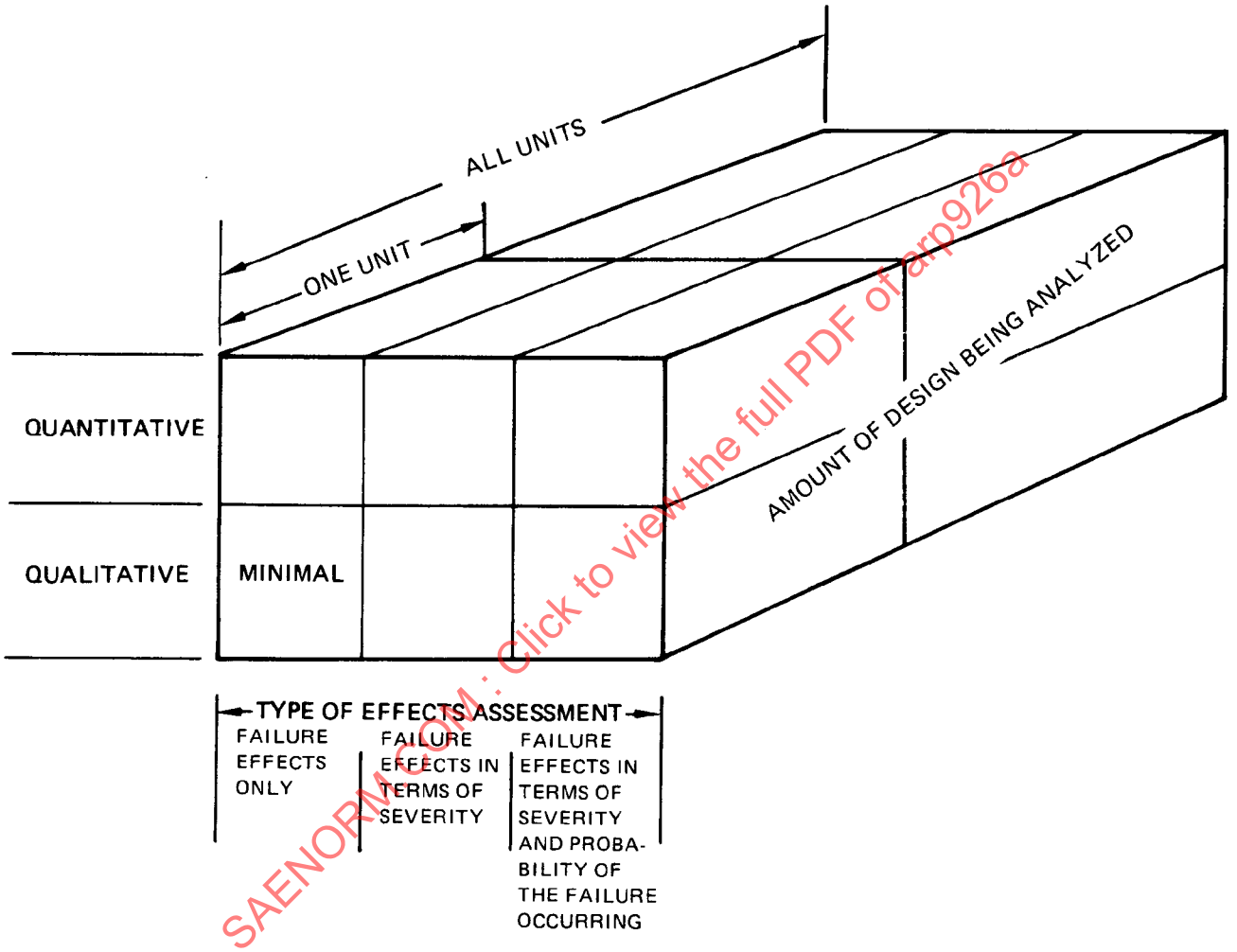


FIGURE 1
FAULT AND FAILURE ANALYSIS COMPLEXITY FACTORS

The "top-down" and "bottom-up" terminologies, however, are not completely descriptive since both the functional and hardware analysis approaches can be initiated at any design level and then be extended through the design in either direction. The "Functional F/FA" and "Hardware F/FA" terminologies have been used in the revised ARP as these are considered more accurate descriptions for the two approaches. Both approaches, when properly extended, have the capability of identifying functional and hardware causes and effects of failures. Thus, a complete analysis by either approach may cover all aspects of the design.

1.3 Purpose and Organization: The purpose of this ARP is to provide guidance material for those intending to utilize F/FA methods of analysis. In this regard, this ARP is organized to present first a discussion of general considerations pertaining both to the specification of the F/FA for procurement purposes and to the performance of the F/FA in response to a requirement. Following this are detailed discussions of the analytical methodologies involved. Included in these dicussions are descriptions of the two approaches (Functional F/FA and Hardware F/FA), what each involves, and when and for what purposes each might be applied. Consideration is also given to the specialized types of analyses within each of the two approaches. The next section of this ARP discusses the specific elements in an F/FA procedure necessary to provide guidance for developing an individual analysis to meet the required objective. Documentation of the F/FA is also discussed. The final section of this ARP presents an appendix containing a bibliography, examples of some specific types of F/FA's, a glossary of terms, and a discussion of new technology, such as digital avionics, as it relates to F/FA.

2. GENERAL CONSIDERATIONS

2.1 Basic Purposes: The basic purpose of the F/FA is threefold: 1) to avoid costly modifications by ferreting out latent design deficiencies in early design and testing phases of equipment item development, 2) to determine the critical failure modes that have a serious effect on the successful completion of a mission (or flight) and/or personnel safety, and 3) to consider the operational, maintenance, and logistic requirements.

In general, these objectives are accomplished by itemizing and evaluating the equipment item in terms of potential failures, based on knowledge of equipment function and statistical data. By sequence, it is determined how these failures might affect the subsystem, the vehicle, and the intended mission (or flight regimes). Specific failure detection methods and compensating provisions may be included in the F/FA for subsequent evaluation. By this approach, the weakness or limitations of the design can be highlighted and appropriate engineering attention directed toward improving the critical area. Reviews of failures that may occur during subsequent tests can also be conducted and the failure effects compared with those previously postulated in the F/FA.

However, an F/FA has its limitations. The F/FA cannot predict when an individual equipment item will fail or what its useful life will be. It can only predict that a certain percentage of items will fail in a given interval or that only a certain percentage will survive until a specified time. It cannot be used as a substitute for sound engineering judgment, but properly conducted, it can be used as a tool for assessing the likelihood of a failure occurring and the effect of that failure on the objectives of the design. The likelihood of a failure occurrence may need to be verified and possibly adjusted in the light of subsequent experience.

A thorough F/FA provides valuable assistance for the design team. The results can identify potential problems, further testing requirements, and required design modification. The F/FA evaluates a system, or portion thereof, and the interrelationships of its elements to determine the effects of potential failures on the system performance.

2.2 F/FA Application: In deciding on the extent that and the way in which F/FA should be applied to a project, the contractor should consider the specific purposes for which F/FA results are needed, the time phasing with other activities, and the importance of establishing a predetermined degree of probabilistic control over unwanted failure modes and effects. This leads into planning F/FA at specified indenture levels (system, subsystem, component) in qualitative and quantitative terms to relate to the iterative design and development process. Some of the possible applications for F/FA in formulating the F/FA plan are as follows:

a. Determining need for redundancy, fail-safe design features, further derating, and/or design simplification

b. Determining need to select more reliable materials, parts, devices, and/or components

c. Identifying single failure points

d. Identifying critical items for design review, configuration control, and traceability

e. Providing the logic model required to quantitatively estimate the probability of anomalous conditions of the system

f. Disclosing safety hazard and liability problem areas

g. Ensuring that the test program is responsive to identified potential failure modes and safety hazards

h. Establishing allowable use time or cycles

i. Pinpointing key areas for concentrating quality, inspection, and manufacturing process controls

j. Establishing data recording requirements and needed frequency of monitoring in testing, checkout, and mission use

k. Supporting logistics planning and maintainability analysis. Providing information for selection of preventive maintenance schedules and development of trouble-shooting guide, built-in test equipment, and suitable test periods

l. Identifying circuits for worst-case analysis. (Failure modes involving parameter drifts frequently require worst-case analysis.)

m. Supporting operation activities such as designing fault isolation sequences and alternate-mode-of-operations planning

3. APPROACH SELECTION

3.1 General Criteria: Normal criteria for the selection of the F/FA approach are to accomplish the objectives of the analysis in the most cost effective manner within applicable constraints. The principal constraints are the budget and time span available for performing the analysis and the design status of the equipment item to be analyzed. The design status establishes the type of source data which is available to conduct the analysis. This section explains the level of detail to be considered and the two basic approaches for starting the analysis, that is, by hardware item or by function. The section then defines the application of the Criticality Analysis and the Fault-Tree Analysis. Finally, it explains the use of a variation of approaches that involves combining the hardware items and functions as analytic starting points.

Whether the approach selection is for a self-imposed work statement or will become a contractual requirement for a supplier, it must be specific. To minimize the cost of the analysis, the required detail and documentation should be no more than required to achieve the objectives. The principal guidelines are the following:

a. Specify quantitative results only to the extent essential

b. Restrict the equipment item indenture levels to be included in the analysis to the minimum number needed

c. Limit the failure effects to those necessary to satisfy the purpose of the analysis

d. Do not call for an analysis of all probable failure modes if an analysis of the principal failure modes will satisfy the purpose of the analysis

e. Restrict the use of the Fault-Tree Analysis to very severe failure effects and to hazard analyses

f. Limit documentation of the analysis to that essential to utilize the analysis to accomplish the intended purpose

g. Do not impose a specific analytic format unless it is essential in order to combine independently developed lower-level analyses into a higher-level analysis. If, however, a format is established, keep it consistent throughout the analysis

3.2 Level of Detail: Before describing the details of the actual procedures for conducting an F/FA, a discussion of the levels of detail to be considered in the analysis will be helpful. Level of detail, as used here, applies to the level of hardware at which failures are postulated. Failures can be considered at any level down to individual parts and up to inputs and outputs of the items being analyzed.

The questions that arise, therefore, are: How does one decide at what level the analysis should be performed? What criteria are to be considered in choosing this level? How can the optimum benefits be realized within overall program constraints?

The greater the number of failure possibilities considered (the higher the level of detail), the greater will be the cost and the time required for the analysis.

During the conceptual phase of system development, the less detailed functional approach is particularly appropriate for eliminating design conceptual inadequacies. In later system development phases, the more detailed hardware approach may be more appropriate for helping implement the selected concept with superior hardware. Thus, the level of detail is affected by the phase of system development which prevails.

A less detailed analysis, completed at a time when it can contribute measurably to the system adequacy, may be much more valuable than a more detailed analysis delivered at such a late date that implementation costs make changes unfeasible. Thus, the level of detail is affected by cost and schedule constraints.

The importance of a subsystem to mission success may also help to determine the level of detail at which the analysis on the particular subsystem will be performed. Consider a system composed of many redundant subsystems and a single important subsystem which necessarily cannot be redundant because of space or weight limitations. A high level of detail is justified for the single important subsystem, whereas a lower level of detail may be indicated for the redundant subsystems.

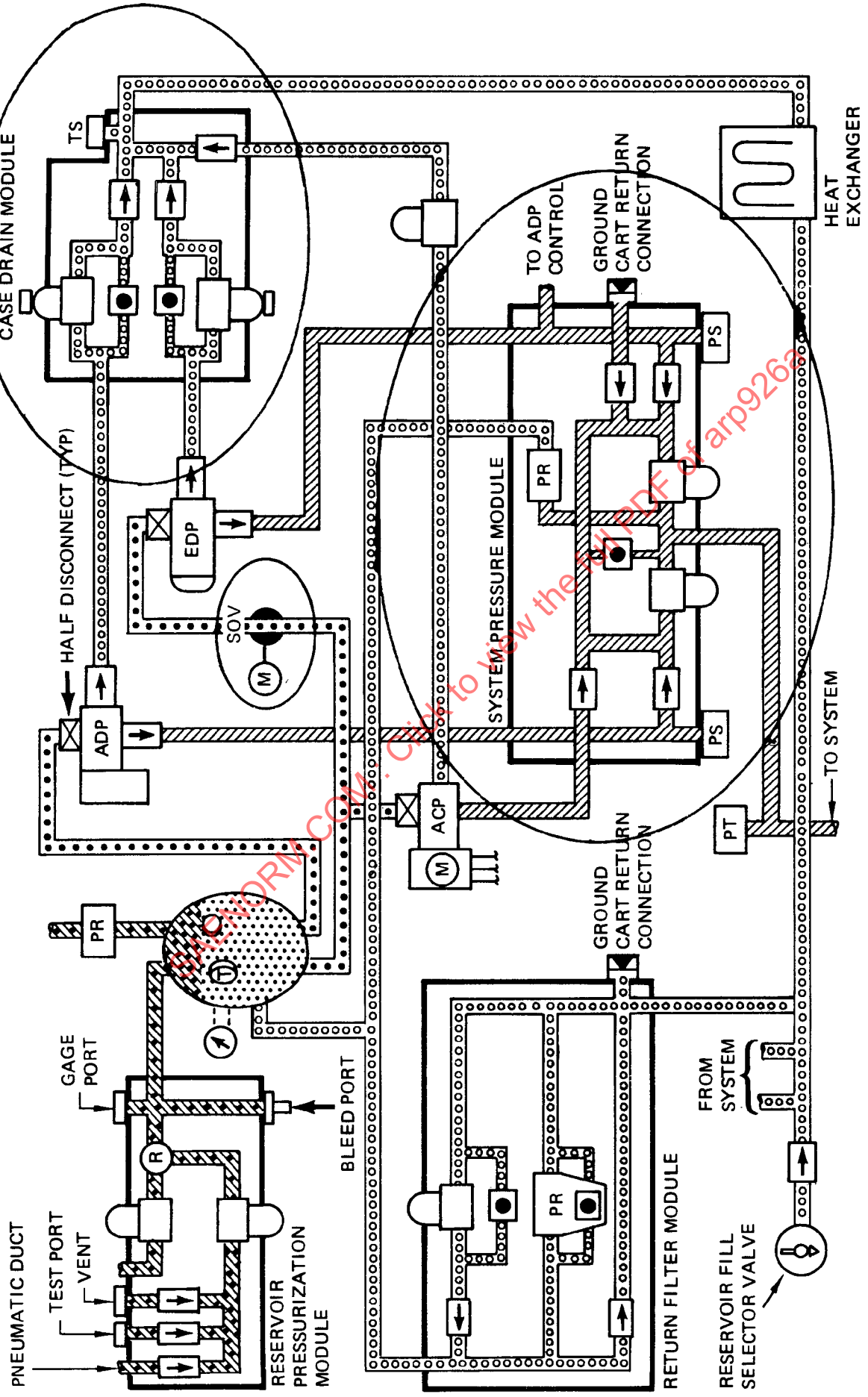


FIGURE 2
SCHEMATIC DIAGRAM OF HYDRAULIC POWER GENERATION SYSTEM

3.3 Hardware Approach: In applying this approach, the effects of each failure mode are evaluated with respect to the function of the related individual hardware item. These individual hardware failure effects are then related in sequence to the subsystem function and ultimately to the system function. For example, consider the shutoff valve in the Engine Driven Pump (EDP) supply line in Fig. 2 as the hardware item, and the EDP, Case Drain Module, and System Pressure Module as subsystems of the overall system. The valve failure mode "fails closed" will have the hardware effect of stopping the supply flow to the EDP. In sequence the effects on the above subsystem items would be: 1) loss of pump output flow and pressure, pump cavitation, pump damage; 2) loss of pump output would signal turning on the Air Driven Pump (ADP) to take over the pump output function, debris from pump damage could clog the case drain EDP filter, causing the clogged filter indicator to become visible and signal the need for maintenance; 3) effect on the system function would be "none," since the ADP output replaces the EDP output as the system output.

The hardware approach is not necessarily performed using the parts-level-up technique just described. The hardware approach can also be initiated by listing components at a higher system level. Failure modes at higher level are listed as well as corresponding failure effects on the equipment item itself and on the next higher level. The cause of the failure is then identified and the items contributing to the failure modes are listed. The analysis is then repeated at progressively lower levels. This type of analysis could be used for equipment modifications when a full analysis is not practical.

3.4 Functional Approach: Detailed analysis using a functional approach is initiated by analyzing a system diagram of equipment functions rather than hardware equipment items. This method of analysis is more adaptable to considering multiple failures and external influences such as human error.

The functional approach is generally preferred when system definition has not reached the point of identifying specific hardware items that will perform the functions. This situation often occurs in the early phases of development when individual item designs may not be completed and detailed item listings, system schematics, or assembly diagrams may not be available. At a later stage of system development, when system definition permits, equipment functions may be replaced by the hardware items selected to implement them. The functional approach is also used when system complexity is such that a system-level-down analysis is the more practical procedure to follow. This method of analysis is not as cumbersome and difficult to perform as the hardware approach. However, since it is function-oriented and not normally as detailed as the hardware approach, there is a possibility of overlooking a hardware failure mode.

The analysis starts with a functional block diagram (see Fig. 3) and may be accomplished by looking at the highest level and determining the potentially critical failures of each functional block. Each of these function blocks can then be broken down into lower level functional blocks with each of the lower level blocks examined to determine which, if any, of the potentially critical failures associated with the next higher functions could possibly occur in each of the lower levels. This process can be repeated at progressively lower functional levels until the piece part level is reached. The function identified with possible system critical failures can then be examined on a piece part level. The hardware associated with a function in which a critical failure may occur can then be examined to determine possible design improvement.

A hydraulic power generation system, illustrated by its schematic diagram (Fig. 2), was chosen as the basis of an example to illustrate this process of progressively moving to the next lower level as the analysis proceeds. Figs. 3 through 7, and the discussion accompanying each, illustrate this downward analysis process at various chronological stages of the system development.

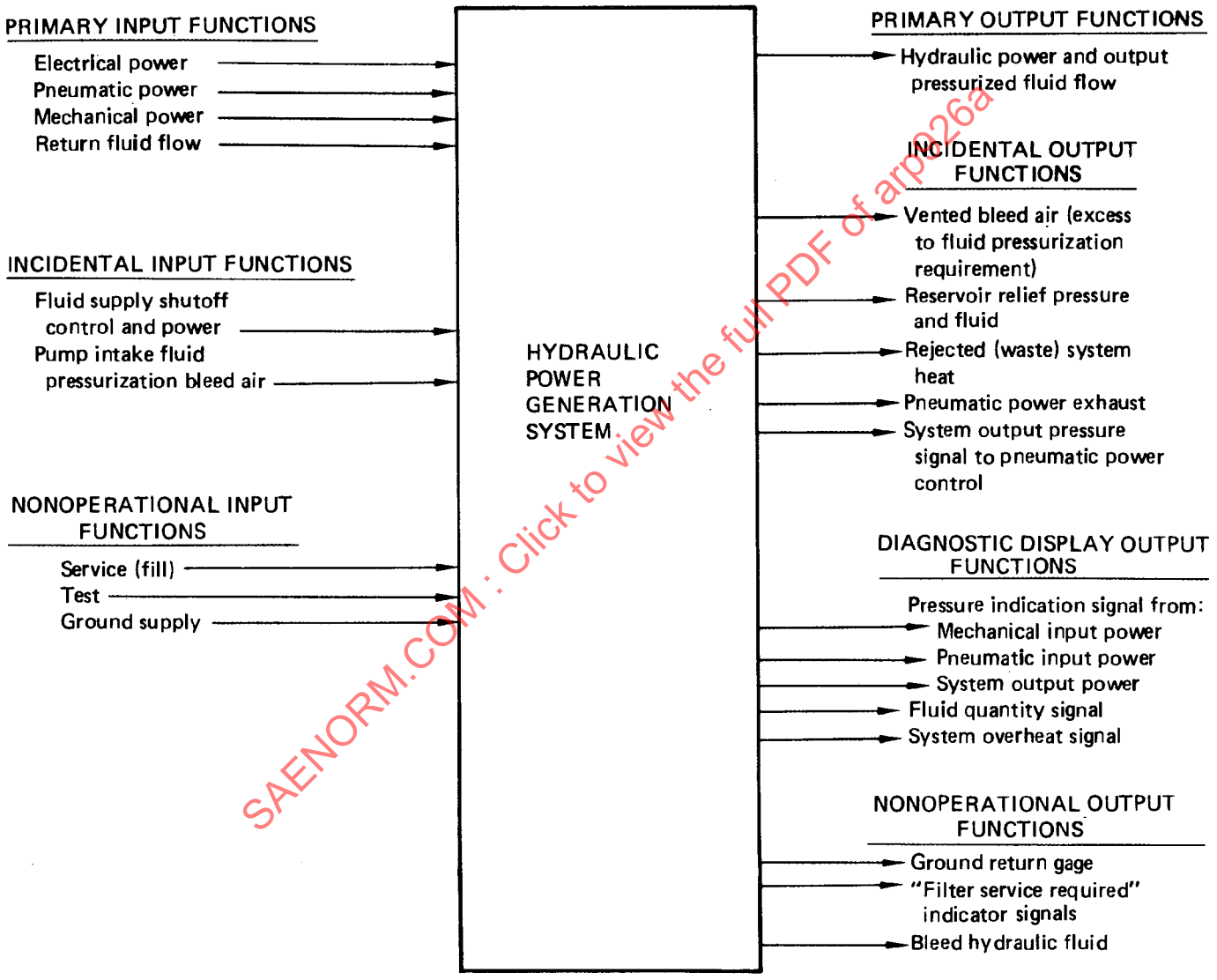


FIGURE 3
SYSTEM FUNCTIONAL BLOCK DIAGRAM

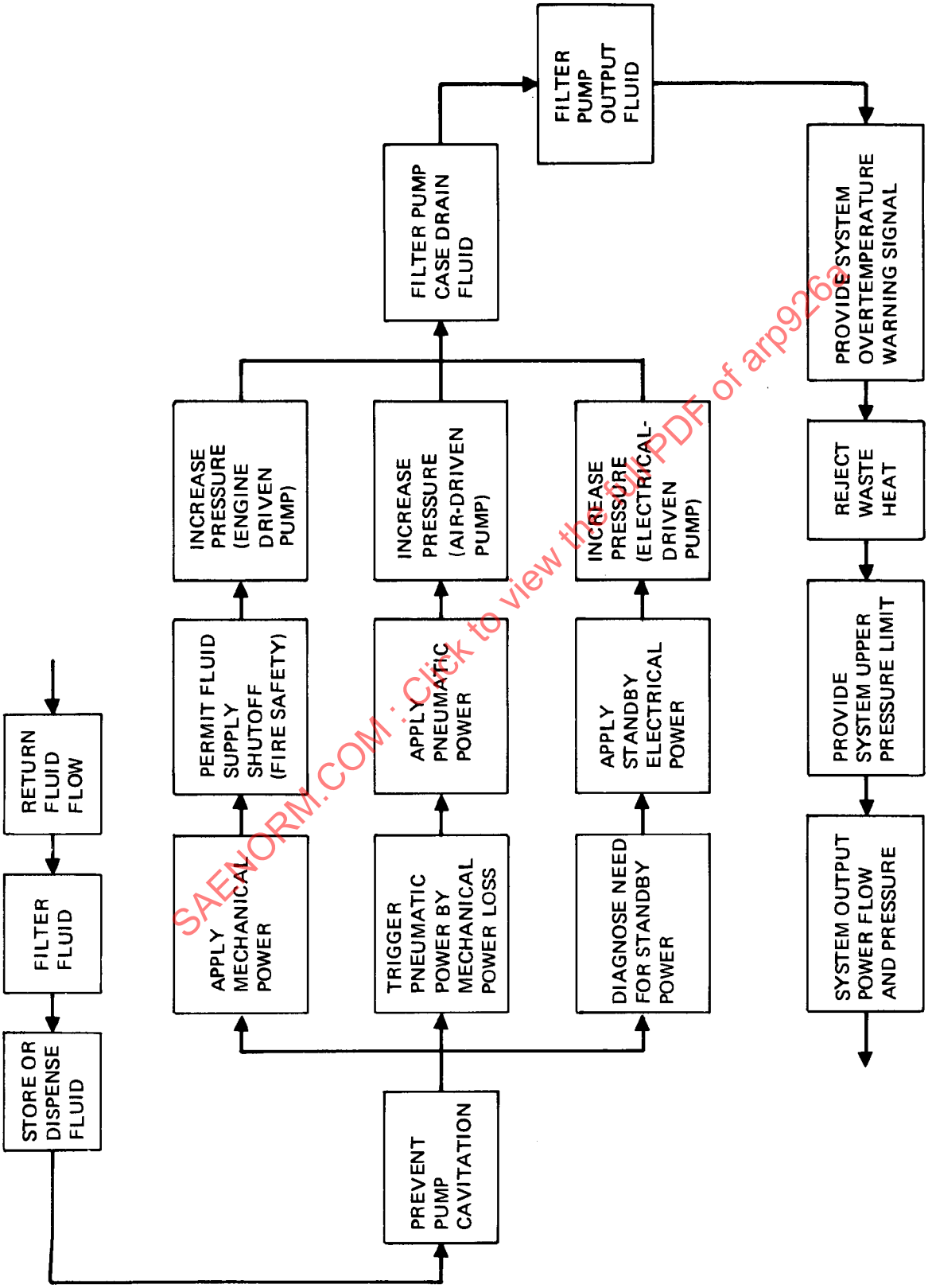


FIGURE 4
SUBSYSTEM FUNCTIONAL BLOCK DIAGRAM

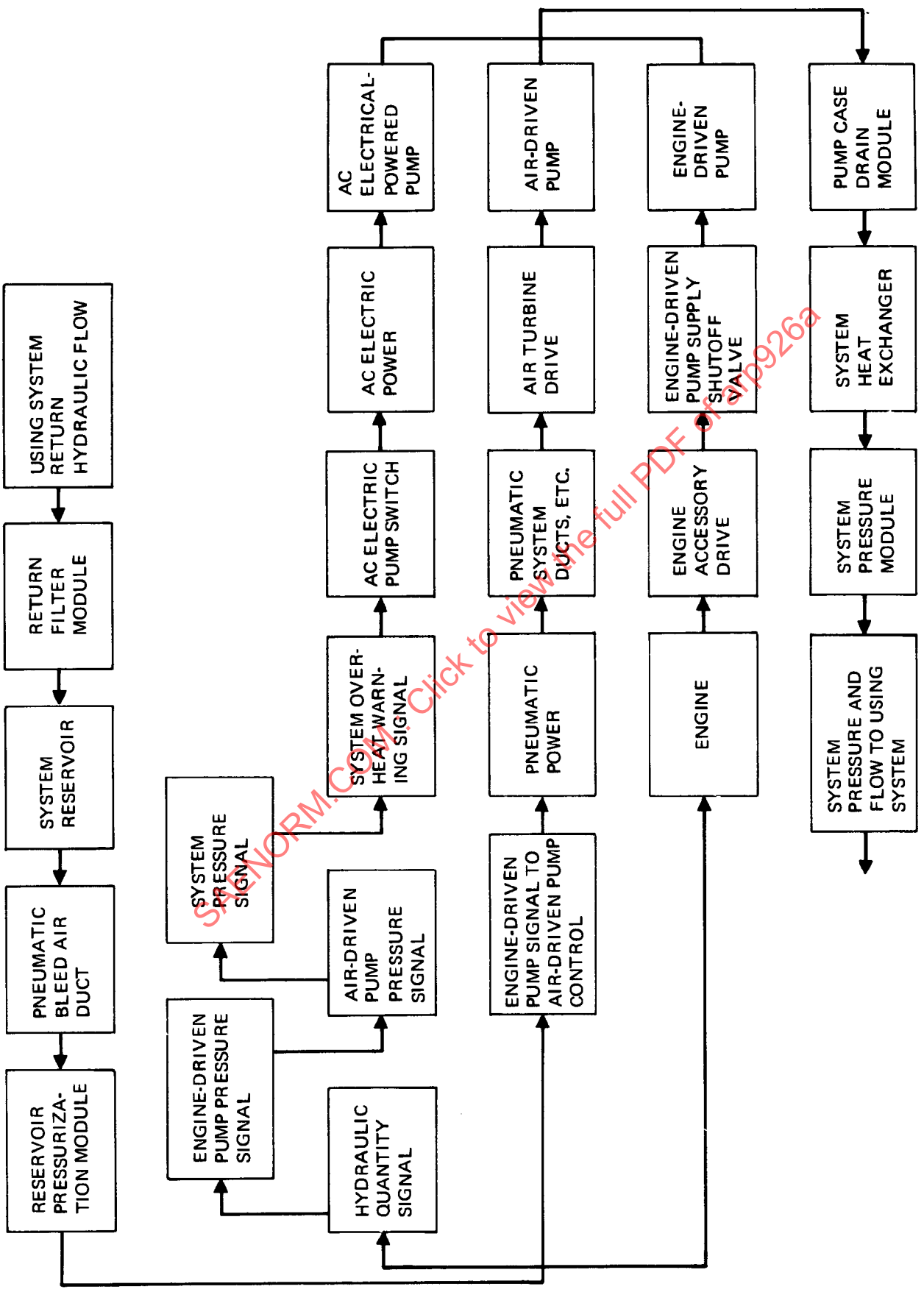


FIGURE 5
SUBSYSTEM HARDWARE FUNCTIONAL BLOCK DESIGN

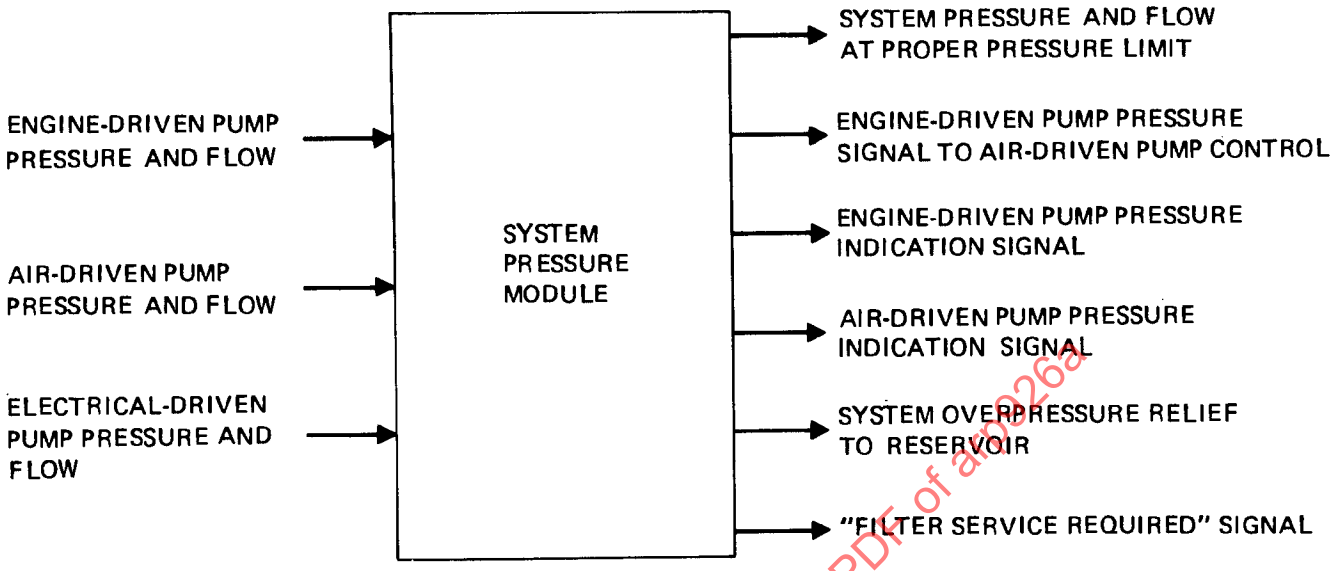


FIGURE 6
COMPONENT FUNCTIONAL BLOCK DIAGRAM

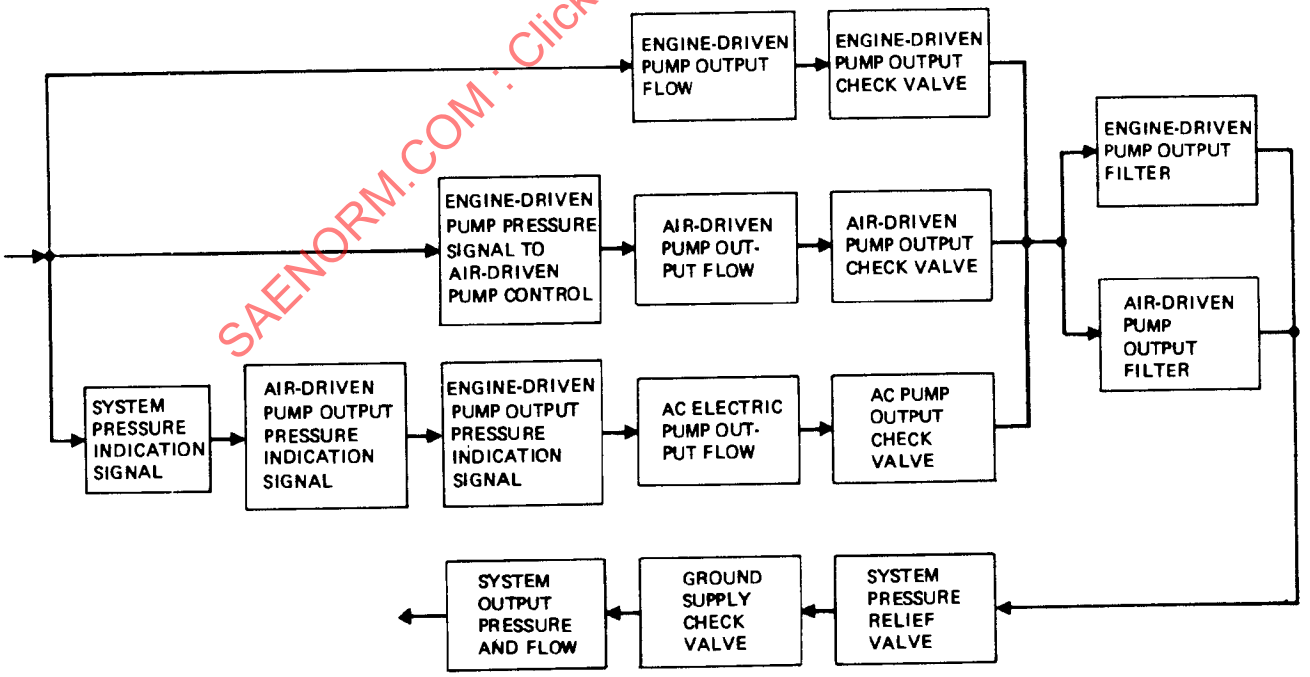


FIGURE 7
COMPONENT PIECE-PART FUNCTIONAL BLOCK DIAGRAM

3.4.1 System Output Level: Fig. 3, "System Functional Block Diagram," represents the system at its earliest conceptual stage as a single block. Its primary functions are to convert input energy (mechanical, pneumatic, or electrical) to hydraulic energy, applying it to a flow of hydraulic fluid by raising the fluid pressure. The remaining input/output functions are anticipated incidental functions, not needed for their own sake, but supportive of the primary function. At this stage of development, the chief concern of the analyst is to determine the effects of system failure on the utilizing system (perhaps a control system) and the need for system redundancy. The analyst would be attempting to help answer such questions as, "How many hydraulic systems are needed? What would give optimum distribution?" The analysis would normally ignore the incidental inputs and outputs and internal functions such as fluid filtration during this phase of development. Treatment of the system as a single functional block is well suited to this early, preliminary design phase.

3.4.2 Subsystem Output Level: Fig. 4, "Subsystem Functional Block Diagram," represents the same system at a time when emphasis has shifted to the system itself, rather than its utilization. Fig. 4 remains function-oriented rather than hardware-oriented, attempting to synthesize the system in terms of the anticipated functions needed to produce the primary functional capability. At this stage of development, although the needed functions can be identified, the hardware may not have been selected to implement the functions. It may not have been determined whether to combine functions in a given hardware item or use separate hardware for each function. Analysis of the functions can determine, nevertheless, which are critical to system performance and which are merely convenience functions.

Fig. 5, "Subsystem Hardware Functional Block Diagram," represents the system at a later stage of development when many of the functions have been replaced by the hardware items which implement them. Analysis at this stage can be carried further and numerical failure probabilities identified where off-the-shelf hardware items of known reliability have been selected. Some hardware items are still sufficiently complex as to be classed as subsystems, wherein the piece-part level has not been reached. Analysis at this level may influence component selection and piece-part redundancy.

3.4.3 Component Output Level: Fig. 6, "Component Functional Block Diagram," focuses on one hardware item from Fig. 5, the System Pressure Module, and represents it as a single functional block, in the manner used in Fig. 3. The primary function of this item is to condition the input hydraulic flow from any of three pumps to produce flow at a definite upper pressure limit. Secondary functions are fluid filtration and production of system diagnostic signals. Fig. 6 reflects a lack of definition at the piece-part level, or uncertainty regarding final hardware selection. Analysis using Fig. 6 could influence this selection or help define the necessary piece parts of this item.

Fig. 7, "Component Piece-Part Functional Block Diagram," represents this same System Pressure Module at a stage of development when the hardware selection has been made and piece-part information is complete. System analysis at this most detailed level is ordinarily directed to confirming design adequacy or identifying candidates for redesign or reliability growth programs.

3.5 Criticality Analysis (CA) Approach: Upon completion of a fault tree analysis, failure mode and effects analysis, or other F/FA procedure, the expected frequency of the critical failure modes occurring should be considered where appropriate. The CA is a procedure which extends the results of other F/FA procedures by categorizing the criticality of failure modes previously identified according to their expected frequency of occurrence and their effect on system performance. The true impact of a failure mode on the operational effectiveness of an equipment item is best described by the combination of these two characteristics. The CA is a procedure which relates the probability of a system component failure to a defined effect such as loss of life or inability to perform a required function. The CA combines the severity level and frequency of the occurrence of a given failure effect. The seriousness of the failure mode effects are described by undesirable event statements such as loss of life or inability to perform a required function. These severity level values and corresponding rate or probability values are used to insert failure mode reference numbers in a matrix indicating the distribution of failure mode criticality. The relationship permits a predetermined criticality threshold to be established in order to identify "critical" situations. Priority for corrective action can then be established from the list of critical items obtained from the matrix.

A criticality analysis can be performed using either a qualitative approach or a quantitative approach. The approach depends upon the availability of data from operational experience and tests that have been performed on equipment similar to those in the system under similar use conditions. If realistic data cannot be located, a qualitative CA should be considered.

3.5.1 Qualitative Approach: The qualitative approach assigns relative probability levels (such as probable, improbable, and extremely improbable) and severity levels. The combination of relative probability and relative severity establishes the relative criticality of the event being considered.

3.5.2 Quantitative or Criticality Number Approach: This approach computes criticality numbers for each mode in relation to the failure effect. The computation of the failure rate or the probability of the failure mode is established to indicate the criticality of the effects of the failure mode.

3.6 Fault Tree Analysis Approach: Fault Tree Analysis, often equated to the "top-down" analytical approach, is commonly utilized in aeronautical, nuclear, and other safety programs, but is also adaptable to non-safety applications. The logic of the fault tree approach makes it a visibility tool for both engineering and management. As one of a family of F/FA techniques for assuring that the equipment item will accomplish its assigned functions, the fault tree method is concerned with assuring that all critical aspects of the design are identified and controlled. The fault tree itself is a graphical representation of the logical relationships of a particular, undesired event (consequence) called the "top event," to basic failures (causes) called "primary events." The pictorial fault tree has a somewhat triangular shape and takes its name from the branching that it displays.

For any given system, the Fault Tree Analysis procedure is basically the construction of one or more fault trees, each dedicated to a top fault event. For each such tree the analyst utilizes system data (schematics, functional flow diagrams, etc.) to determine each of the possible faults or failures that could be a cause of the top event. Next he determines the causes of those causes, and so on downward to the basic causes of the primary events. Using special symbols, the fault tree shows precisely how the various faults and failures could logically combine to cause the top event. The completed fault tree, because it includes only those fault and failure events that could individually or collectively cause the top event, forms a concise statement of all events critical to the system insofar as the top event is concerned.

Some of the advantages of the fault tree analytical approach are:

a. It displays only faults and failures or combinations of them that lead to the undesired event, thus facilitating technical and management assessments and reviews.

b. It facilitates quantification of probabilities of events, notably the top event.

c. It facilitates subdivision of major events into lower level events for ease of analysis.

d. It is inherently flexible with regard to the degree of detail to be included; the analyst can choose the level of detail and can decide on the extent of qualitative versus quantitative analysis.

Section 4 treats the Fault Tree Analysis in some detail.

3.7 Variation of Approach: A variation of approach at the same level of analysis applies a combination of a Hardware Approach to some items and a Functional Approach to other items. Under some circumstances this may be the optimum approach, depending upon the available data or the intrinsic composition of the hardware or functions at the level of analysis under consideration. These circumstances can be readily illustrated by the following example.

When a subsystem being synthesized from a combination of established off-the-shelf components and newly designed components is under analysis, the source data may dictate a combination analysis. That is, complete Hardware F/FA's may be available for the established equipment items whereas the newly designed or about-to-be-designed items may exist only as Design Control Specifications and Functional Block Diagrams. Functional F/FA's would be appropriate for the latter.

4. F/FT PROCEDURES

4.1 General: This section provides the procedural methodology used in F/FA's. The family of F/FA's is depicted in Fig. 4.1. First, it provides general procedural elements which may be applied in any F/FA. Next, definitive procedures for the FMEA, CA, and FTA are provided.

The following general procedural steps should be used in performing the F/FT. A flow diagram outlining a step by step process is shown in Fig. 9.

Step 1. Define the system or hardware and its requirements.

Step 2. Establish ground rules and assumptions for performing the analysis, e.g., define failure criteria.

Step 3. Establish a block diagram and/or a sequence of events diagram.

Step 4. Identify failure modes, effects, failure detection methods, and other worksheet requirements.

Step 5. Evaluate criticality of the failure modes.

Step 6. Provide for the required corrective action in the design or manufacturing process and for evaluation of the corrective action adequacy.

Step 7. Document the analysis and provide recommendations for those items which could not be corrected by design or manufacturing process and changes which should be imposed as maintenance requirements in order to ensure that the inherent reliability is achieved.

Alternatively, individual procedures and formats may be utilized to perform a specific F/FA (e.g., FMEA, CA, or FTA); however, as a general rule, the above seven steps should be performed.

4.2 F/FA Procedure Elements: Variation in equipment design complexity and application dictate an individualized F/FA procedure for the equipment item being analyzed. Development of the procedure depends on the data available at the time of the analysis and the intended use of the F/FA results. Since the F/FA format will vary depending upon the specific program application, standardized worksheets are not recommended. Basic elements necessary for performing an F/FA are presented in the following paragraphs. The decision to follow the hardware approach, the functional approach, or some combination will be made at the appropriate stage. Any step unique to a particular approach is so noted.

4.2.1 Equipment Item Definition: A thorough understanding of the item and its characteristics and functions is required in order to perform the F/FA. The first step in performing an F/FA is to define the equipment item to be analyzed. Information used to describe the item should include such documents as functional block diagrams and schematics, item descriptions, specifications, drawings, failure definitions, operational profiles, environmental profiles, and reports bearing on reliability (e.g., feasibility or reliability studies of the items and other similar items).

The descriptions and specifications of the item internal and interface functions, starting at the highest level and progressing to the lowest level to be analyzed, will establish the interdependencies within the item so the effects of a failure may be traced. Equipment item descriptions and specifications also provide limits of acceptable performance under specified operating and environmental conditions.

The item definition derived from available descriptive information should include utilization and performance expected, functional narratives for each operational mode, and failure definitions.

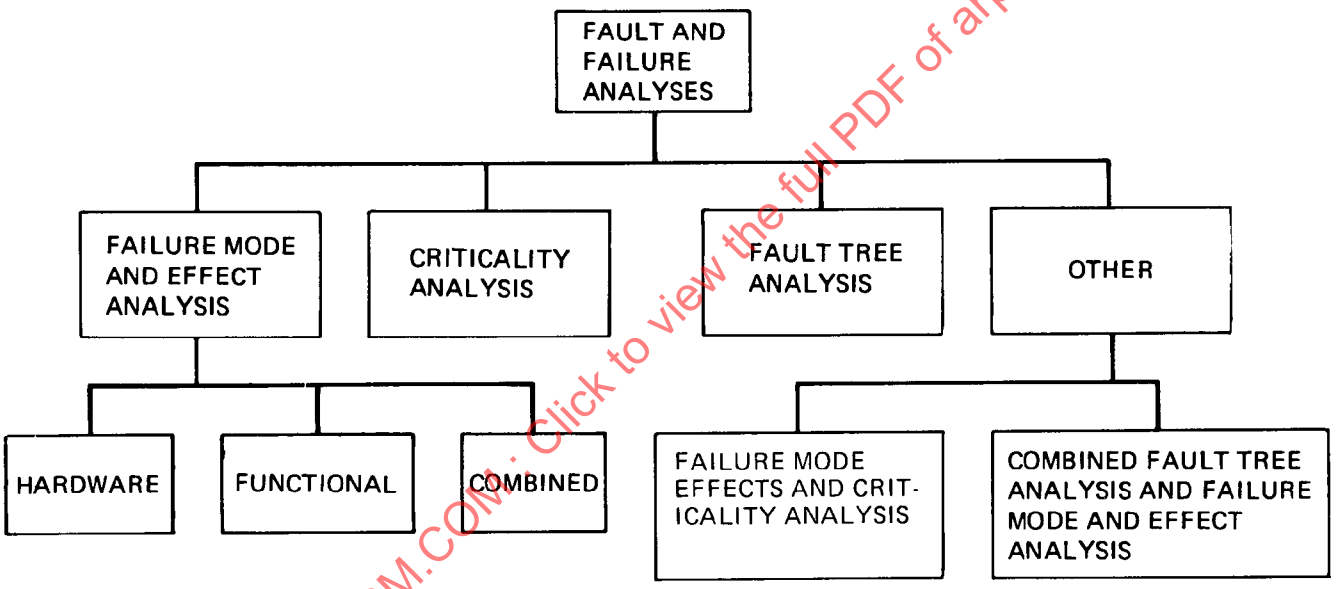


FIGURE 8
FAMILY OF FAULT AND FAILURE ANALYSES

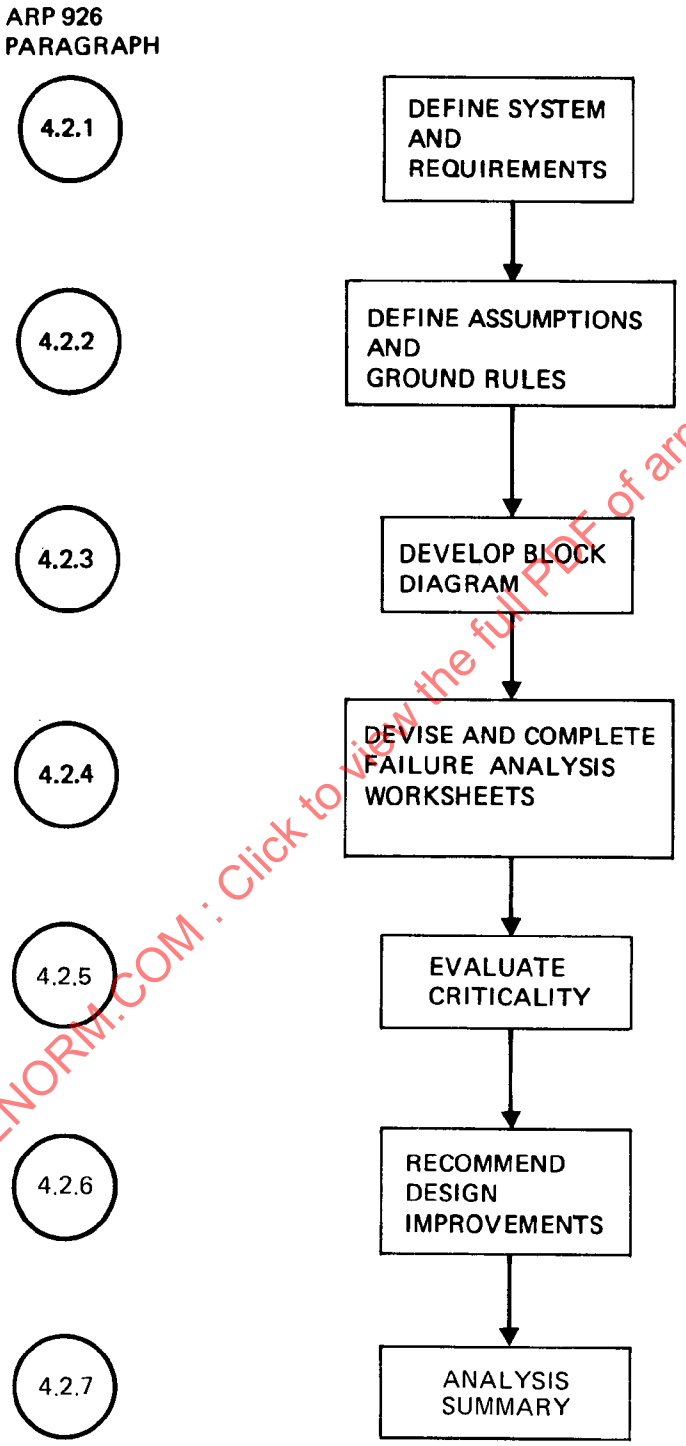


FIGURE 9
FLOW DIAGRAM OF GENERAL FAULT/FAILURE ANALYSIS PROCEDURE

4.2.2 Assumptions and Ground Rules for Failure Definition: To define what constitutes and contributes to the various types of failure, the technical specifications, requirements, and development plans for the system should be studied. These will normally state the system objectives and specify the design requirements for operation, maintenance, test, and activation. Detailed information in the plans will normally provide operational profiles and functional flow block diagrams showing the gross functions the system must perform for successful operation and are usually included at the system level. A definition of the operational and environmental stresses the system is expected to undergo, as well as failure definitions, will either be provided or must be developed.

4.2.3 Reliability Diagrams: The third step of the F/FA procedure is to diagram the item to be analyzed. A general method for constructing a diagram is shown in Fig. 10. This example system, with notes provided, explains the functional dependencies of the components. While this type of diagram is widely used, other diagrams such as a functional flow diagram are equally applicable and may be used when they accurately represent the operational relationship and functional interdependencies of the various elements of the system.

One of the first tasks in constructing the diagram is to determine the complexity levels of various elements of the system. A complex system may be more conveniently broken down into several diagrams. The first would usually be a simple diagram showing the first-order subdivision of the system. Separate diagrams are then constructed for each of the first-order subdivisions.

A system element at any level may be treated as a system and diagrammed in like manner for F/FA. Results of the analysis of this element will define the failure modes critical to the element's operation: i.e., those that cause loss of element inputs or outputs. These failure modes will then be used to accomplish the F/FA at the next system level. All system redundancies or other means for preventing failure effects should be shown in the reliability diagram.

It should be pointed out that for a given system, a separate diagram may be required for each operational phase or mode since both component use and criticality may vary with the phase or the mode of operation.

4.2.4 Documenting the F/FA: The F/FA and its documentation are accomplished by the following elements as appropriate. Examples of completed F/FA's are shown in Appendix B.

a. Item Identification: Identify the system function or hardware item being analyzed. Breakdown of a system for analysis should be down to the lowest level required for the F/FA. In special cases such as electronic systems using integral modular units as system building blocks, the modules may be listed rather than individual parts.

The name of the hardware item or function being analyzed along with an identification number by which each is identified should be listed. The reference designation is assigned for traceability purposes and should include the reliability diagram identifier. The same designation is used for the Criticality Analysis procedure.

b. Coding Systems: For consistent identification of system functions and equipment, an established coding system should be adhered to during the analysis. Any convenient method that relates the failure mode listings back to the reliability diagram and provides the capability to track each failure mode through the analysis can be used.

c. Function: If the hardware approach is being utilized to conduct the F/FA, a concise statement of the function performed by the item should be listed.

If the functional approach is being utilized to conduct the F/FA, the hardware identification corresponding to the function should be listed.

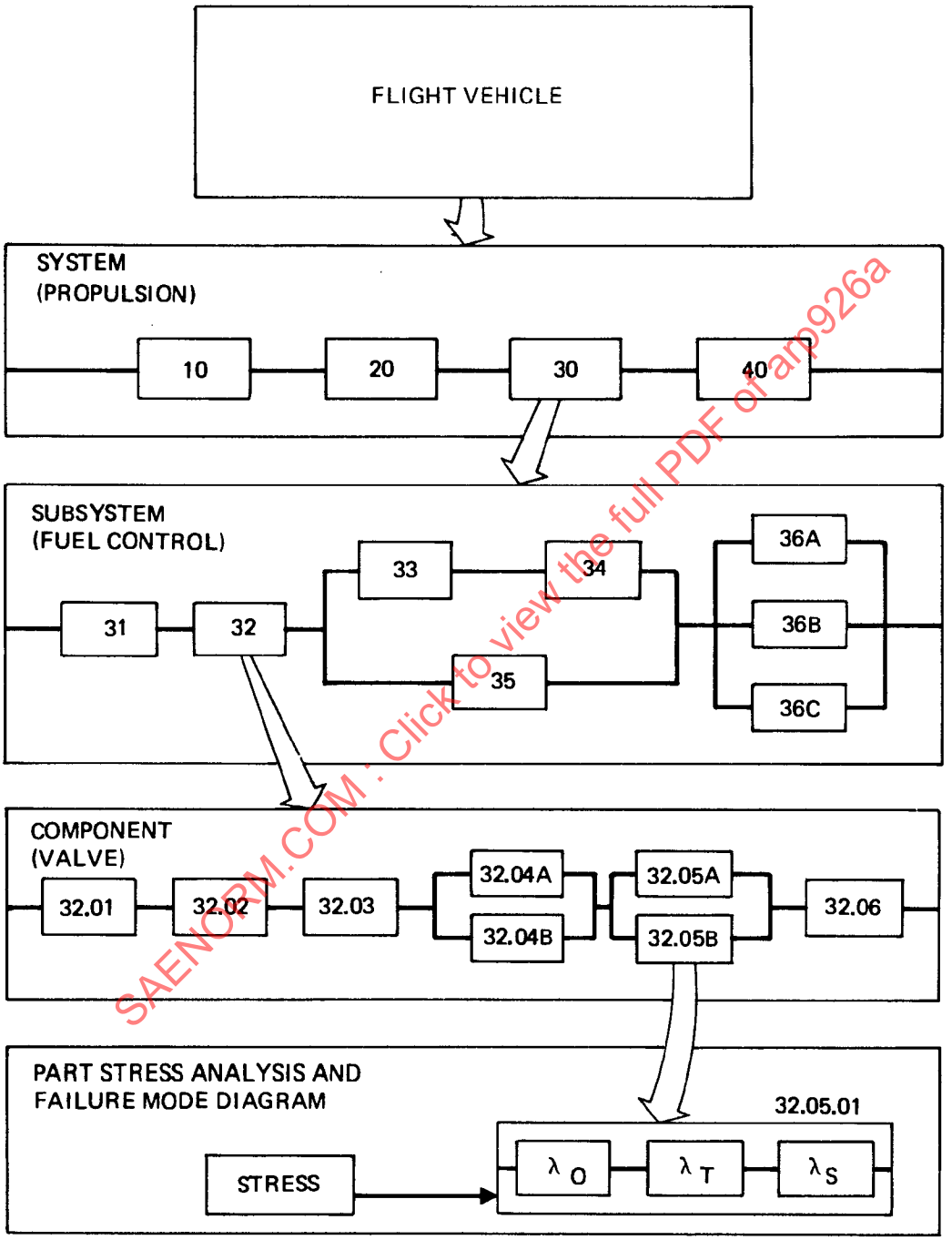


FIGURE 10
PROGRESSIVE EXPANSION OF LOGIC BLOCK DIAGRAM

d. Failure Mode Determination: For each hardware item or function, analysis of individual failure modes and system effects may be required. By examining the outputs of the reliability diagram, failure modes may be identified. Failure modes of the individual hardware item or output functions of each diagram element are postulated on the basis of the stated requirements contained in the system definition. Where system definition has not reached the piece part level, the system component will be an assembly. Where system hardware definition has not reached the stage of identifying system functions with the specific type of hardware that will perform these functions, the F/FA should be based upon failure of the system functions, stating the general type of hardware envisioned as the basis for system design.

d. 1. Top Down Technique: In the Top-Down Technique, the initial effort is to identify the failure modes at the top functional subdivision level. This is done by first establishing a list of failure effects that could occur at the highest level. These effects are the loss or degradation of one or more output parameters of the system. For example, in a voice and data communications system, failure effects could include loss of transmitter output, no receiver output, distorted output, and total inoperation, among others. Another failure effect category is the occurrence of something that is not desired such as some form of output when none should occur. For any of these failure effects, it is pertinent to establish, at the next lower functional tier, the failure mode that could occur to produce the specific failure effect under consideration. Thus, the loss of transmitter output could relate to a short circuit or open circuit failure mode at some point in the transmitter, resulting in loss of signal or power. Each functional subdivision of the transmitter (antenna, output stage, driver, modulator, etc.) is then considered with regard to what failure mode, for each overall functional assembly, could result in the failure effect under consideration. A list of all relevant failure modes is compiled. Each of these, in turn, can be considered a failure effect for the purpose of identifying failure modes at the next lower functional tier (subassembly or circuit). Again, relevant failure modes are added to the list. The procedure is iterated for successively lower functional tiers until the lowest level of interest has been considered. Through this procedure, all of the failure modes, at any functional level, that can result in any specific failure effect become identified. The complete routine is essentially a deductive analysis.

d. 2. Bottom-Up Technique: Application of the Bottom-Up Technique is initiated by selecting the lowest level of interest (usually either the parts, circuit, or module level). At this lowest level the various failure modes that can occur for each item at that level are tabulated. The corresponding failure effect, in turn, is interpreted as a failure mode for consideration of the failure effect at the next higher functional level. Successive iterations result in the eventual identification of the failure effects at all functional levels-up to the system or highest level in relation to specific failure modes. This Bottom-Up Technique is in essence one of inductive synthesis.

The procedures for identifying failure modes and related failure effects can often be effectively employed in a hybrid relationship. Where the procedure is initiated as a Bottom-Up Technique, it is desirable to determine not only what the failure effects are in the direct functional chain to higher levels, but also what happens in related elements at the same functional level as well as the interactions that could result at lower levels within any of these related elements. Similarly where the initial procedure is Top-Down, it is significant to consider what all of the higher level effects are that could result from lower level failure modes initially identified with a particular higher level failure effect. This is especially pertinent where an intermediate function feeds or couples directly to more than one higher level function.

e. Operating and Maintenance Conditions: Operating conditions include the equipment item's operational profile and the environmental conditions prevailing during the various periods of operation. The operational profile is defined in terms of the operating phase in which the system is operational. The sequence of functions necessary for system success and the duty cycle of system components are elements of the operational profile that must be considered. The pertinent environmental conditions during each phase of operation should be established by reference test or assumption. The definition of environmental conditions should encompass all the factors that might affect the intent of the analysis. The anticipated maintenance conditions affecting the system should also be noted.

f. Failure Causes and Mechanisms: An understanding of failure causes and mechanisms can be beneficial in assessing the effects of a failure mode. Failure causes and mechanisms are used to estimate the probability of a failure mode occurring and to determine possible secondary failure effects, failure cause, and the source for corrective action. Many times the conclusions of the analysis translate directly into recommendations for design improvement.

g. Failure Effects: The effects of the failure mode being analyzed on the system itself must be described. A brief description of the effect of the failure on the next higher level of the functioning entity within the system is recorded. Finally, a description of the effect of the item failure on the system being analyzed is recorded. For lower level items where effects on the overall system are unknown, the effects of a failure on the system under analysis may be described as loss of system inputs or outputs.

h. Failure Detection: Another F/FA consideration is the method of detecting failures. Many equipment items are concerned with a ground checkout phase followed by an operational phase where, if the failure is detected during checkout, reaction time to a failure may not be critical. In operation, however, reaction time may be critical since, if a failure occurs, there may not be sufficient warning or time for corrective action. It may be necessary that a description of the technique for detecting the failure be shown in the F/FA. Failure detection is also used to establish severity and criticality level of failure effort.

Redundant subsystems are often analyzed on the assumption that all elements are operational at the start of a mission; hence, subsystem failure generally involves the occurrence of two or more independent failures during the same mission. In many practical cases, one or more elements are not checked between missions and a failure is not ordinarily detectable in operation unless other elements also fail. Where a redundant subsystem is provided, consideration should be given to undetected failures and the exposure time to such undetected failures (see 3.5.2).

i. Quantification: When quantification is appropriate, the data elements needed are: (1) the failure rate for each different item at the lowest functional level (i.e., part or module) for which failure modes have been employed, (2) the various failure modes that can occur for each of these items, and (3) the fraction of the total failure rate attributable to each of the identified failure modes. The first element is the customary failure rate value, including all types of failure or failure modes of the part such as is given in MIL-HDBK-217, RADC Reliability Notebook, or GIDEP. The second element includes all identifiable failure modes for the part without considering the fraction of total part failures that can be expected to occur in each failure mode category. The following tabulation is a sample listing of the second and third data elements for a fixed paper capacitor:

FAILURE MODE	FRACTION OF ALL PARTS FAILURES
Short	0.4
Open	0.1
Excessive leakage current	0.3
Capacitance drift beyond acceptable limits	0.2

On the basis of the qualitative analysis, which identifies those individual parts and their particular failure modes that pertain to the specific failure effect under consideration, each part type and the applicable failure modes are compiled in a list. The product of the part failure rate and its applicable failure mode fraction provides the effective failure rate for that part applicable to the failure effect of interest. The summation of products for all parts then provides the total failure rate for the failure effect of interest.

4.2.5 Evaluate Criticality: If a criticality analysis is required by contract or established as part of the plan, loss frequencies of each identified failure mode shall be derived. Values of severity level and loss frequency will be used to insert failure mode identification numbers into a matrix indicating the distribution of failure mode criticality.

4.2.6 Recommend Design Improvements: For the F/FA to contribute to the development process, conclusions which indicate significant cost-effective design improvements or a requirement for further testing shall be clearly documented. Throughout the performance of the F/FA, emphasis shall be placed on the earliest reasonable identification and resolution of critical failure modes. All failure modes defined during the analysis as unacceptable shall be documented and investigated, and design improvement recommendations shall be made to eliminate the failure mode or reduce the loss frequency to an acceptable level. All potential failure shall be reviewed to determine the effect on maintenance or personal safety, the effect on any induced human response, and the indication of failure at the man-machine interface. Recommendations for corrective action shall be made as the unacceptable failure modes are detected and shall be made as early in the development process as possible. The relative urgency and priority for corrective action for each critical failure made shall be identified and clearly established.

4.2.7 Analysis Summary: The final step of the F/FA process is to provide a concise summary of the recommendations and action items for design improvement. The analysis summary should include a compilation of notes and recommendations from the worksheet remarks column, a design evaluation summary of the major problems detected by the F/FA general conclusions, and recommendations.

4.3 FMEA Hardware and Functional Approaches:

4.3.1 FMEA Hardware Approach:

4.3.1.1 Purpose: The basic objective of an FMEA is to determine each possible mode of failure within an equipment item and the effect of each mode of failure on the overall equipment or portion thereof. A detailed analysis using the hardware approach is initiated by tabulating each individual equipment item which is then analyzed. Failure effects on performance of the item iteself and on other hardware system elements are then determined and become the failure modes at the next higher indenture level.

4.3.1.2 Application: The hardware approach is the more rigorous method of conducting an FMEA and is normally used whenever the hardware items can be identified from engineering drawings. While the hardware approach is normally utilized from the part level up, it can be initiated at almost any indenture level and can progress in either direction.

4.3.1.3 FMEA Hardware Procedure: The failure modes and effects analysis and its documentation at the hardware level are accomplished by completing the columns of a FMEA format similar to that given in Fig. 11 as follows:

Column Number	Explanation or Description of Entries
(1)	Name of system function or component under analysis for failure mode and effects. Breakdown of a system for analysis should normally be to the lowest practicable level at the time of the FMEA.
(2)	Drawing identification number by which the analyst identifies and describes each component or module. These drawings should include configuration, mechanical, and electrical characteristics.
(3)	Reference designation used by the manufacturer to identify the component or module on the schematic. Application schematic and drawing numbers should also be listed.
(4)	Identification number of the FMEA reliability logic block diagram and of the function.
(5)	Concise statement of the function performed.
(6)	The specific failure mode investigated, after consideration of the four basic failure conditions: Premature operation. Failure to operate at a prescribed time. Failure to cease operation at a prescribed time. Failure during operation. For each applicable failure mode, describe the cause, indicating operational and environmental stress factors, if known.
(7)	Phase of mission in which critical failure occurs, e.g., taxi, take-off, climb, cruise, descent, approach, flare-out, roll, etc. Where the subphase, event, or time can be defined from approved operational or flight profiles, the most definitive timing information should also be entered for the assumed time of critical failure occurrence. This time information should also be given for the failure effects under the columns titled "Failure Effect On."
(8)	A brief statement describing the ultimate effect of the failure on the function or component being analyzed. Examples of such statements are: "component rendered useless," "component's usefulness marginal," or "structurally weakened to unacceptable reliability level." Timing information as described under (7) should be given as to time of failure effect.
(9)	A brief description of the effect of the failure on the next higher assembly. Timing information as described under (7) should be given as to time of failure effect.

(10) A description of the effect of the component failure on the uppermost system. For major systems, these effects are divided into two groups: 1. failures affecting operational success (examples: operation ended, limited operation, degrade operational objectives, delay, fail to start operation, etc.); and 2. personnel safety (examples: total loss of life, personnel injury, etc.). For lower level systems where effects on the overall system are unknown, a failure's effects on the system under analysis may be described as loss of system inputs or outputs (examples: loss of signal output, loss of output pressure, shorted power input).

(11) A description of the methods by which the failure could be detected. Identify which of the following categories the failure detection means fall under:

On-board visual/audible warning devices.
Automatic abort-sensing devices.
Ground operational support system failure-sensing instrumentation.
Flight telemetry, ground support equipment console display, etc.
None

Timing information as described under (7) should be given with respect to the reaction time available between time of component failure, time of detection, and time of critical failure effect.

(12) A description of what corrective actions the flight crew and the ground crew could take to circumvent the failure. If applicable, the time available for effective action and the time required should be noted.

(13) List the design (or other) provisions which have been made to reduce criticality.

(14) This column may be used to identify pertinent information not included in the other columns.

4.3.2 FMEA Functional Approach:

4.3.2.1 Purpose: The functional approach is initiated by listing equipment functions at the initial indenture level. Failure modes contributing to nonconformance of the desired functions are then analyzed and failure effects are determined which become the failure modes at the next lower indenture level. The procedure is continued down or up to indenture levels as determined by the analysis to identify all critical items.

4.3.2.2 Application: The functional approach is normally used for those cases where hardware system definition has not reached the point of identifying specific hardware items, or in those situations where hardware system complexity is such that an analysis from the initial indenture level-down approach is the more practical procedure to follow. This method of analysis is not as cumbersome and difficult to follow as the hardware approach. While the functional approach is normally utilized from an initial level down, it can be initiated at almost any indenture level and can progress in either direction.

4.3.2.3 FMEA Functional Procedure: The following procedural steps should be used in performing the functional FMEA. A typical example of an FMEA is shown in Fig. 11:

Step 1 - Define the system and then break it down into functions.
Step 2 - Construct a block diagram as shown in Fig. 12.
Step 3 - Establish ground rules and assumptions for performing the analysis.
Step 4 - Identify failure modes, effects, failure detection methods, and other worksheet requirements.
Step 5 - Evaluate criticality of the failure modes.

System Propulsion

Subsystem Pneumatic Control

Equipment RD-400 Flight AS 340

Module Stage 2 GSE

FAILURE MODE AND EFFECTS ANALYSIS

Page 1 of 2 Pages

Date January 15, 1979

By John Doe

Approved

Item Identification				Function (5)	Failure Mode (6)	Operation Phase (7)	Failure Effect On			Failure Detection Method (11)	Corrective Action Time Available/Time Required (12)	Design Provisions To Reduce Criticality (13)	Remarks (14)
Name (1)	Dw. Ident. Number (2)	Drawing Reference Designation (3)	Reliability Logic Diagram Number (4)				Component/ Function (8)	Next Higher Subsystem (9)	Uppermost System (10)				
Disconnect	BL-26	A24729 C 85M0963 (Schematic)	11.01	Provide means of connecting GSE 2nd stage to transfer He	Fail to engage	Countdown	Ability to transfer He is lost	Loss of pressurization in the control system	May cause launch delay	Visual	One hour required to replace disconnect. Recycle of countdown required if failure occurs after T-4 hours.	Improved detect device now in use, plus special material seals to eliminate leakage	This newly designed disconnect has been thoroughly Lab tested in addition to two successful flights.
					External leakage	Countdown & powered flight	Ability to transfer He is degraded	Ability to fill or drain He tanks is degraded	None Redundance is provided by check valve	Visual			
					Failure to disengage	Countdown	None	None	May cause launch delay	Visual			
Valve-Pilot	ZA-01	674296 B 65M1832 (Schematic)	11.02	To control operation of propellant tank shutoff valves. Shutoff valves are closed by opening this pilot valve and opened by closing this valve.	Fail to open	Powered flight	Ability to close propellant tank shut-off valve is lost.	None; Propellant is consumed and subsystem has completed its mission	None	Telemetry	Four hours required to repair pilot valve. Necessary to scrub mission if failure occurs after T-46 hrs.	None	
					Failure to close	Powered flight	Ability to open propellant tank shut-off valve is lost.	Loss of thrust (propellant starvation)	Actual mission loss	Visual Telemetry			
					Failure to remain open	Countdown	Ability to keep propellant tank shut-off valve closed is lost	Possible delay in launching	Possible delay in launching	GSE signal			
						Powered flight		Probable loss of thrust due to pump cavitation	Probable loss of mission	Telemetry			
					Failure to remain closed	Powered flight	Ability to keep propellant tank shut-off valve open is lost	Loss of thrust (propellant starvation)	Actual mission loss	Telemetry			

FIGURE 11
WORKSHEET EXAMPLE FOR FMEA USING HARDWARE APPROACH

Step 6 - Provide for the required corrective action in the design or manufacturing process and for evaluation of the corrective action adequacy.

Step 7 - Document the analysis and provide recommendations for those items which could not be corrected by design or manufacturing process and changes which should be imposed as maintenance requirements in order to ensure that the inherent reliability is achieved.

4.4 Criticality Analysis (CA) Procedure:

4.4.1 Elements of the CA: The CA format may be varied to meet specific program requirements. Figs. 28 and 29 in Appendix B have been partially completed with typical information and serve as examples of the type of information to be recorded on the worksheets.

4.4.1.1 Critical Failure Mode Identification: The first step of the CA is to identify the critical failure modes from the FMEA, fault tree analysis, or other F/FA methods. Critical failure modes at the higher levels in the overall system should be identified according to established undesired events similar to the following examples:

Category I: Failure which results in potential loss of life.
Category II: Failure which results in loss of ability to perform a critical required function.
Category III: Failure which results in delay or loss of operational availability.
Category IV: Failure which results in excessive unscheduled maintenance.

At the lower system levels where it is not possible to identify critical failure modes according to the undesired event of this type, undesirable event statements based upon loss of system inputs or outputs should be used.

In evaluating the criticality of a failure mode the following factors should be taken into account:

a. Monitorability. A measure of confidence in being able to detect (and to act upon detection) that the failure has occurred. (When system self-tests - preflight, inflight, or on-line monitoring - are used, an evaluation of test effectiveness should be included.)

b. Exposure time. The period of time since the system, or a given portion of the system, was known to be good. If the failure is critical for a specific phase of flight, but is also monitorable, the exposure time for that flight phase should be considered. For example, in automatic landing systems, certain critical failures have an exposure time of between 10 and 20 seconds due to monitoring capabilities and the limited time between alert height and touchdown.

c. Probability. Given that a failure is undetectable, or only monitorable under certain conditions, its resulting exposure time may be significant. The probability should be considered that other specific failures may combine within the defined exposure time to result, in the aggregate, in a critical failure effect. At some point, the failure combinations become so improbable that the failure need no longer be considered. The requirement for how improbable must necessarily be a function of the application.

4.4.1.2 Criticality Rate Determination: The second step of the CA procedure is to determine probabilities of the critical failure modes occurring or alternately, criticality number calculations.

a. Failure Probability Determination: The probability of each postulated, identified failure mode occurring can be assessed by means of a numerical estimate. This probability provides a measure of the expected number of occurrences of each identified failure mode during a specific time interval. The probability of a particular failure mode occurring is the combined probability of the occurrence of all the identified causes for that failure mode. The following sample guidelines are suggested for developing definitions for failure probability levels in relative terms. They may be modified or expanded depending on the equipment being analyzed and the amount of reliability data available.

a. 1 Level 1 (very low): Any single failure mode probability which is less than 0.01 of the overall probability of failure during the item operating time interval.

a. 2 Level 2 (low): Any single failure mode probability which is more than 0.01 but less than 0.10 of the overall probability of failure during the item operating time interval.

a. 3 Level 3 (medium): Any single failure mode probability which is more than 0.10 but less than 0.20 of the overall probability of failure during the item operating interval.

a. 4 Level 4 (high): Any single failure mode probability which is more than 0.20 of the overall probability of failure during the item operating interval.

b. Criticality Number Calculation: A criticality number for an equipment item is the number of failures of a specific type expected per some predefined appropriate number of cycles due to the item's critical failure modes. The specific type of failure is expressed by the critical failure mode undesired event discussed in 4.4.1.1. For a particular undesired event and operational phase, the Cr for an item with critical failure modes is calculated with the following formula:

$$Cr = \sum_{n=1}^{j} [(\text{alpha})\ (Ke)\ (Ka)\ (\text{lambda}_o)\ (t)\ (\text{beta})\ (10^6)]_n$$

$$n = 1, 2, 3, \ldots, j$$

where:

Cr = Criticality Number for the item in losses per million hours or cycles.

j = Last critical failure mode in the item for the particular undesired event category.

n = The critical failure modes in the item that fall under a particular undesired event category.

alpha = The fraction of lambda_o attributable to the critical failure mode.

Ke = Environmental factor which adjusts lambda_o for difference between environmental stresses when lambda_o was measured and the environmental stresses under which the component is going to be used. The environmental stresses are those stresses induced by sources external to the system such as vibration, sand, dust, humidity, shock, temperature, etc. The environmental factor Ke for operation under laboratory conditions using a generic failure rate is equal to 1.

Ka = Operational factor which adjusts lambda_o for the difference between operating stress when lambda_o was measured and the operating stress under which the item is going to be used. The operating stresses are those system internal stresses such as voltage, power, temperature, pressure, stress reversals, etc. The operating factor Ka for operation under laboratory conditions using a generic failure rate is equal to 1.

lambda_o = Generic failure rate of the item in failures per hour or cycle. The generic failure rate of an item is the failure rate that an item would be expected to have when operated under laboratory conditions and will normally be the lowest operation failure rate that can be expected.

t	=	Operating time in hours or number of operating cycles of the item.
beta	=	Conditional probability that the failure effects of the critical failure mode occur, given that the critical failure mode has occurred.
10^6	=	Factor which transforms Cr from losses per cycle or hour to losses per million cycles or hours so Cr will normally be greater than one.

The factor beta is the probability of loss and should be selected from an established set of ranges such as:

Failure effects	Typical value of beta
Actual loss	1.0
Probable loss	0.1 to 1
Possible loss	0.0 to 0.1
None	0.0

4.4.2 Documenting the Criticality Analysis: Individual worksheets should be designed for the particular analysis being performed. Detailed worksheet design will also depend upon the use of a qualitative or quantitative approach. The CA can be documented on the same worksheets with the F/FA methods, or separate worksheets can be used if desired. If separate worksheets are used, sufficient columns from the FMEA should be duplicated on the CA worksheets to permit data tracking. Examples of CA worksheets are shown in Appendix B, Figs. 28, 29.

4.4.3 Criticality Analysis Summary: A summary list of critical items can be made from the information derived from the Criticality Analysis. There are several methods to accomplish this list and the method used should be tailored to the needs in each case. Generally, this list will include groups of critical items with each group in descending order of criticality number for a given loss statement.

4.4.4 Criticality Matrix: The criticality matrix displays the severity distribution of the failure modes and can be used for the assignment of corrective action priorities. The matrix is constructed by scaling failure probability of criticality numbers as the ordinate and level of severity values as the abscissa. Failure mode identification numbers are then inserted in the matrix in their respective locations. If the number of critical items is sufficiently large, a critical items list may be needed in addition to the matrix.

4.5 Fault Tree Analysis Procedure: The principles of fault tree analysis are straightforward and easy to grasp. The notation to be used and the discipline to be followed ought to be learned before trying to construct a fault tree for a system. Although fault tree analysis may be considered tedious and time consuming, it can be most profitable. Ordinarily, it is done in conjunction with an FMEA because both of the analyses deal with causes and consequences. The bookkeeping aspects - i.e., the keeping track of each item, its states (conditions) which are to be considered, and its place in the hierarchy - are very important because mistakes are so easy to make. Unless a strict discipline of labeling items and their states is followed, it is easy to make errors in identifying items; e.g., two different codes might be assigned to one item.

During the course of constructing the fault tree, much will be learned about the system; in fact, this scheme of knowledge organization is useful precisely because it does require that the analyst know or make explicit assumptions about the relationships of items in the system.

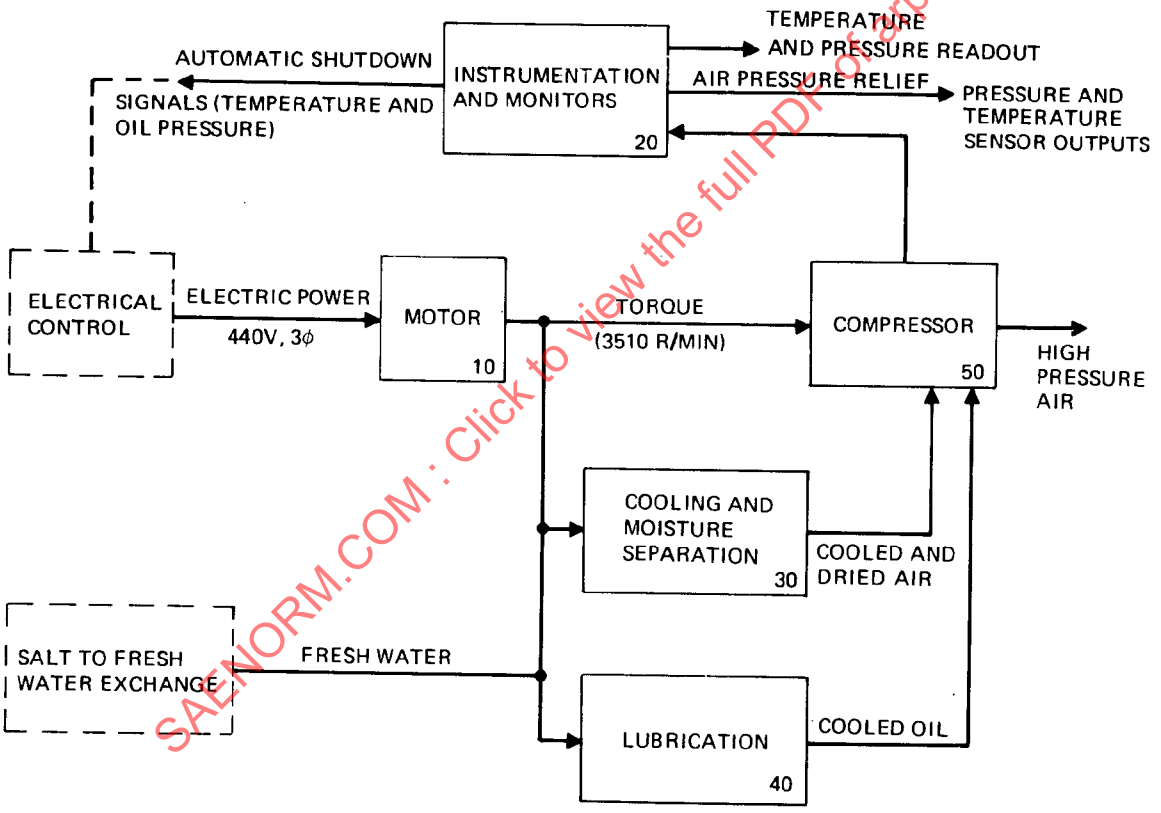


FIGURE 12
EXAMPLE FUNCTIONAL BLOCK DIAGRAM FOR AIR CONDITIONING SYSTEM

Fault Tree Analysis involves the following steps:

a. Define the type of analysis application desired (whether safety, reliability, maintainability, or whatever).
b. Define the top fault tree event appropriate to that application. For each top event and its tree, the following apply.
c. Establish the system criteria by which to judge whether or not fault and failure events can lead to the top event.
d. Gather the definitive system data and analyze it to determine the possible fault and failure events which violate system success criteria, thereby leading to the top event.
e. Construct the fault tree, showing the top event and its branching causes, interconnected by appropriate, conventional fault tree logic symbols.
f. Extend the branches to connect each fault and failure event with its possible causes by appropriate logic symbols, tracing each event to its root causes or to the selected level of interest suiting the analyst's needs.

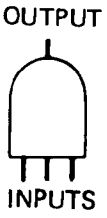
4.5.1 Fault Tree Symbols: Two kinds of symbols are conventionally used in a fault tree: logic symbols as shown in Fig. 13 and event symbols as shown in Fig. 14. An example of their use is illustrated in Fig. 15. The logic symbols are used to interconnect the events that contribute to the specified main top event. The logic symbols most frequently used are the basic AND and OR Boolean logic gates. The AND gate provides an output event only if all input events occur. The OR gate provides an output event if any one or more of the input events occur.

The usual event symbols are the rectangle, circle, and diamond. The rectangle designates an event resulting from the combination of other, more basic events acting through a logic gate. Events designated by circles and triangles are treated as primary events. The circle designates a primary failure event that is usually independent of all other events designated by circles and diamonds. The diamond designates an event that is also considered primary in the given fault tree, although the event is not primary in the sense that laboratory data are applicable; rather, the diamond event is simply not developed further, because it is of insufficient consequence or necessary information is unavailable. To quantitatively solve a fault tree, both circles and diamonds must usually be used to represent events for which quantitative reliability information is necessary to the fault tree.

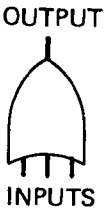
The triangle indicates a transfer from one part of the fault tree to another. A line from the side of the triangle (making it a transfer-out triangle) denotes an event transfer out from the associated logic gate from the transfer-out triangle with the same identification number.

4.5.2 Minimal-Cut Sets: The analyst must be aware of the lack of independence of two or more primary failures in the fault tree if he is to avoid serious errors in his qualitative and quantitative conclusions. Lack of independence can occur in two ways: (1) whenever the same event appears more than once in the fault tree (this situation exists wherever an upright triangle transfer symbol is used or could be used), or (2) when certain single failures can result in more than one fault event simultaneously (many such "common-cause" failures can be pointed out in a detailed fault tree analysis, but it does not do so inherently). By determining the minimal-cut sets, as described below, the analyst can be alerted to these two situations.

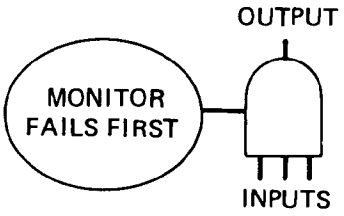
A minimal-cut set in a fault tree is a smallest set of primary events, inhibit conditions, and/or developed events which must all occur in order for the TOP event to occur. The minimal-cut sets represent the modes by which the TOP event can occur. For example, in the fault tree shown in Fig. 16, the minimal-cut set AB means that both primary events A and B must occur in order for the TOP event to occur and that the occurrence of A and B is a mode by which the TOP event occurs. If either A or B does not occur, then the TOP event does not occur by this mode. AC is another minimal-cut set in this example. The set of events ABC, where C is another primary event, is not a minimal-cut set, because C is not necessary for the occurrence of the TOP event. C can either occur or not occur, and so long as A and B both occur, then the TOP event will occur. The complete set of minimal-cut sets (AB and AC in this example) includes all the failure modes by which the TOP event occurs.



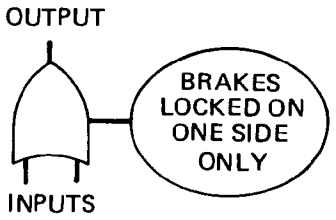
The "AND" gate describes the logical operation whereby the coexistence of all input events is required to produce the output event.



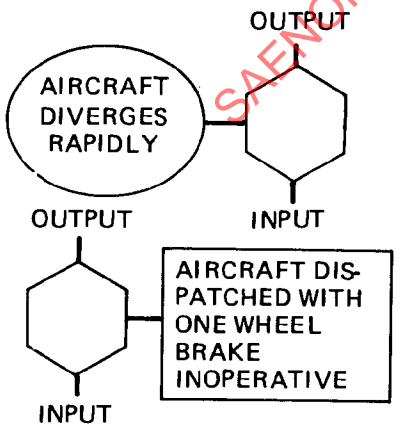
The "OR" gate defines a situation whereby the output event will exist if one or more of the input events exist.



The "Priority AND" gate performs the same logic function as the "AND" gate with the additional stipulation that sequence as well as coexistence is required.

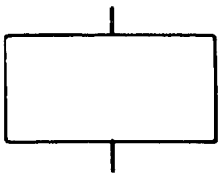


The "Exclusive OR" gate functions as an "OR" gate with the restriction that specified inputs cannot coexist.

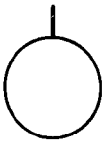


"INHIBIT" gates describe a causal relationship between one fault and another. The input event directly produces the output event if the indicated condition is satisfied. The conditional input defines a state of the system or a specific failure mode that permits the fault sequence to occur and may be either normal for the system or result from failures. It is represented by an oval if it describes a temporary condition that permits a fault sequence to occur; a rectangle is used to indicate a condition that is presumed to exist for the mission life of the system.

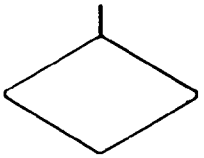
FIGURE 13
LOGIC OPERATIONS (GATES)



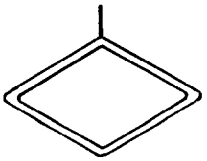
The rectangle identifies an event that results from the combination of fault or failure events through the input logic gate.



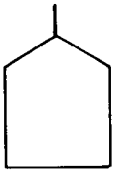
The circle describes a primary failure event that requires no further development. Frequency and mode of failure of items so identified are derived from empirical data.



The diamond describes an event that is considered primary in a given fault tree. The possible causes of the event are not developed, either because the event is of insufficient consequence or the necessary information is unavailable.



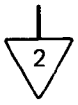
The double diamond is used in the simplification of a fault tree for numerical evaluation. The event described results from the causes that have been identified but are not shown on a particular version of the fault tree.



The "house" indicates an event that is normally expected to occur, such as a phase change in a dynamic system.

Triangles are used as transfer symbols. A line from the top of the triangle indicates a "transfer in" and a line from the side denotes a "transfer out."

The upright triangle (△) is used where the sequence of events being transferred to another part of the fault tree is to have all identical events in both locations.



The inverted triangle (▽) is used where the sequence of events being transferred to another part of the fault tree is to have one or more different events in the second location but is to be identical in function.

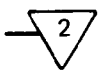


FIGURE 14
EVENT REPRESENTATIONS

(1) OR gate
(2) AND gate
(3) Transfer "in"
(4) INHIBIT gate with condition
(5) Transfer "out"
(6) Top undesired event
(7) Commanded failure
(8) PRIORITY AND gate
(9) Primary failure
(10) Expected event
(11) Undeveloped fault event

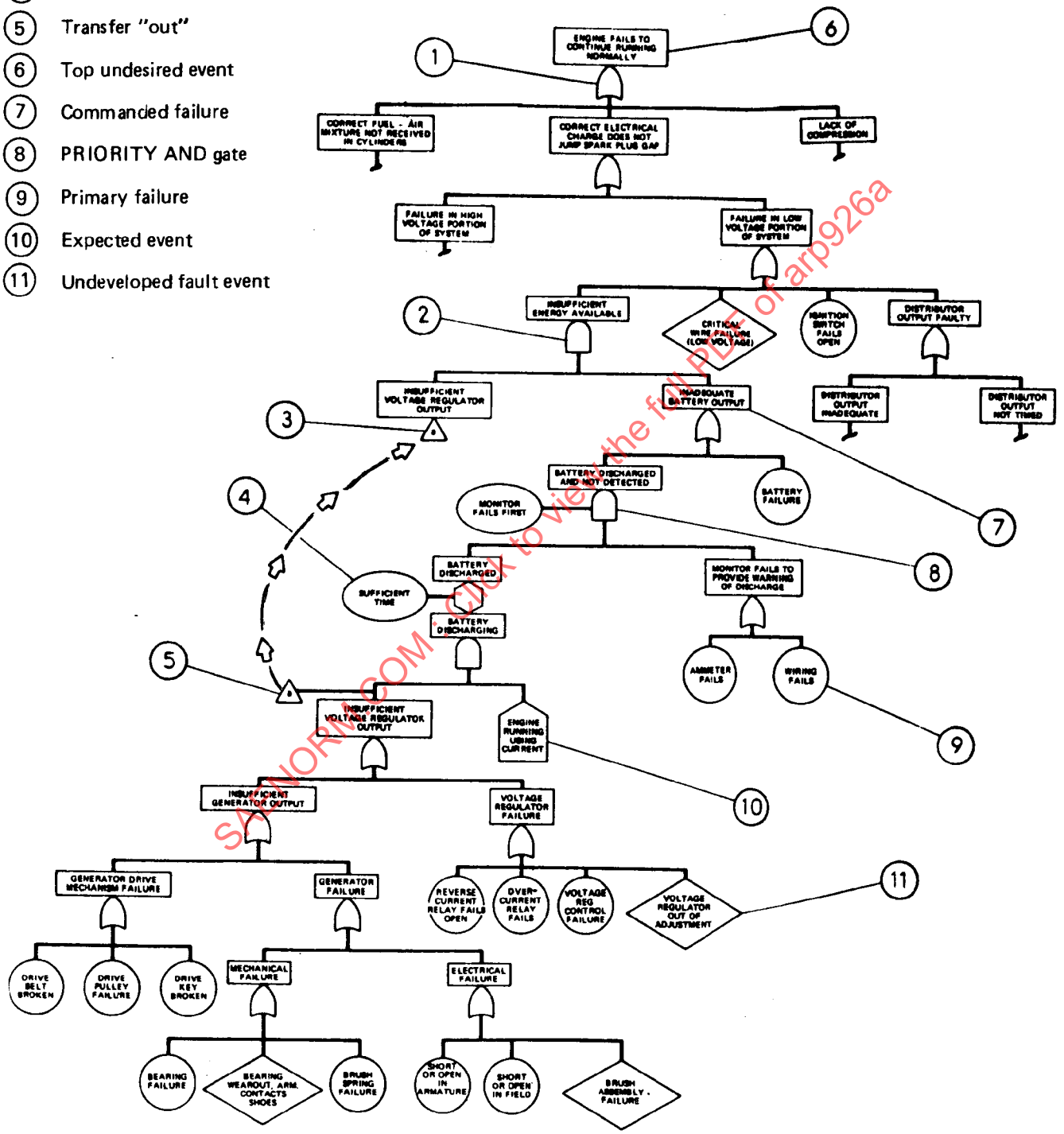


FIGURE 15
SECTION OF AN AUTOMOTIVE FAULT TREE

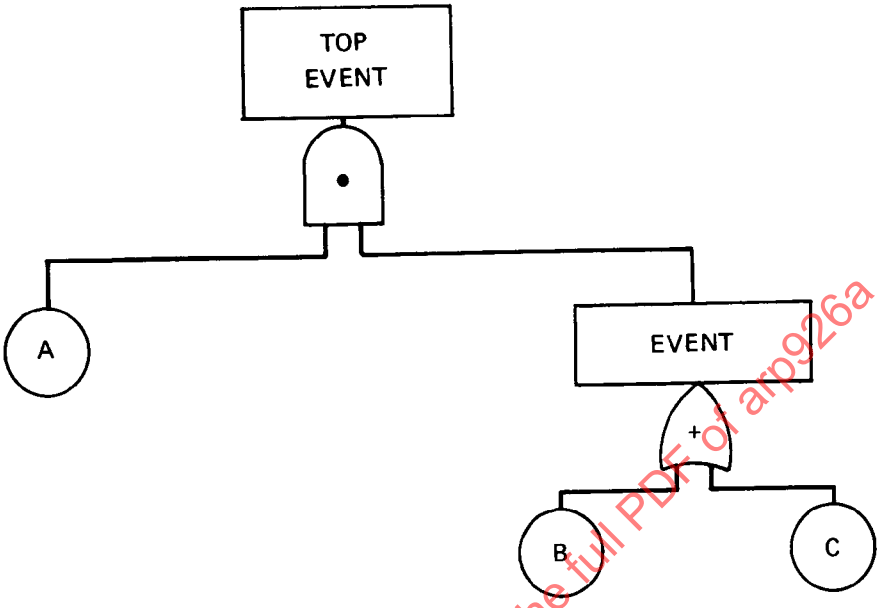


FIGURE 16
FAULT TREE

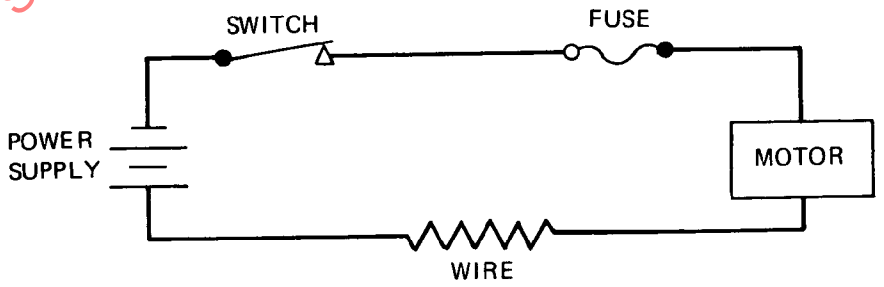


FIGURE 17
SAMPLE SYSTEM

The minimal-cut sets, because they depict which failures must be repaired in order for the TOP fault to be removed from the failed state, point out the weakest links in the system.

4.5.3 System Definition: System definition is often the most difficult task associated with fault tree analysis. Ofprimary importance is a functional layout diagram of the system showing all functional interconnections and identifying each equipment item. An example might be a detailed electrical schematic diagram. Physical system bounds are then established to focus the attention of the analyst on the precise area of interest. Sufficient information must be available for each of the equipment items to allow the analyst to determine the necessary modes of failure of the items. This information can come from the experience of the analyst, from the technical specifications of the items, or from another F/FA.

4.5.3.1 Top Event Selection: The TOP event must then be established. The TOP event defines the situation for which the fault tree is to be drawn. For any given system, there may be many possibilities for TOP events, and the selection must be made with care. The initial configuration must represent the system in the unfailed state. Consequently, system boundary conditions depend on the TOP event. Initial conditions are then system boundary conditions that define the component configurations for which the TOP event is applicable. All items that have more than one operating state or failure mode generate an initial condition for each such operating state or failure mode.

4.5.4 Example of Fault Tree Construction: An example demonstrates some of the fundamental aspects of fault tree construction. A sample system schematic is shown in Fig. 17. The system physical bounds include this entire system. The system boundary conditions might be:

TOP event	Motor overheats
Initial condition	Switch closed
Not-allowed events	Failures due to effects external to system

For such a system with the selected TOP event given above, a fault tree like that shown in Fig. 18 could be developed. For this fault tree the minimal-cut sets are, by inspection, the sets of primary events:

a. Motor failure (overheated) (1)

b. Fuse failure (closed); wiring failure (shorted) (2 and 3)

c. Fuse failure (closed); power supply failure (surge) (2 and 4)

Although minimal-cut sets can be determined by computer programs using Boolean methods or by simulation, many fault trees can be resolved into their minimal-cut sets merely by examination of the tree as was done in this example. A key point of this method is that an AND gate alone always increases the size of a cut set, while an OR gate alone always increases the number of cut sets. The first level gate of Fig. 18 reflects the inductive reasoning that the motor overheats if an electrical overload is supplied to the motor or if a primary failure within the motor causes the overheating (for example, bearings lose their lubrication or a wiring failure occurs within the motor).

From inductive reasoning and a knowledge of the components, the rest of the fault tree shown in Fig. 18 is constructed. The event "excessive current thru motor" occurs if excessive current is present in the circuit and the fuse fails to open. The event "excessive current in circuit" occurs if the wire fails shorted or the power supply surges. The fault tree is now complete to the level of primary failures.

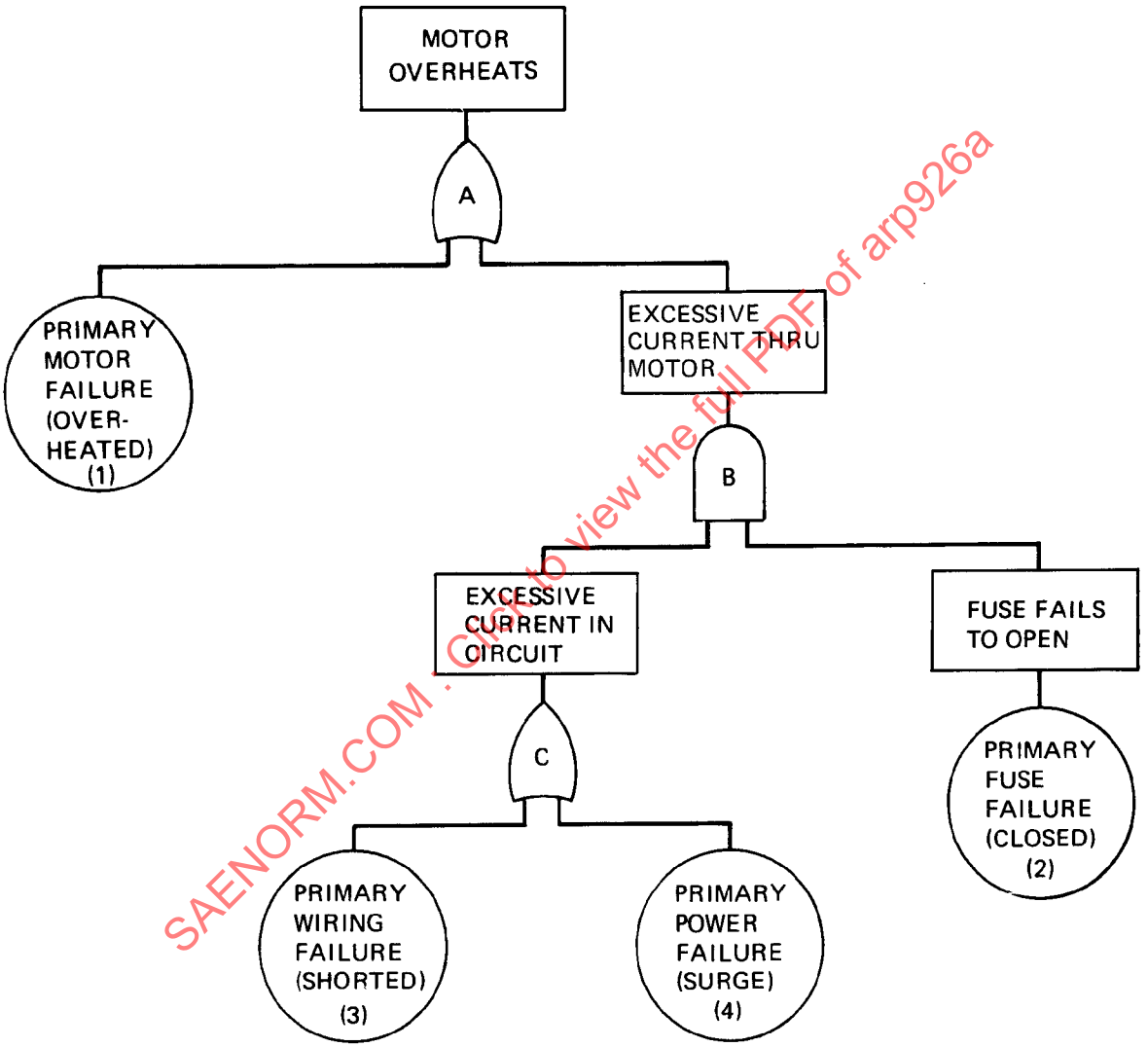


FIGURE 18
SAMPLE SYSTEM FAULT TREE

Even though the generation and analysis of fault tree nominally are separate tasks, there is a great deal of interaction between the two. During the course of analysis, engineers become aware of things they had forgotten or not realized while the tree was being generated.

Trees can be evaluated qualitatively and quantitatively. Qualitative evaluation is very profitable because so much understanding of the system is developed during the evaluation. In both qualitative and quantitative evaluations extreme care must be taken not to miss mutually exclusive and nonindependent primary failures when establishing minimal-cust sets.

4.5.5 Calculating Event Probability: There are basically two methods for solving fault trees: (1) Monte Carlo, and (2) direct analysis.

Monte Carlo methods are perhaps the most simple in principle but in practice can be expensive. Since Monte Carlo is not practical without the use of a digital computer, it is discussed in that framework. The most easily understood Monte Carlo technique is called "direct simulation." The term "simulation" frequently is used in conjunction with Monte Carlo methods, because Monte Carlo is a form of mathematical simulation. (This simulation should not be confused with direct analog simulation.) Probability data are provided as input, and the simulation program represents the fault tree on a computer to provide quantitative results. In this manner, thousands or millions of trails can be simulated. A typical simulation program involves the following steps:

a. Assign probability of failure data to primary failures within the tree.

b. Represent the fault tree on a computer to provide quantitative results for the overall system performance, subsystem performance, and the basic input event performance.

c. List the failures that lead to the undesired event and identify minimal-cut sets contributing to the failure.

d. Compute and rank basic input failures and availability performance results.

In performing these steps, the computer program simulates the fault tree and, using the input data, randomly selects the various parameter data from assigned statistical distributions, and then tests whether or not the TOP event occurred. Each test is a trial, and enough trials are run to obtain the desired quantitative resolution. Each time the TOP event occurs, the contributing effects of input events and the logical gates causing the specified TOP event are stored and listed as computer output. The output provides a detailed perspective of the system under simulated operating conditions and provides a quantitative basis to support objective decisions.

To illustrate how direct analysis might be applied to a simple fault tree for static conditions, the fault tree shown in Fig. 19 is considered. It contains independent, primary events A, B, C, and D with constant probabilities of failure 0.1, 0.2, 0.3, and 0.4, respectively. The fault tree as shown in Fig. 19 is not in convenient form because Event X1 and X2 are not independent - they both are functions of Primary Event B. By Boolean manipulation the fault tree shown in Fig. 20 is equivalent to the one shown in Fig. 19; the minimum-cut sets for both fault trees are identical. The fault tree shown in Fig. 20 is in convenient form for calculating the probability of the TOP event.

Two basic laws of probability are used in a fault tree evaluation. The Multiplication Law:

$$P\ (S \text{ and } T) = P(S) \times P(T/S) \qquad \text{(Eq. 1)}$$

The Addition Law:

$$P(S \text{ or } T) = P(S) + P(T) - P(S \text{ and } T) \qquad \text{(Eq. 2)}$$

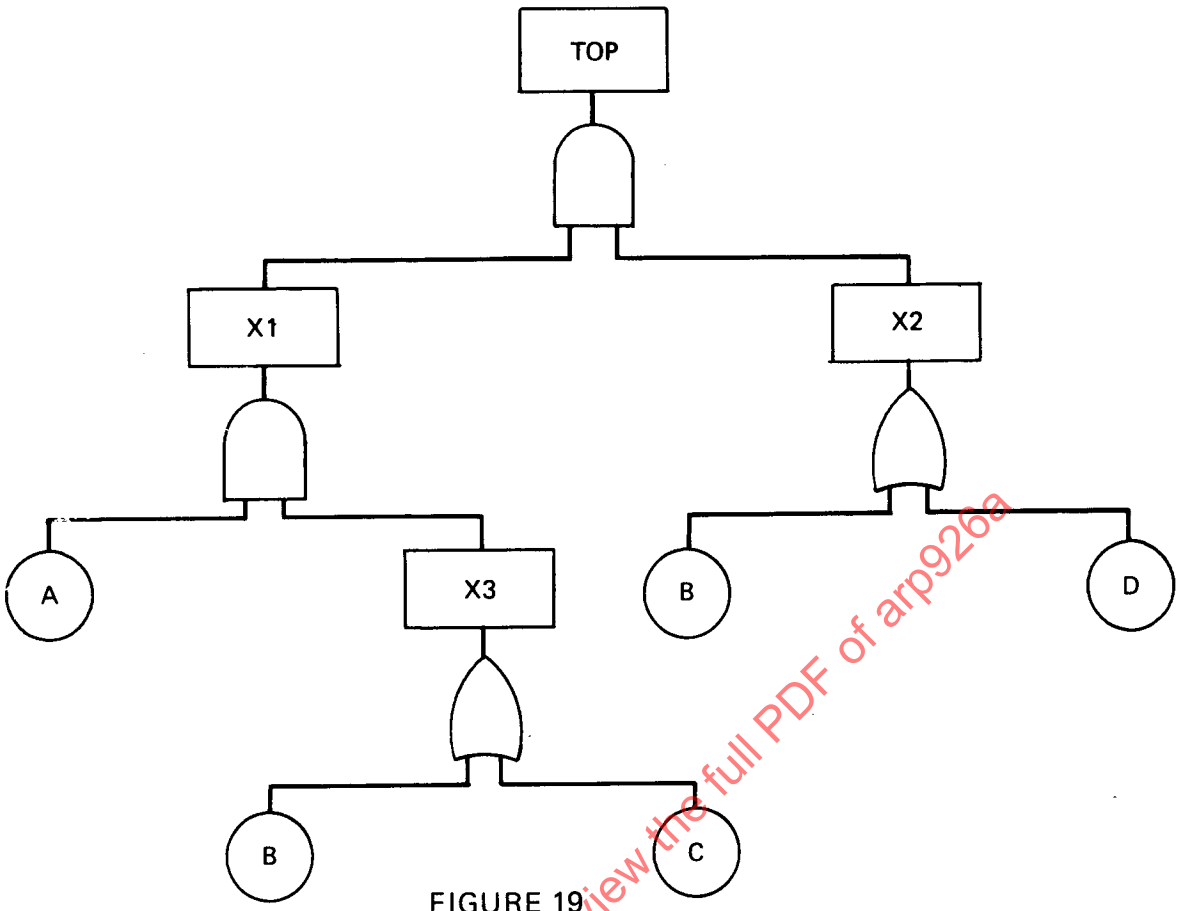
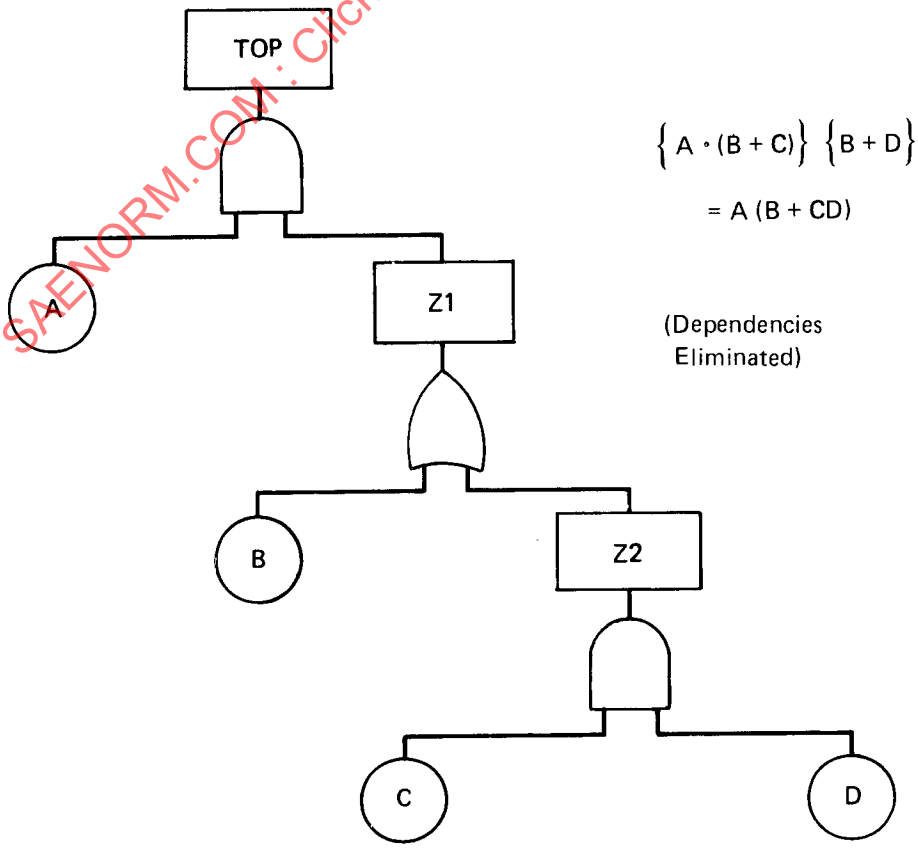


FIGURE 19
SAMPLE FAULT TREE FOR PROBABILITY EVALUATION



$\{A \cdot (B + C)\}\ \{B + D\}$

$= A\,(B + CD)$

(Dependencies Eliminated)

FIGURE 20
BOOLEAN EQUIVALENT OF SAMPLE FAULT TREE SHOWN IN FIGURE 19

Where, S, T = any two events

P(S) = probability of the noted event

P(T/S) = conditional probability of event T given event S has already occurred. If the two events are independent, P(T/S) = P(T).

Note that the word "and" has the same meaning as an AND gate in the fault tree. The logic symbol used in many texts is $\cap$, which means intersection of the events. Likewise, the word "or" has the same meaning as an OR gate in the fault tree. The logic symbol used in many texts is $\cup$, which means union of the event.

Eq. 1 states that the probability of an intersection of two events is the probability of one, P(S), times the probability of the other, given the occurrence of the first event. In terms of the fault tree in Fig. 20, the probability of a 2-event AND gate is the product of the probabilities of the two attached events, because primary events of a fault tree are independent; if not, special precautions must be taken as previously discussed. Note that this is the case in Fig. 19 because X1 and X2 are not independent as B is common to both branches.

Eq. 2 states that the probability of a union of two events is the sum of the probabilities of the individual events minus the probability of their intersection. In terms of the fault tree, the probability of a 2-event OR gate is the sum of probabilities of the two events attached to the gate minus the probability of two events both occurring.

Since all events are independent in the fault tree shown in Fig. 20, unlike the events of the tree shown in Fig. 19, the event probabilities are as follows:

$$P(Z2) = P(C) \times P(D)$$

$$P(Z1) = P(B) + P(Z2) - [P(B) \times P(Z2)]$$

$$P(TOP) = P(Z1) \times P(A)$$

The probability of the system being in the failed state is 0.0296 for the given primary event failure probabilities. This fault tree has two minimal-cut sets, AB and ACD. Primary Event A appears in both minimal-cut sets and hence is most crucial to the system. If the P(A) can be reduced to one-half of its original value, i.e., from 0.1 to 0.05, the system failure probability is reduced to 0.0148, or one-half its original value.

PREPARED BY

SAE COMMITTEE S-18, AD HOC COMMITTEE
TO UPDATE ARP 926

APPENDIX A: BIBLIOGRAPHY

1. AMCP-706-200, U.S. Army Materiel Command, Engineering Design Handbook, January 1976, "Development Guide for Reliability, Part 6, Mathematical Appendix and Glossary"

2. Electronic Industries Association, Safety Engineering Bulletin No. 3, May 1971, "Safety Analytical Techniques"

3. Electronic Industries Association, Reliability Bulletin No. 9, November 1971, "Failure Mode and Effect Analyses"

4. MIL-STD-721, 10 March 1970, "Definitions of Effectiveness Terms for Reliability, Maintainability, Human Factors and Safety"

5. MIL-STD-1629 (PRELIMINARY), "Procedures For Performing a Failure Mode and Effect Analysis"

6. NASA Ames Research Center Publication AHB5326-1, March 1973, "Failure Mode, Effects, and Criticality Analysis"

7. MIL-HDBK-217B, "Reliability Stress and Failure Rate Data for Electronic Equipment," September 20, 1974

8. RADC-TR-67-108, Vol. II, RADC Reliability Notebook, Vol. II, September 1967

9. Hayes, John P., "A NAND Model for Fault Diagnosis in Combinational Logic Networks," IEEE Transactions on Computers, Vol. C-20, No. 12, December, 1971

10. Friedman & Menon, "Fault Detection in Digital Circuits," Prentice-Hall, 1971

APPENDIX B: EXAMPLES

CONTENTS

F/FA Example

EXAMPLE I

FAULT TREE CONSTRUCTION EXAMPLE

The approach consists of analyzing first primary and then secondary failures. Suppose that prior analyses have indicated that destruction of the wire between A and B (Fig. 21) from overheating is a critical event. Perhaps this particular wire is near ordnance wiring which it may short circuit, or maybe it passes through an area that is frequently saturated with combustible vapors. In any event, a fault tree must be constructed to define the failure modes by which the wire between A and B can be overheated.

Before attempting any analysis, it is necessary to learn how the system functions. (See Fig. 21). The sample system is designed to make available mechanical energy from the MOTOR whenever the SWITCH is closed by the action of an external control system. When the SWITCH is closed, power is applied to the RELAY COIL through the TIMER CONTACTS. With power on the RELAY COIL, the RELAY CONTACTS close and cause power to be applied through the FUSE to the MOTOR. When the SWITCH is later opened, power is removed from the RELAY COIL, thereby opening the RELAY CONTACTS and removing power from the MOTOR. The TIMER and FUSE are safety devices. If the SWITCH fails to open after some preset time interval, the TIMER CONTACTS should open and remove power from the RELAY COIL. If the MOTOR fails shorted while the RELAY CONTACTS are closed, the FUSE should open and deenergize the circuit.

The actual preparation of a fault tree begins with a definition of the final "undesired event" and proceeds with a series of "a posteriori" judgments until basic input events are defined. In the sample problem, overheating of the wire between A and B can result only from the application of current beyond the rated capacity of the wire for an extended period of time. The coexistance of both excessive current and an "overrun" condition are essential to produce the undesired event. Using the AND gate, this is represented in Fig. 22.

The development of the tree is shown considering only primary failures in Figs. 23 and 24. The logic of the tree is complete when secondary failures are considered and added to Fig. 25.

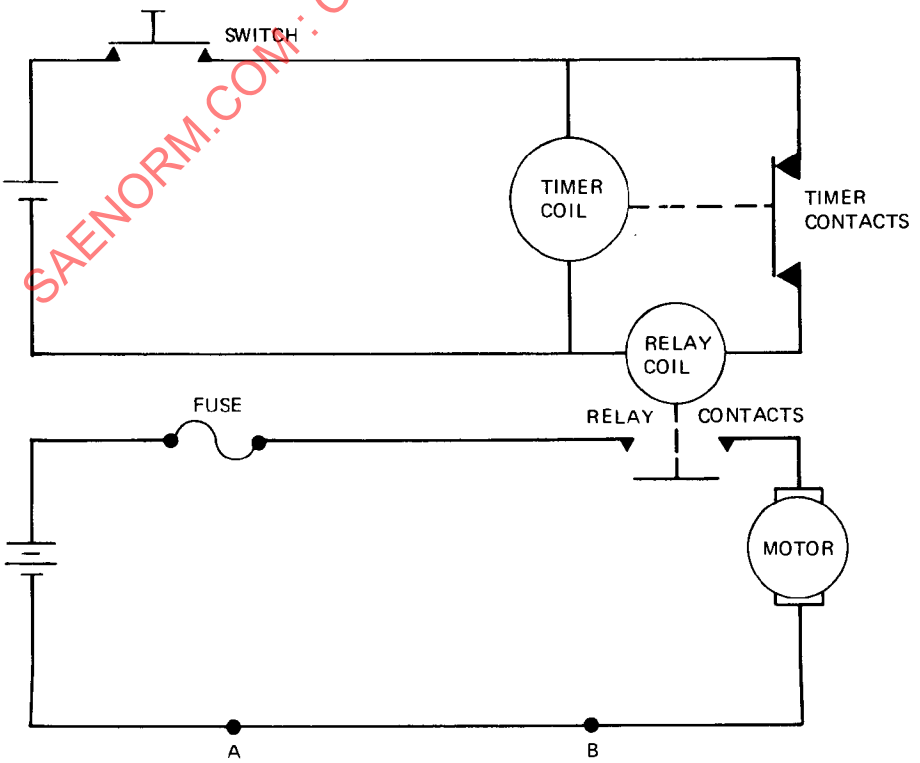


FIGURE 21
SAMPLE SYSTEM

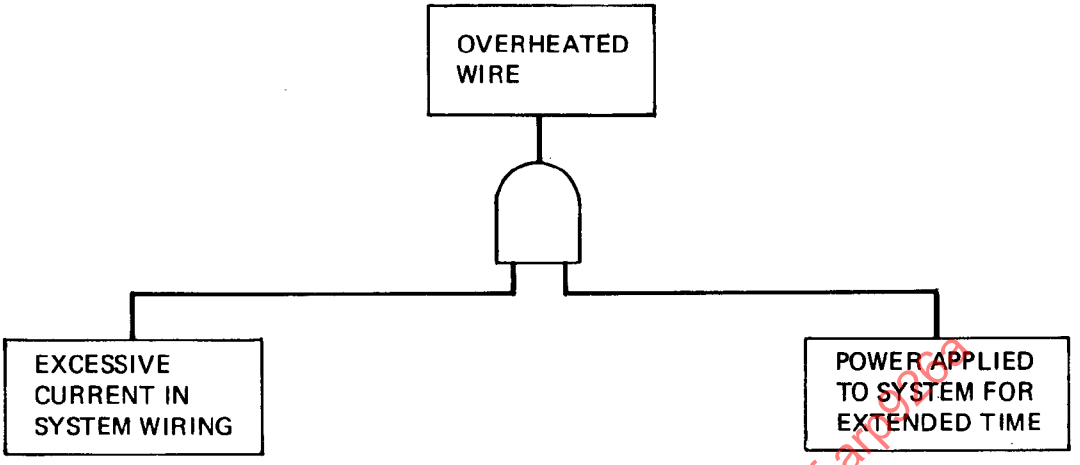


FIGURE 22

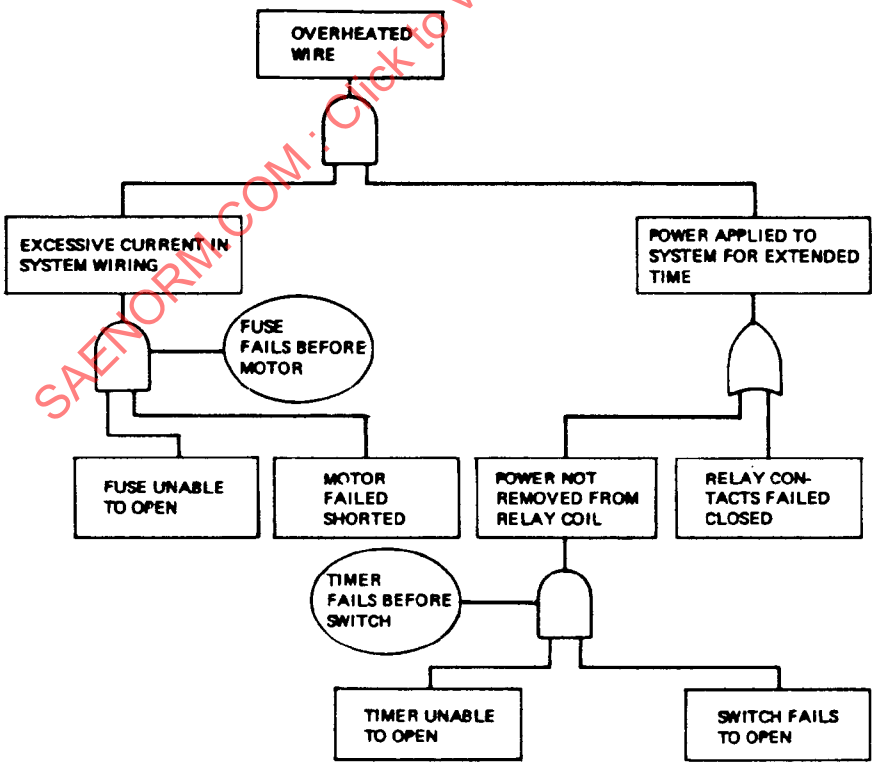
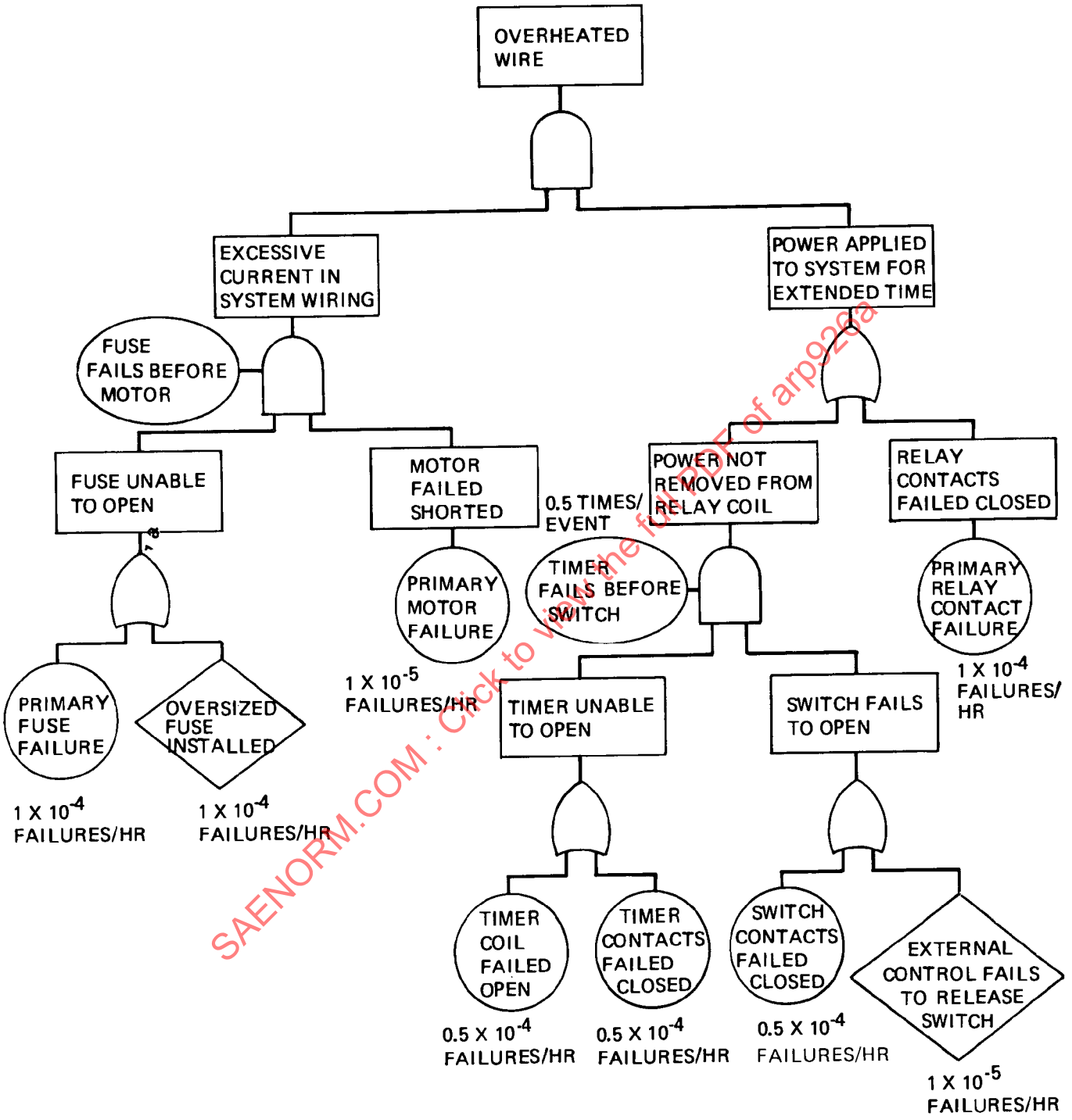


FIGURE 23



NOTE: Failure rates shown must be converted to probabilities by applying appropriate exposure times before calculating higher level event probabilities.

FIGURE 24
FAULT TREE WITH PRIMARY FAILURES