

IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems

IEEE STANDARDS
ARCHIVES
DO NOT REMOVE

ANSI/IEEE Std 352-1975



Published by The Institute of Electrical and Electronics Engineers, Inc. 345 East 47th Street, New York, New York 10017
April 14, 1974

Documents
Document Sharing Hub
SH13524

Authorized licensed use limited to: Tsinghua University. Downloaded on March 07, 2026 at 02:44:08 UTC from IEEE Xplore. Restrictions apply.

ANSI IEEE
N41.4-1976 Std 352-1975
(Revision of IEEE
Std 352-1972)

An American National Standard

**IEEE Guide for
General Principles of Reliability Analysis of
Nuclear Power Generating Station Protection Systems**

Sponsor
**Nuclear Power Engineering Committee of the
IEEE Power Engineering Society**

Approved January 5, 1976
American National Standards Institute

© Copyright 1975 by
The Institute of Electrical and Electronics Engineers, Inc.

*No part of this publication may be reproduced in any form,
in an electronic retrieval system or otherwise,
without the prior written permission of the publisher.*

Approved September 5, 1974

IEEE Standards Board

Joseph L. Koepfinger, *Chairman*

Sava I. Sherr, *Secretary*

Warren H. Cook, *Vice-Chairman*

**Jean Jacques Archambault
Saul Aronow
Robert D. Briskman
Dale R. Cochran
Louis Costrell
Charles W. Flint
Jay Forster**

**Irvin N. Howell, Jr
Irving Kolodny
William R. Kruesi
Benjamin J. Leon
Anthony C. Lordi
Donald T. Michael
Voss A. Moore
William S. Morgan**

**Harvey C. Nathanson
James D. M. Phelps
Saul W. Rosenthal
Gustave Shapiro
Ralph M. Showers
Robert A. Soderman
William T. Wintringham**

Foreword

(This foreword is not a part of IEEE Std 352-1975, Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems.)

This document is basically tutorial and has been prepared to provide the user with the basic principles that are needed to conduct a reliability analysis of protection systems. It is not expected or intended that any individual or organization would need all of the principles that are presented. For example, an organization may be concerned only with qualitative analysis as discussed in Section 4. Another organization may be concerned with quantitative analysis and mathematical modeling as discussed in Section 5. The very important problem of failure data is discussed in Section 6; the material on probability distributions, estimation, and confidence intervals may be used by those who are concerned with analysis and evaluation of failure and repair rate data that will be accumulated as nuclear power generating station operating experience is accrued. The material on established data programs may be of more immediate use to those who make reliability or availability predictions on current protection system designs.

This document was prepared to provide a common and consistent means of reliability analysis for protection systems covered by IEEE Std 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations. Reference is especially made to Sections 4.2, 4.3.7, and 5.2 of IEEE Std 338-1971, Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems.

The general principles presented in this document, and further information given by the references, are sufficient to conduct the reliability/availability analyses of protection systems, but every analysis will not necessarily employ all of the general principles that are presented. Furthermore, the principles contained herein are not necessarily limited to protection systems. They may be applied, as applicable, to the analyses of other systems. The user may select those parts of the document that apply to his particular problem.

The IEEE will update this document as the state of the technology changes. Comments and suggestions for additional material may be added; these should be addressed to:

Secretary
IEEE Standards Board
The Institute of Electrical and Electronics Engineers, Inc
345 East 47 Street
New York, NY 10017

This document was prepared by Subcommittee 5, Reliability, of the Nuclear Power Engineering Committee of the IEEE Power Engineering Society. At the time of approval for ballot, the members of the subcommittee were:

D.G. Fitzgerald, *Chairman*

S. J. Ditto
M. L. Faught
I. M. Jacobs
R. Lohrding

H. Otway
E. S. Patterson
J. R. Penland

R. Salvatori
B. M. Tashjian
E. C. Wenzinger
J. J. Wroblewski

Contents

SECTION	PAGE
1. Introduction	7
2. Definitions	7
3. Objectives	8
3.1 Qualitative Analysis	8
3.2 Quantitative Analysis	9
3.3 Test Interval	10
4. Qualitative Analysis Principles	10
4.1 Failure Mode and Effects Analysis (FMEA)	10
4.2 Fault Tree Analysis	14
4.3 Reliability Block Diagram	15
4.4 Example	16
4.5 Extended Qualitative Analysis	17
5. Quantitative Analysis Principles	21
5.1 Mission Definition	21
5.2 Mathematical Modeling	23
5.3 Tabular Reference to Popular Logic Configurations	29
5.4 Input Parameters	30
5.5 Trial Calculations	31
5.6 Credibility Check of Results	31
6. Guides for Failure Data Acquisition and Use	32
6.1 Probability Distributions, Estimations, Confidence Intervals, and Examples of Use	32
6.2 Established Data Programs	37
6.3 Developing Field Data Programs	39
7. Guide for Establishment of Intervals	43
7.1 Numerical Goals	43
7.2 Initial Test Intervals	44
7.3 In-Service Adjustment of Test Intervals	45
8. References	45
Appendix A	47
A1. Introduction	47
A2. Procedure	47
A2.1 System Definition	47
A2.2 Failure Mode and Effects Analysis (FMEA) (Qualitative Analysis)	47
A2.3 Common-Mode-Failure Analysis	48
A2.4 Reliability/Availability Prediction (Quantitative)	48
A3. Illustrative Examples	48
A3.1 System Definition	48
A3.2 Qualitative Analysis — FMEA	48
A3.3 Common-Mode-Failure Analysis	63
A3.4 Quantitative Analysis	65
FIGURES	
Fig. 1 Schematic of a Typical Reactor Trip Function	12
Fig. 2 Fault Tree for a Typical Trip Function	13

Fig. 3	Reliability Block Diagram of a Typical Trip Function	18
Fig. 4	Alternative Reliability Block Diagram of a Typical Trip Function	19
Fig. 5	Basic Two-Out-of-Three (2/3) System	23
Fig. 6	Venn Diagram for Basic (2/3) System	25
Fig. 7	Reliability Block Diagram of a Simple 2/3 System	26
Fig. 8	Improved Model of a 2/3 System	27
Fig. 9	Sensitivity Study of Model of Fig. 8	33
Fig. 10	Distribution Graphical Evaluation	42
Fig. A1	One Function Diagram for a Typical Reactor Trip Function	49
Fig. A2	Fault Tree for No Typical Trip Function	69
Fig. A3	Fault Tree for Limit Consequences	70

TABLES

Table 1	Typical Failure Mode and Effects Analysis Documentation	9
Table 2	Unavailability as a Function of Logic Configuration and Testing Schedule	29
Table 3	Some Typical Failure Modes and Mechanisms	40
Table 4	Test Interval as a Function of Logic Configuration and Unavailability Design Goal G	45
Table A1	Generic Part Failure Rate and Failure Mode Classification	50
Table A2	Principal Design Components and Their Primary Function	51
Table A3	Failure Mode and Effects Analysis	52
Table A4	Summary of Failure Modes and Effects	62
Table A5	Summary of Results	63
Table A6	Nonannunciating Failures Detectable by Test	63
Table A7	Minimum Number of Like Functional Blocks Required to Suffer Common-Mode Failure to Prevent Automatic Reactor Trip	64
Table A8	Common-Mode Failure Preventative Measures	64
Table A9	Common-Mode-Failure Matrix Relating Causative Factors to Equipment Required Failure Modes in Reactor Protection System	66
Table A10	Logic and Boolean Expressions for Events in a Fault Tree	68

An American National Standard

IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems

1. Introduction

This document was prepared to provide the designers and operators of nuclear power plant protection systems and the concerned regulatory groups with the essential methods and procedures of reliability engineering that are applicable to protection systems. By applying principles given, systems may be analyzed, acceptable test intervals may be established, results may be reconciled with reliability objectives, and the analyses may be suitably documented.

The quantitative principles are applicable to the analysis of the effects of random failures on protection system reliability. They are not intended for use in treating the problem of systematic or common-mode failure.

The principles are applicable during any phase of a protection system's lifetime. They have their greatest value during the design phase. During this phase reliability engineering can have the greatest effect for enhancing safety.

The principles may also be applied during the preoperational phase or at any time during the normal lifetime of a system. When the principles are applied during either of these two phases, they will aid in the evaluation of systems and in improving test programs. Although not inherently limited, these principles are intended for application to systems covered in the scope of IEEE Std 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations, ANSI N42.7-1972.

2. Definitions

availability. The characteristic of an item expressed by the probability that it will be operational at a randomly selected future instant in time.

break-in period. That early period, beginning at some stated time, during which the failure rate of some items is decreasing rapidly. Also called early-failure period.

common-mode failure. Multiple failures attributable to a common cause.

failure. The termination of the ability of an item to perform its required function. Failures may be unannounced and not detected until the next test (unannounced failure), or they may be announced and detected by any number of methods at the instant of occurrence (announced failure).

failure rate. The expected number of failures of a given type, per item, in a given time interval (for example, capacitor short circuit failures per million capacitor hours).

mean time between failures (MTBF). The arithmetic average of operating times between failures of an item.

mean time to repair (MTTR). The arithmetic average of time required to complete a repair activity.

mission. The singular objective, task, or purpose of an item or system.

mission time. The time during which the mission must be performed without interruption.

mutually exclusive events. Events that cannot exist simultaneously.

probability distribution. The mathematical function that relates the probability of an event to an elapsed time or to a number of trials.

reliability. The characteristic of an item expressed by the probability that it will perform a required mission under stated conditions for a stated mission time.

repair rate. The expected number of repair actions of a given type completed per unit of time.

risk. The expected detriment per unit time to a person or a population from a given cause.

sensitivity analysis. An analysis that determines the variation of a given function caused by changes in one or more parameters about a selected reference value.

test frequency. The number of tests of the same type per unit time interval; the inverse of the test interval.

test interval. The elapsed time between the initiation of identical tests on the same sensor, channel, etc.

test schedule. The pattern of testing applied to the parts of a system. In general, there are two patterns of interest:

- (1) *Simultaneous.* Redundant items are tested at the beginning of each test interval, one immediately following the other
- (2) *Perfectly Staggered.* Redundant items are tested such that the test interval is divided into equal subintervals

unavailability. The numerical complement of availability. Unavailability may occur as a result of the item being repaired (repair unavailability) or it may occur as a result of undetected malfunctions (unannounced unavailability).

wearout period. The time interval, following the period of constant failure rate, during which failures occur at an increasing rate.

3. Objectives

This document presents the general principles that may be used to evaluate the qualitative and quantitative reliability and availability of safety related nuclear power plant systems.

Qualitative analysis provides the designer an identification of the various failure modes of the parts of a system that contribute to the system unreliability. Quantitative analysis utilizes operating experience of the system's components and provides the designer with a numerical value for the probability that the system will perform its intended function for the environments and time period of interest. The output of the analysis is to be used as inputs to determine and to update the test interval of the system.

3.1 Qualitative Analysis. Qualitative reliability analyses are used to locate possible failures and to identify proper precautions (design changes, administrative procedures, etc) that will reduce the frequency or consequences of such failures.

A qualitative reliability analysis can be performed with one or more of the following objectives:

- (1) To identify weak spots or unbalances in the design
- (2) To aid in the systematic assessment of overall plant safety
- (3) To document and assess the relative importance of all identified failures
- (4) To develop discipline and objectivity on the part of a designer of safety-related systems
- (5) To provide a systematic compilation of data as a preliminary step to facilitate quantitative analyses

It should be stressed that this type of analysis should become an integral part of the normal system design process. The designer is the most qualified to identify the particular failure modes and chains of importance, but it should be realized that a designer might overlook in his systematic analyses those failure modes that he considered unimportant during the original design process. Therefore, his systematic analysis should be reviewed and checked by qualified people who are not directly involved in the particular design being studied.

A reliability analyst should provide methods, data, and analysis services to the design groups, and participate in the analysis.

The general steps in a qualitative system reliability analysis are as follows:

- (1) Identify significant failures, and their consequences (generally called Failure Mode and Effects Analysis — FMEA)
- (2) Display the above information in a table, chart, fault tree, or other format
- (3) Evaluate overall system reliability relative to the information above and resolve identified problems

Each of these steps requires different types of documentation, methods, and personnel. In the first step, special forms similar to those shown in Table 1 are useful for documenting an FMEA. Failure modes are identified by design and operating personnel, in fact, by everyone involved in a project; but it is usually

Table 1
Typical Failure Mode and Effects Analysis Documentation

FAILURE MODE AND EFFECTS ANALYSIS — TYPICAL TRIP FUNCTION						
Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
1. Circuit Breaker 52/RTA, RTB, BYA, BYB	Trip	Fail Closed	Jam Mechanism UV Trip Attachment Mechanism Stuck Fuse Main Contacts	Makes Trip 1/1 "	Monthly Test "	Immediate Detection
		Fail Open	Loss of DC Control Power UV Coil Failure Worn Trip Latch	Spurious Trip " "	Spurious Trip " "	
2. DC Control Relay	Break Ckt. To Trip Breaker UV Coil on Trip (DE-EN To Trip)	Fail Closed	Contacts Shorted or Fused Armature Jammed Wiring Fault	Makes Trip 1/1 " "	Monthly Test " "	Immediate Detection
		Fail Open	Loss of DC Control Power Coil Failure Broken Contacts Broken Wire or Loose Connec.	Spurious Trip Spurious Trip if 2/2 Fail " "	Spurious Trip " " "	
3. AC Control Relay X1A, B, X2A, B, X3A, B	Break Ckt. To DC Relays on Trip (DE-EN To Trip)	Fail Closed	Contacts Shorted or Fused Armature Jammed Wiring Fault	Makes 1 Train 2/2 vice 2/3 " "	Monthly Test " "	
		Fail Open	Loss of AC Power (Instr. Bus) Coil Failure Broken Contacts Broken Wire or Loose Connec.	Spurious Trip if 2/3 " " "	Spurious Trip " " "	
4. Alarm Unit PC-1, 2, 3	Remove AC Power To Relays For PM>P set	Fail Off	Transformer Failure Open Circuit in Output Sect. Setpoint Drift	Makes Both Trains 1/2 " "	Spurious Trip if 2/3 Fail " "	Partial Trip Alarm
		Fail On	Short in Output Section Setpoint Drift	Makes Both Trains 2/2 "	Monthly Test "	
5. DC Power Supply PQ-1, 2, 3	Provide Power For Analog Cur- rent Loop	Fail Low or Off	Transformer Failure Diode Failure	Makes Both Trains 1/2 "	Spurious Trip if 2 Fail "	Partial Trip Alarm
		Fail High	Heat Effects Misadjustment	Makes Both Trains 2/2 "	Monthly Test "	
6. Pressure Transmitter PT-1, 2, 3	Convert Pressure To Analog Current	Fail Low	Corrosion Wear Mechanical Damage Heat Effects	Makes Both Trains 2/2 " " "	Monthly Test and Comparison with Redundant Channel Indicators	Possible Immediate Detection
		Fail High	Misadjustment	Makes Both Trains 1/2	Spurious Trip if 2 Fail	Partial Trip Alarm

the job of the design engineer to document these modes. In the second general step, failure data forms of various types such as fault trees, system functional diagrams, and block diagrams are used; and in the third step the analyst is usually required to obtain and to interpret the data and to evaluate reliability.

3.2 Quantitative Analysis. The quantitative analysis represents the system in a mathemat-

ical model, apportions the reliability and availability goals, and reconciles the calculated reliability and availability with the overall system goals. The analysis provides an appropriate model to represent the system that will facilitate the applications of reliability engineering techniques during the design, production, and operating stages of a plant's life.

This analysis helps the designer to minimize system complexity, to be cognizant of the characteristic of the components selected, and to provide a reliable design. The designer considers the failure rates and failure modes of the components that he selects and determines whether they are self-annunciating or nonself-annunciating under failed conditions to determine appropriate system or operator actions, or both.

The mathematical model generated can be used in a sensitivity analysis. Thus, one can identify the critical items in the design and establish the credibility of the analysis. The relative significance of each component's failure rate in the reliability and availability prediction for the protection system can also be determined.

3.3 Test Interval. Testing verifies the operability of the system and its components on a regular basis. The test intervals selected must be adequate for the safety needs of the plant.

3.3.1 Initial Selection. The initial test interval is established by using the quantitative reliability model, and the importance, complexity, and the purpose of items being tested are considered. This interval is based principally on the results of the trial analysis of the availability model reflecting the expected up-time and down-time of the equipment relative to the design goals. The failure rates and field data applicable to the model are used in the calculation. The test selection process ensures that projected trends, life cycles, and drift characteristic of the components have been adequately accounted for when exposed to the expected operating conditions.

3.3.2 In-Service Assessment. This effort ensures that the initial test intervals are suitable or indicates the need for change because of differences between the assumed and observed values of the analysis input parameters. The changes shall not conflict with the protective system design goals and shall be consistent with the safety needs of the plant. The in-service assessments should be based on the evaluation of the test data to determine if changes in the frequency, mode, complexity, mechanism, or perturbations, etc, are necessary and warranted. It may become necessary or desirable to change the test interval because of feedback data from operating experience or because of changes in numerical goals.

4. Qualitative Analysis Principles

As mentioned in Section 3.1, the first general step of a reliability analysis is the identification of failure modes. This step, the FMEA, is discussed in the following paragraphs, along with fault tree and reliability block diagram analyses that represent pictorially the relationships of important events.

4.1 Failure Mode and Effects Analysis (FMEA). The FMEA is a systematic procedure for identifying the modes of failure and for evaluating their consequences.

4.1.1 Purposes of Failure Mode and Effects Analysis [1].¹ The purposes of an FMEA are to:

- (1) Assist in selecting design alternatives with high reliability and high safety potential during early design phase
- (2) Ensure that all conceivable failure modes and their effects on operational success of the system have been considered
- (3) List potential failures and identify the magnitude of their effects
- (4) Develop early criteria for test planning and the design of the test and checkout systems
- (5) Provide a basis for quantitative reliability and availability analyses
- (6) Provide historical documentation for future reference to aid in analysis of field failures and consideration of design changes
- (7) Provide input data for tradeoff studies
- (8) Provide basis for establishing corrective action priorities
- (9) Assist in the objective evaluation of design requirements related to redundancy, failure detection systems, fail-safe characteristics, and automatic and manual override

When considering reliability analysis of a design, one usually thinks of all the analytical steps leading to an estimate of the reliability of a given item. A complete analysis requires comprehensive input data that include material properties, design details, and component failure rates; however, it is not necessary to wait until all of these are known before much can be determined about the reliability of the design.

By confining the scope of an analysis to how the article can fail and the consequences if it

¹References are listed in Section 8.

should fail, it is usually not necessary to be concerned about stresses and strengths. This limited-scope analysis is the FMEA, which does not do the whole job, but it does provide some early answers when they are most needed, and it provides a basis for later studies and analyses.

4.1.2 Timing of a Failure Mode and Effects Analysis. The FMEA should be an integral part of the early design evaluation and should be periodically updated to reflect changes in design or application. An updated FMEA should be a major consideration in design reviews, inspections, or other major system review points in the program. FMEAs have been used as part of concept selection procedure. The major program points at which an FMEA should be performed are as follows:

- (1) Concept formulation or selection
- (2) Preliminary design or layout
- (3) Completion of detail part design
- (4) Design improvement programs

The FMEA may be performed with limited design information because it is not primarily concerned with rate of occurrence or frequency of failure. The basic questions to be answered by an FMEA are as follows:

- (1) How can each part conceivably fail?
- (2) What mechanisms might produce these modes of failure?
- (3) What could the effects be if the failures did occur?
- (4) Is the failure in the safe or unsafe direction?
- (5) How is the failure detected?
- (6) What inherent provisions are provided in the design to compensate for the failure?

4.1.3 Preparatory Steps for Failure Mode and Effects Analysis. The depth to which one performs the preparatory steps is a function of the complexity of the equipment being studied and the experience that one has with similar equipment. Each of the following preparatory steps is essential but may vary greatly in scope:

- (1) Definition of the system to be analyzed and its mission
- (2) Description of the operation of the system
- (3) Identification of failure categories
- (4) Description of the environmental conditions

The system should be described to the extent that what constitutes the system and its mission is described. Interfaces should be clearly defined. One may use a similarly detailed product specification, parts list, or sales agreement. The important point is that the analyst must know just what he is to analyze; he will then be able to define the interface functions. The more complex the system, the greater the need to carefully define the system. A functional diagram may be used in the FMEA to show the functional interdependencies in the system so that the effects of failure can be traced. Fault trees may also be used. These techniques are discussed later.

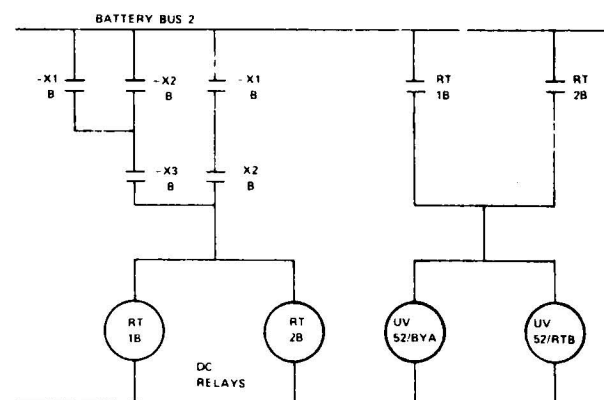
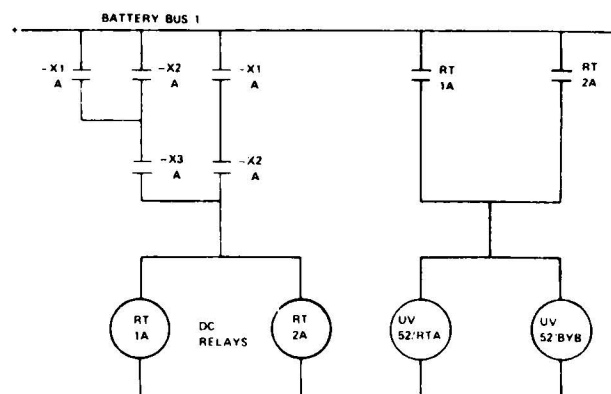
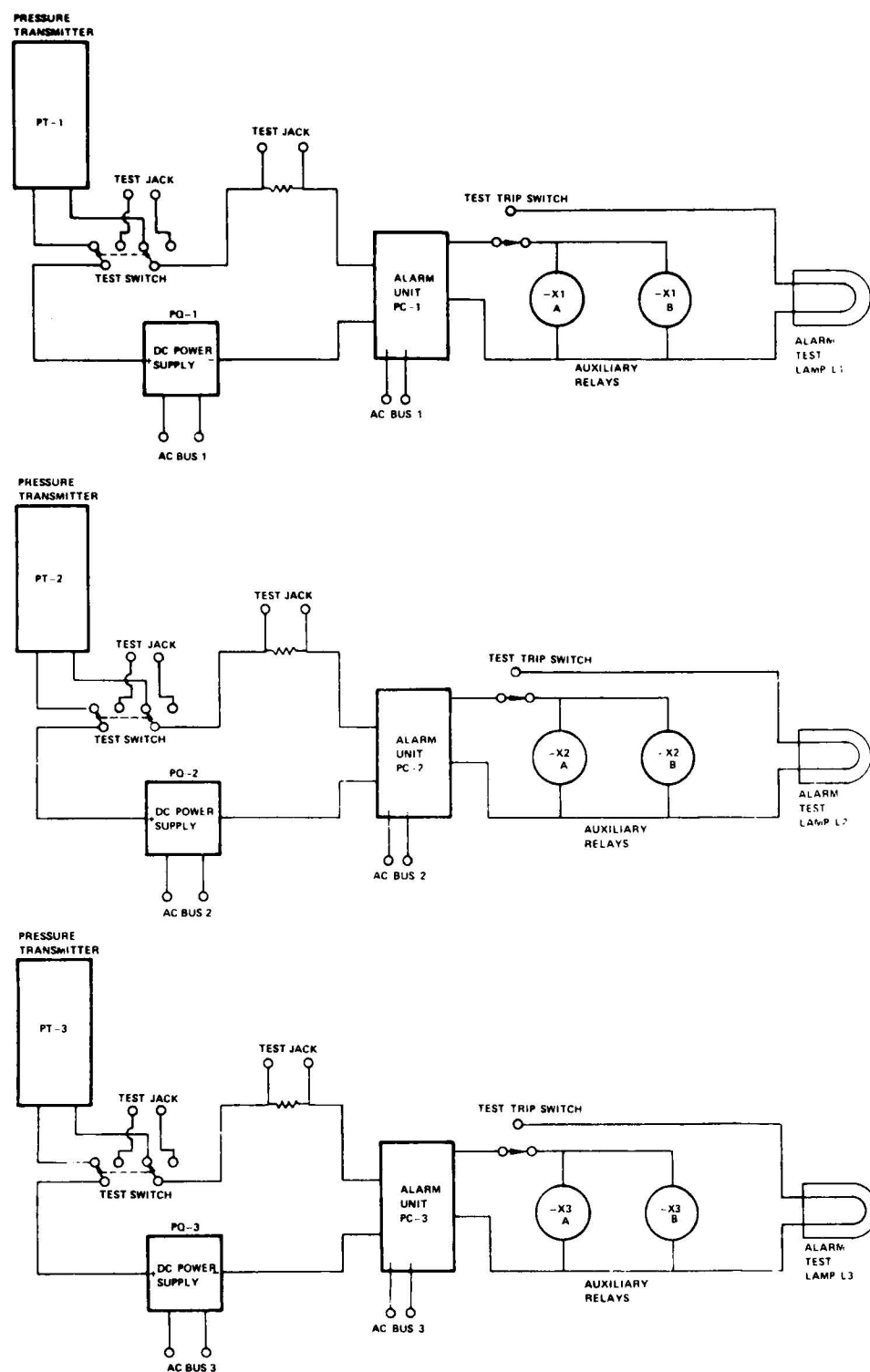
Once the system and its intended use are defined and understood, the actual FMEA can be performed. As stated previously, the amount of work required to arrive at this point is a function of the complexity of the system and the experience and knowledge of the people performing the analysis.

4.1.4 Procedure in a Failure Mode and Effects Analysis. A partial FMEA has been performed on a typical reactor trip system. Table 1 documents the FMEA for the typical reactor trip function shown in Fig 1 and described in Section 4.4. The form shown in Table 1 is typical of that which can be used to document an FMEA; however, other forms may be used. A form similar to that shown in Table 1 is not only very helpful but also the very heart of the procedure for documenting the FMEA.

The system component or part being analyzed is shown in Table 1, column 1. The breakdown of a system for analysis should normally be to the lowest level of system description at the time of the FMEA. In special cases, such as electronic or control systems using integral modular units as system building blocks, the modules rather than their parts may be listed. The term "part" will be used to indicate this lower level of detail. Functional parts codes that have been assigned to assist in defining the system can also be shown.

The drawing or scheme number by which the part is identified is recorded. If a reliability logic block diagram is used, reference to it and the particular functions associated with the part being analyzed should be noted.

All of the functions performed by the part are shown in a concise manner in column 2. (See Table 1.)



NOTES

1. BYA AND BYB BYPASS BREAKERS ARE CONNECTED ONLY FOR TESTING
2. TEST SWITCHES SHOWN IN OPERATE POSITION
3. RT1A, RT2A, ETC., ARE REACTOR TRIP AUXILIARY RELAYS
4. 52/RTA AND 52/RTB REFER TO REACTOR BREAKERS

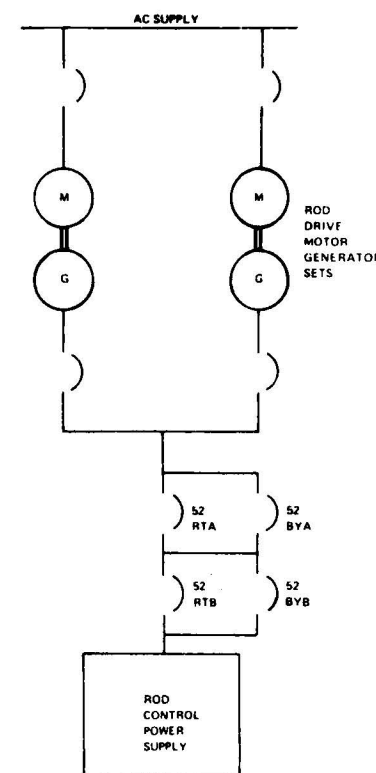


Fig. 1
Schematic of a Typical Reactor Trip Function

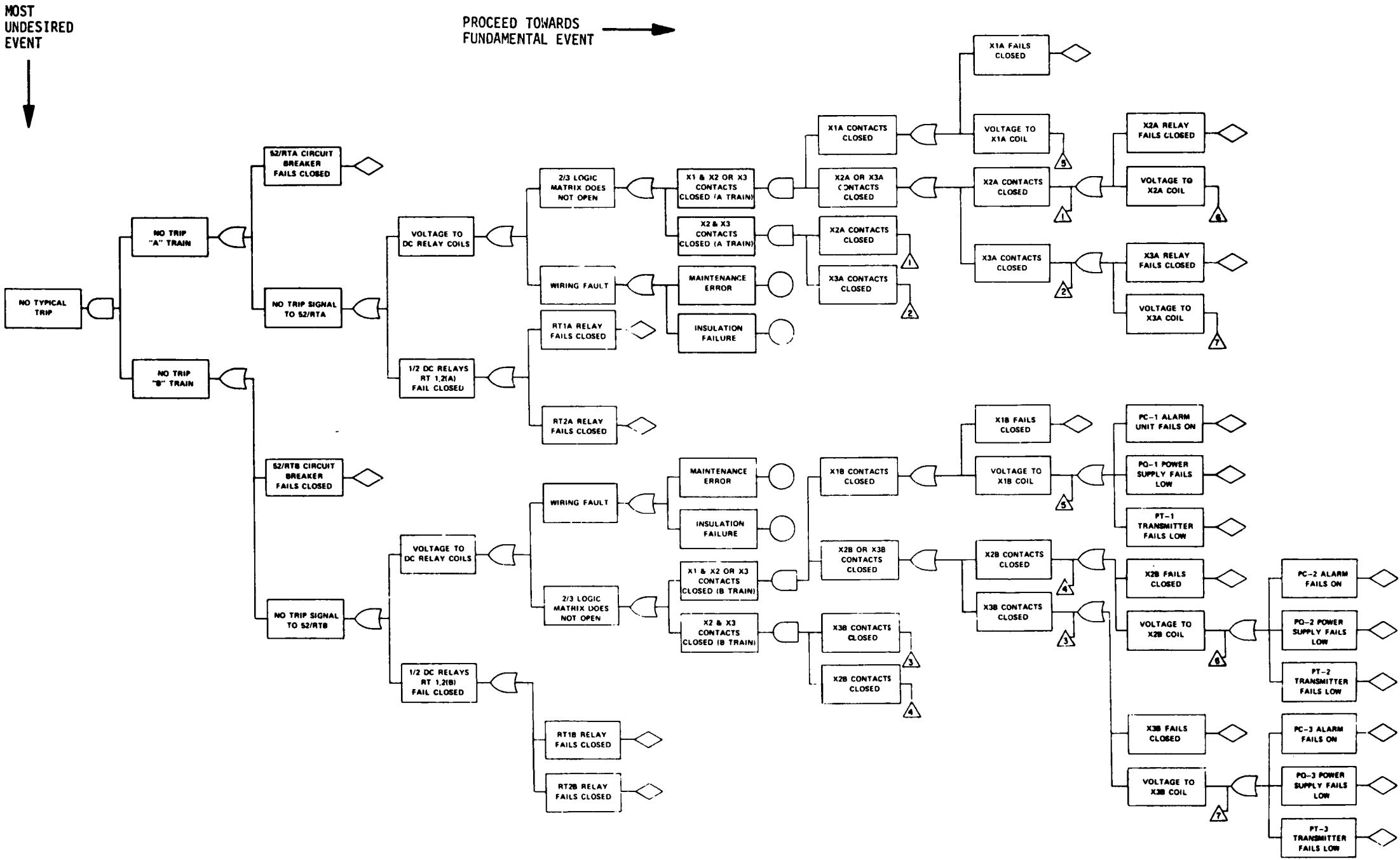


Fig. 2
Fault Tree for a Typical Trip Function

Each failure mode which the analyst can conceive for each feature or location of the part is noted in column 3. Again, the question is "Could it?" not "Will it?" When the item designated in column 1 is a piece-part, the failure modes will be: open, shorted, leaking, broken, spalled, cracked, or other applicable modes and a statement as to the location on the part where the failure mode could occur.

All mechanisms of failure that could result in the mode described in column 3 are noted in column 4.

In column 5 the effects of the failure on the overall system are described. It is at this point that a reliability logic block diagram can be helpful. Apparent redundancies may not protect against a single failure for a particular system mode of operation.

In column 6 the ways that failure can be detected are shown. In the absence of some means of detection, it is possible that loss of redundancy will not be noticed until the whole system fails.

Column 7 contains information that the analyst may feel is pertinent to his analysis.

4.2 Fault Tree Analysis. Fault tree analysis is a technique by which failures that can contribute to an undesired event are organized deductively and represented pictorially. It is one way to diagram and relate the information developed in a failure mode and effects analysis (FMEA). The resulting arrangement is a treelike structure with information flow from the branch tips, with the single most undesired event at the convergence of the branches. A fault tree diagram is illustrated by Fig. 2.

4.2.1 Functions and Benefits of Fault Tree Analysis. The primary features of the technique are as follows:

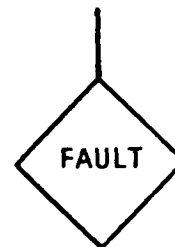
- (1) It forces the analyst to actively seek out failure events in a deductive manner
- (2) It provides a visual display of how the system can malfunction, allowing an easy understanding of the system by persons other than the designer
- (3) It points out the critical aspects of system behavior
- (4) It provides a reference for the evaluation of modifications
- (5) It provides a systematic basis for quantitative analysis

4.2.2 Representation of Events and Operations in a Fault Tree. Because the basic elements of a fault tree are the same regardless of the types of events or systems being analyzed, a standard jargon and a set of symbols have been developed to represent the events and operations. The symbols can be understood more fully by studying the sample fault tree in Fig 2. The symbols and their explanations are as follows:

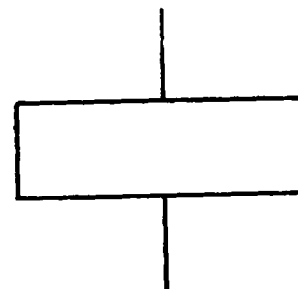
(1) *Circle.* The circle represents a basic fault event that requires no further dissection because the probability of such events is derived from empirical data or physics of failure analysis. This probability is an input to the fault tree when quantitative analysis is performed.



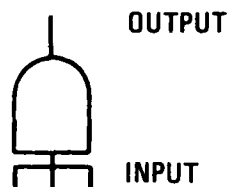
(2) *Diamond.* The diamond represents a fault event that is assumed basic in a given fault tree. This event could be divided further to show how it is caused from more basic failures, but is not developed either because of lack of significance in such fault, or because of lack of sufficient details to develop it further.



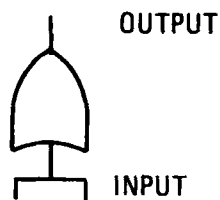
(3) *Rectangle.* The rectangle represents an event that results from the combination of events of the types described above through the input of a logic gate.



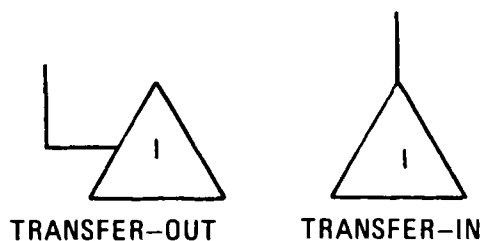
(4) **AND Gate.** The AND gate is the intersection operation of sets; that is, an output event occurs if and only if all the inputs occur.



(5) **OR Gate.** The OR gate is the union operation of sets; that is, an output event occurs if one or more of the inputs occur.



(6) **Transfer Gates.** The transfer symbol provides a tool to avoid repeating sections of the fault tree. The "transfer-out" gate represents the full branch that follows it, represented by a symbol, say I , and indicates that the branch is repeated somewhere else. The "transfer-in" gate represents the branch (in this case, I) that is already drawn somewhere else, and instead of drawing it again it is simply input at the point.



4.2.3 Procedure for Constructing a Fault Tree. The general steps in constructing a fault tree are as follows.

(1) Define the most undesired event. This event, called the top event, is the starting point of the fault tree. It is important that this event be precisely worded so that its interpretation will not vary.

For a particular fault tree there is one and only one most undesired event. This event

and others related to it may have been identified in an FMEA.

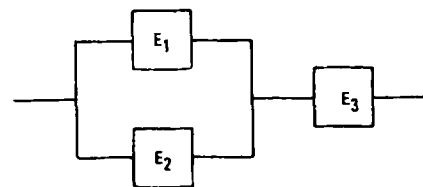
(2) Define, for the main branches of the tree, those events that lead directly to the top event and decide what logic gate should be used to relate them to the top event of the tree. These events are deduced from experience and knowledge of what can happen. They should be kept sufficiently general so that the details of the system can be developed by subsequent branches.

(3) Select one of the branches and deduce its next level of sub-branches. The manner of deducing the sub-branches is identical to that used in deducing main branches, and so on throughout the rest of the tree. The termination of a sub-branch of a tree occurs when the event being considered is a fundamental event (basic fault) or when a transfer gate can be used for another subtree already developed.

These general steps can be carried out after an FMEA, or concurrently with a formal or informal FMEA. Once the fault tree is prepared, it may be possible to assign numerical values to the probabilities of the events and conditions and, by using methods discussed later, to determine the probability of the event at the top of the tree.

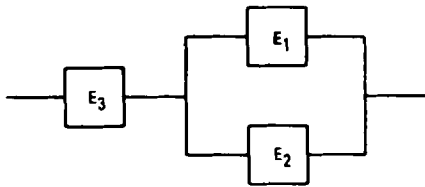
4.3 Reliability Block Diagram. The reliability block diagram (RBD) is a success-oriented diagram which represents pictorially the logic of a system. Reliability block diagrams are developed through analysis of the functional relationships among items shown by functional block diagrams and circuit schematics. The interrelation of events is expressed by the way that the blocks are interconnected in the block diagram.

For example, the blocks shown below represent a system with two success paths, $E_1 - E_3$, and $E_2 - E_3$.

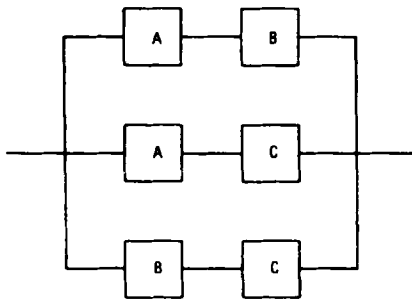


If either path is good, that is, made up of unfailed components, the system is good or successful.

The order of the blocks is unimportant. For example, the block shown below is equivalent to the RBD above.

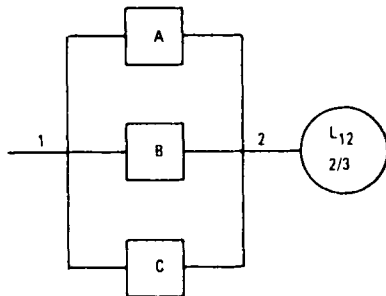


The system logic may be shown in different ways. For example, a two-out-of-three system of logic with success paths $A-B$, $A-C$, and $B-C$ may be shown as follows:



Note that each block appears twice in the diagram for clarity in depicting the logic, but it is understood that when a block is in a failed state, all blocks with the same designation are considered failed.

The same logic may be shown in a shorthand fashion as in the diagram below.



1 and 2 represent nodes, and the circle indicates that the logic between nodes 1 and 2 (L_{12}) are to be combined in all the success paths associated with a two-out-of-three ($2/3$) logic.

The general procedure for constructing a reliability block diagram is as follows:

(1) Define the mission so that the completion of the mission yields system success. If the system has more than one mission, then each mission must be considered individually.

(2) From functional diagrams, the FMEA, and other applicable data, construct the reliability block diagram. Define all of the elements and number all of the nodes. Each block in the diagram represents the applicable failure mode of the component identified, inhibiting the success path in which it is located.

(3) Investigate the reliability block diagram to ensure that all possible paths leading to success have been included.

The steps above yield a reliability block diagram that shows in detail what goes on. To get a general picture of what is happening, many of the paths may be reduced into fewer, more important paths. This reduction is achieved from the detailed reliability block diagram as follows:

(1) The success of each path is related to the success of its elements in some simple fashion. Determine the logical description for success of each path and treat the path as one composite element. Construct a new diagram where the paths are composite elements.

(2) Continue this process until a diagram is developed that needs no further simplification.

It is important to note the difference between the reliability block diagram and the fault tree diagram. The two diagrams should not be compared; they perform different functions and are used for different purposes. The fault tree represents dependent and independent events having only an indirect correspondence to a system functional diagram. The use of fault trees stimulates the identification of possible failures and events, and the fault tree can represent all kinds of dependencies and common mode failures and events. The reliability block diagram corresponds closely to a system functional diagram and allows a visual understanding of the normal functioning of a system. Therefore, the fault tree represents the system in terms of the events leading to failures, and the reliability block diagram describes the system in terms of the events leading to success.

4.4 Example. A typical reactor trip function has been selected to illustrate the application of the methods described in the previous sections.

4.4.1 Description of a Typical Reactor Trip Function. In the typical trip function, shown

schematically in Fig. 1, a process pressure is sensed by three pressure transmitters PT-1, PT-2, and PT-3. During normal operation, pressure is below the setpoint and each alarm unit supplies ac voltage to energize two ac control relays (for example, PC-1 energizes X1A and X1B). Contacts of these relays, arranged in two sets of two-out-of-three logic, connect dc voltage to two pairs of dc control relays (RT 1 and 2). Contacts of the pairs of dc control relays in parallel arrangement connect dc voltage to the undervoltage trip attachments of the trip breakers, holding the trip plungers down against their springs. The two trip breakers (52/RTA and 52/RTB) in series connect three-phase ac power from the rod drive MG sets to the rod control power supply cabinets using the single scram bus principle of design. Bypass breakers, provided to permit testing, are cross-connected to the dc control relay contacts.

In an abnormal situation, where the process pressure exceeds the setpoint, the three alarm units switch off power, deenergizing the ac control relays. When two out of three of the normally open contacts of these ac relays open, the dc control relays are deenergized. As the normally open contacts of the pairs of dc relays open, the undervoltage coils sense a loss of dc voltage, release the trip plunger, and trip open the trip breakers. When either of the trip breakers opens, power is interrupted to the rod control power supply, and the control rods fall by gravity into the core. The trip action is then complete and rods cannot be withdrawn until an operator resets the trip breakers and the process pressure is below the setpoint again.

4.4.2 Failure Mode and Effects Analysis. Table 1 contains a tabular summary of a failure mode and effects analysis for the typical reactor trip function described in Section 4.4.1.

4.4.3 Fault Tree Analysis. Fig. 2 is a fault tree for the typical trip function described in Section 4.4.1. This tree presents the possible combinations of failures or basic events which can generate the ultimate system failure to trip on demand.

4.4.4 Reliability Block Diagram. Figs. 3 and 4 illustrate two possible reliability block diagram representations of the trip function described in Section 4.4.1.

When using reliability block diagrams, as well as fault tree analyses, for reliability calculations, care must be exercised when the same component failure affects more than one branch and when coincidence logic is employed.

4.5 Extended Qualitative Analysis. In this section an extended qualitative analysis procedure is described. This procedure, or another procedure similar in content or purpose, may be used to qualitatively assure that a system is not vulnerable to common-mode or cascade failures. This procedure is not suggested as a standard nor as an ideal method of analysis. Rather, it is presented only as a possible design and analysis tool.

The extended qualitative analysis is a systematic procedure to identify potential common-mode and cascade failures in reactor systems. The approaches described here are extensions of the failure modes and effects analysis (FMEA) as explained below. These extensions are designed to suggest to the analyst common-mode failure mechanisms and cascade-failure sequences not normally considered in a random failure analysis.

The common-mode-failure analysis (CMFA) is designed to identify modes and mechanisms of failures of components normally considered to be redundant. For example, this extension should have identified a situation in which all protection system relays could fail closed due to an insufficiently baked coating. This type of analysis is most applicable to systems with well-defined boundaries and a high order of redundancy.

The cascade-failure analysis (CFA) is intended to identify failures which can lead to "chain-type" events affecting several different areas or systems in a plant. This extension of the FMEA should have identified the potential for an incident in which the failure of a battery charger resulted ultimately in damage to the plant turbine and in deformation of a reactor coolant pump shaft. The CFA is well suited to the analysis of interconnected and complex systems.

Different aspects of the procedure should be stressed in the analysis of different types of systems. Some systems are more readily analyzed by the CMFA and others by the CFA; however, many systems warrant consideration of both. This procedure need not be

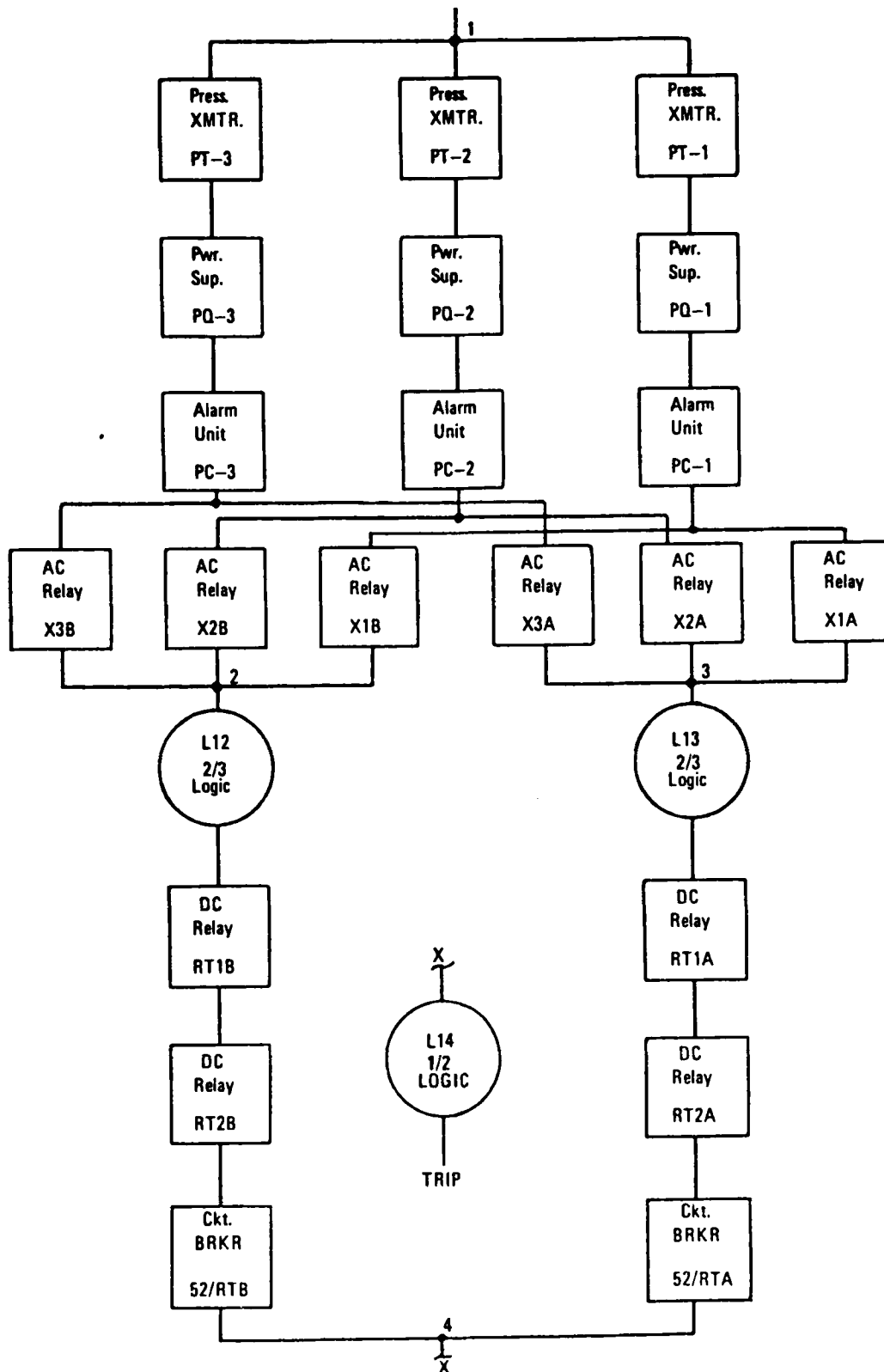


Fig. 3
Reliability Block Diagram of a Typical Trip Function

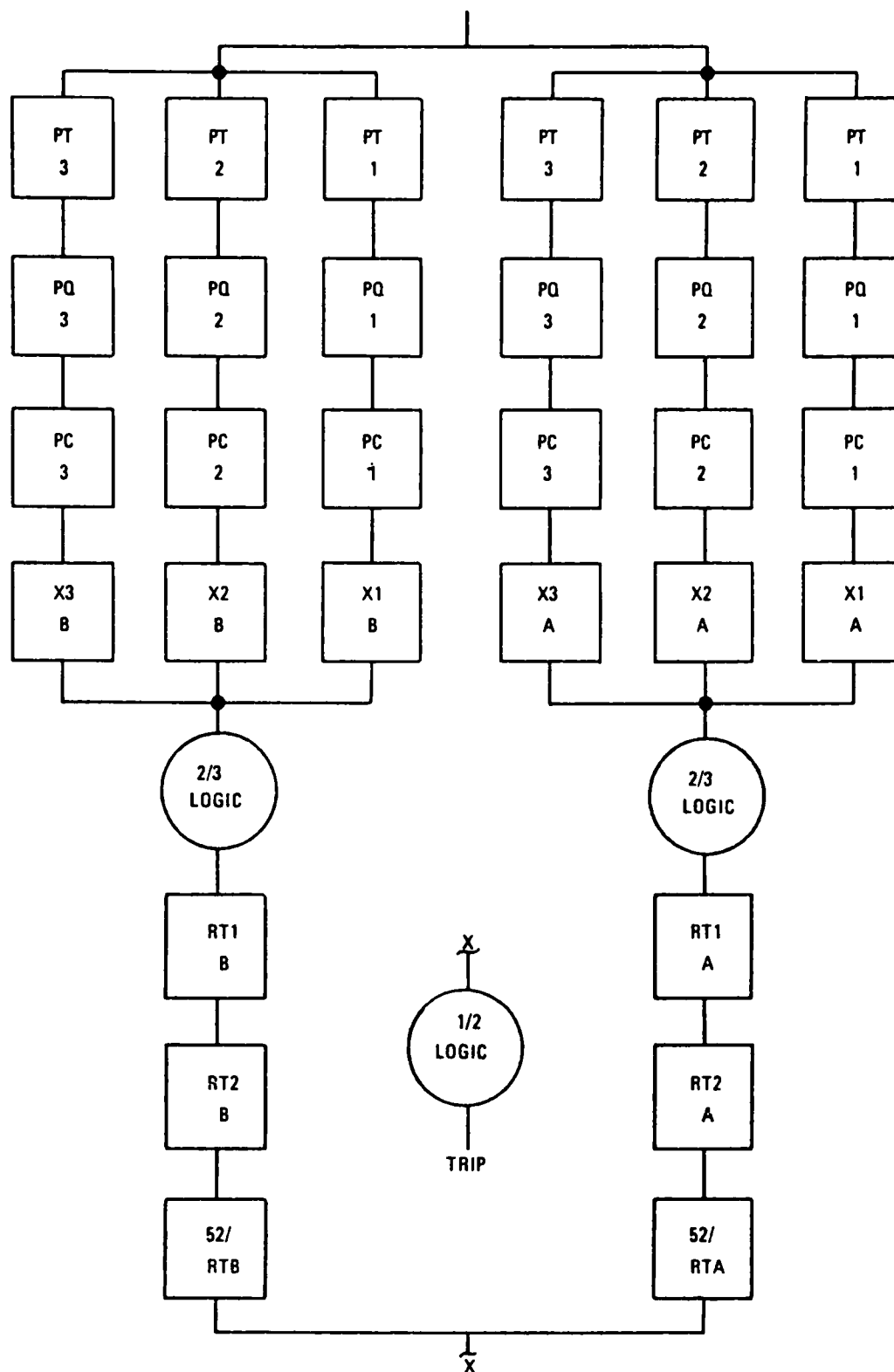


Fig. 4
Alternative Reliability Block Diagram of a Typical Trip Function

slavishly adhered to. Rather, this is a general guide, portions of which may be inapplicable to a given study and, more importantly, it is not complete but may suggest further steps in the analysis of a given system.

4.5.1 Procedure in Extended Qualitative Analysis. The depth and scope of this analysis may vary with the system being studied and with the purposes of the analysis. The following procedural steps should be considered.

(1) *Define System and System Boundaries.* Particular care must be taken in the definition of system boundaries. Channels of inter-system communication (pipes, wires, relays, etc) must be completely specified. A list of all such channels should be made.

(2) *Define All Anticipated System Operation Modes.* Typically the operation modes would include auto, manual, test, bypass, etc. It is important to consider all credible modes of operation because experience has shown that systems designed for one mode may perform or fail in unexpected manners under unusual, but anticipated, operating conditions.

(3) *Describe Operation of System and Environment Conditions Applicable to All Operating Modes.* The environmental description should include, as well as those normally anticipated, any conditions which can be credibly expected to occur within the life of the plant.

(4) *Prepare Critical Items Lists.* List A contains a list of all system components and/or modules (as defined in IEEE Std 279-1971 (ANSI N42.7-1972)). List B contains a list of units each of which is composed of all components/modules identical or similar in design or construction. List C contains a list of units composed of all components/modules that have identical function and are not completely diverse.

(5) *Prepare List of Failure Modes.* Determine and list all possible failure modes of each unit identified above. When appropriate the failure modes of a component/module should not be limited to upscale/downscale failures. For instance, if an amplifier can fail with a constant midrange output (as opposed to zero or full-scale output), this event must be considered.

4.5.2 CFA. For each operation mode and each unit failure mode, determine the following effects produced by the cascade failure.

(1) The effect on the system being studied (the primary system), for example, failure of valve closing, failure to trip on demand, spurious trip, etc.

(2) The effects on the communication channels, for example, high level signal, oscillatory signal, no flow, etc.

(3) For each abnormal signal [from step (2)] on a communication channel, determine the effect on the system communicated with (the secondary system). If the effect is seriously abnormal, examine effects on related systems.

(4) If a system communicated with in step (3) contains elements similar to those in the primary system whose failures cause the abnormal communication, evaluate the effect of the abnormal communication and the similar elements in the secondary system being failed.

(5) Assume abnormal signals (high, low, etc) on channels into the primary system and examine the effects. If the consequences are serious, examine how the abnormal signal can arise.

4.5.3 CMFA. For each failure mode examined above which causes primary system failure or fails secondary systems, determine and document all means by which the failures may occur. Examine, as a minimum, the following considerations:

(1) Random failure (list A only).

(2) Were members of a unit made by a single manufacturer? What are credible sources of failure in the manufacturing processes?

(3) What environmental factors (dust, humidity, radiation, liquid spillage, etc) could cause the failure?

(4) Can maintenance or installation errors cause simultaneous failures of members of a unit? Installation and maintenance procedures should be evaluated realistically to determine what *can* happen rather than what should occur.

(5) What possible operator interactions could produce unit failure?

(6) Examine operating transients and credible accidents. Estimate rate of occurrence of transient β and the fraction of time F system is in the mode being analyzed. If $\beta F \geq 10^{-6}$ per year, examine the effects on the system to identify "failed by accident" failures (that is, could hot steam be released on instruments or cables, etc?); if $\beta F < 10^{-6}$ per year, the probability of occurrence of such postulated occur-

rences is so small as to be incredible irrespective of the consequences. The numerical value of 10^{-6} per year is used as a threshold for continuation of this phase of the analysis. The actual value used may vary with application.

4.5.4 Termination of the Analysis. An inordinate amount of time could be spent in applying the outlined procedure to a real system. This is not the intent. Good engineering judgment must be used in determining when and how the study is terminated. Although it is difficult to define when the analysis should be halted, a few suggestions are offered.

(1) If the consequences of a failure are not severe in comparison to others identified, a detailed analysis of the causes is not necessary.

(2) Secondary systems need only be analyzed to the extent to which they communicate with the primary system.

(3) When the effects on a communication channel are the same for several sequences of failures, consequences should be analyzed once.

(4) If the causes of failure are obviously incredible, detailed study of the consequences is unnecessary.

(5) As far as possible, the analyst should keep in mind the relative credibility of causes of failure. Time should be spent on the most probable events at the expense of others.

5. Quantitative Analysis Principles

The quantitative analysis uses what is known or assumed about the failure characteristics of individual component parts to predict the failure probability of the system. A mathematical model for system success is used as a function of some or all of the following: failure rates, repair rates, test intervals, mission time, system logic, and surveillance test schedule. In practice the validity of quantitative results may be limited by the quality and quantity of data; however, useful comparative results and sensitivity analyses do not depend on the availability of extensive data.

5.1 Mission Definition. A detailed description of what the system must do for success for the

time interval or task of interest, and for the environmental conditions under which the system must perform is called the mission definition. There may be more than one function of interest, and each must have its own particular mission definition.

Two ways in general use to express mission success, reliability, and availability, are discussed in the following sections.

5.1.1 Reliability. Reliability is the characteristic of an item expressed by the probability that it will perform a required mission under stated conditions for a stated mission time. In the simplest case, repair is not allowed during the stated period of time. If redundant channels comprise a system, one or more channels may fail and may be repaired, provided there is no discontinuity of function. The exact ground rules for treating repair must be clearly delineated.

In all cases, the exact period of time of interest must be stated. A statement of numerical reliability without an accompanying statement of time is meaningless. Two examples of valid reliability missions are as follows:

(1) A pressure switch monitoring reactor pressure is inaccessible for maintenance during reactor operation. An assessment of the numerical reliability of the switch to survive one fuel cycle (a stated time) is a meaningful measure of its integrity.

(2) A safeguard system is initiated and must continue to operate without failure for 100 hours.

The reliability of any component for a mission time t may be calculated exactly by the expression:

$$R(t) = \exp \left[- \int_{t_1}^{t_2} h(t) dt \right] \quad (\text{Eq 1})$$

where

$R(t)$ = reliability (probability of success)

$h(t)$ = hazard rate (instantaneous failure rate)

t = stated time duration of the mission which begins at time t_1 and ends at t_2

Eq 1 is perfectly general and does not require any approximations for its use. Since the hazard rate $h(t)$ is time variant, the reliability can be calculated through times of break-in as well as wear-out.

Generally, data are not available to give a good description of the hazard rate throughout a component's whole lifetime. Also, it has been demonstrated that on many components, there is a period of middle life wherein the hazard rate is relatively constant. Under these conditions Eq 1 reduces to

$$R(t) = \exp[-\lambda t] \quad (\text{Eq 2})$$

where λ is the constant component failure rate which is characteristic of the exponential distribution (see Section 6.1). Eq 2 is the form generally used in most reliability calculations. The exponential form can be expressed as a series of the form:

$$\exp[-\lambda t] = 1 - \lambda t + (\lambda t)^2/2! - (\lambda t)^3/3! + \dots$$

For small values of the product λt ,

$$R(t) = 1 - \lambda t \quad (\text{Eq 3})$$

Where λt is equal to 0.1, the error when using Eq 3 is approximately 5 percent. For the range of values of λt normally encountered, the error is trivial.

The unreliability $\bar{R}(t)$ is the complement of the reliability, and, for small values of λt ,

$$\bar{R}(t) = \lambda t \quad (\text{Eq 4})$$

5.1.2 Availability. Availability may be considered as the fraction of the time the system is operational. If a record is maintained on an operating system, the availability may be computed from the following formula:

$$\text{Availability} = \frac{\text{Up Time}}{\text{Up Time} + \text{Down Time}} \quad (\text{Eq 5})$$

Availability allows for failure, that is, complete loss of function, and subsequent repair. Unlike reliability, availability is not expressed as a function of time, since the long-term availability is time invariant.

For a system that is being designed, the availability may be predicted by calculating the expected down time in any period of interest, usually the interval between tests. Some of the failures that occur in systems announce themselves, and the repair process may start immediately. Other failures are not self-annunciating and can be discovered only by periodic testing. Thus, the down time in Eq 5 is a function of the test interval as well as the actual repair time.

Power plant protection systems are standby systems awaiting a command that may come at any random instant in time. Thus, availability is a good measure of the integrity of such systems.

$$\text{Availability} = \frac{\text{Average time in the "good" state per test interval}}{\text{Average time per test interval}} \quad (\text{Eq 6})$$

For a single component, the availability may be calculated from:

$$\text{Availability} = \frac{\theta - (\lambda\theta)(\theta/2)}{\theta} \quad (\text{Eq 7})$$

where θ is the average time per test interval, $\lambda\theta$ is the probability that the single component fails sometime in interval θ (Eq 4), and $(\theta/2)$ is the expected (average) time that the component was in a failed state.

Eq 7 reduces to

$$\text{Availability} = 1 - \frac{\lambda\theta}{2} \quad (\text{Eq 8})$$

for a single component.

Eq 8 for availability is valid if the following criteria are satisfied:

- (1) The system consists of a single component with failure rate λ
- (2) The product $\lambda\theta$ is small compared to unity
- (3) The system is known to be good at the beginning of each test interval
- (4) Every test interval lasts for a time θ
- (5) When a failure occurs, it is not detected until a test is conducted at the end of the time interval θ
- (6) When a failure is detected at the end of a test interval, it is repaired instantaneously, or the process to be protected is placed in a state not requiring the protection (for example, plant shut down)

Alternatively, the availability can be viewed as the "average" reliability during a given test interval, expressed as

$$\text{Availability} = \frac{1}{\theta} \int_0^{\theta} R(t) dt \quad (\text{Eq 9})$$

where $R(t)$ is an expression for either the reliability of a system, or a single component. In the special case of a single component with

a constant failure rate λ and the product $\lambda\theta$ small compared to unity, Eq 9 yields Eq 8.

For a system consisting of multiple components, the procedure is the same as that above except that the average time in the "good" state per test interval must be calculated by using the mathematical modeling techniques covered in Section 5.2 by using Eq 9.

Availability is frequently defined as the probability that the system will be operational at a randomly selected future instant in time. This definition follows directly from Eq 5, and is a useful definition regardless of whether the availability of a system is being measured or predicted.

5.2 Mathematical Modeling. To compute the reliability or availability of a system, a mathematical expression interrelating the logic and components is used. On simple systems, this mathematical expression may be derived and evaluated manually. On more complex systems, it is convenient to use computer programs especially fitted for this purpose.

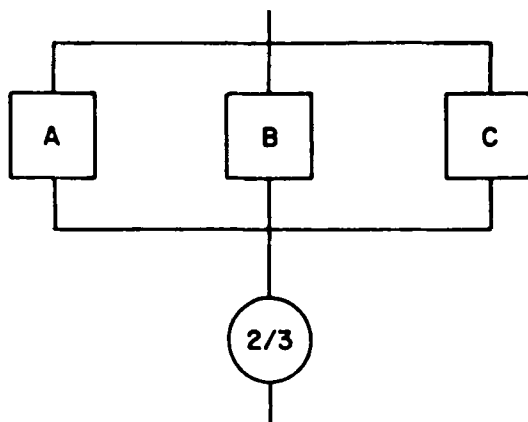
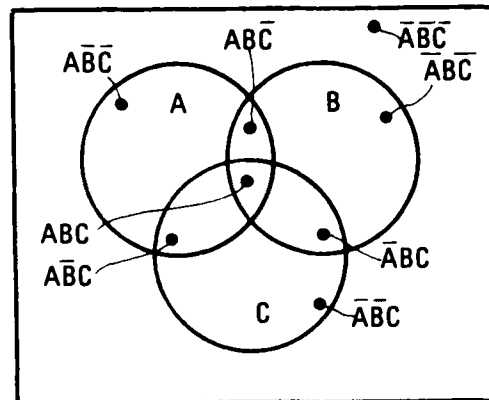


Fig. 5
Basic Two-Out-of-Three (2/3) System

5.2.1 For Manual Calculation. As an example of a manual calculation, consider the reliability block diagram of Fig. 5 wherein A, B, and C represent three channels arranged in a 2-out-of-3 (2/3) logic. There are many ways to calculate the reliability of such a simple system. One basic method is to list all the combinations of the three components in a "truth" table as follows:

	A	B	C	System	Term
(0)	0	0	0	0	$\bar{A} \bar{B} \bar{C}$
(1)	0	0	1	0	$\bar{A} \bar{B} C$
(2)	0	1	0	0	$\bar{A} B \bar{C}$
(3)	0	1	1	1	$\bar{A} B C$
(4)	1	0	0	0	$A \bar{B} \bar{C}$
(5)	1	0	1	1	$A \bar{B} C$
(6)	1	1	0	1	$A B \bar{C}$
(7)	1	1	1	1	$A B C$

where a 1 represents the successful operation of the component, and a 0 represents the failure of the component to operate. Each term in the truth table is mutually exclusive of all other terms as is illustrated in the following Venn diagram:



Since success is defined as "at least any two of the three components operate successfully," terms (3), (5), (6), and (7) of the truth table each represent a success term. All other terms in the truth table are failure terms. The system success probability is now calculated as the sum of the probabilities of each of the success terms. The success probability of each term is now written as:

$$\text{Term (3)} \quad P(S) = P(\bar{A}) P(B) P(C)$$

$$\text{Term (5)} \quad P(S) = P(A) P(\bar{B}) P(C)$$

$$\text{Term (6)} \quad P(S) = P(A) P(B) P(\bar{C})$$

$$\text{Term (7)} \quad P(S) = P(A) P(B) P(C)$$

where $\bar{A}$ is the negation (complement) of A, etc. The system success probability is now expressed as the sum of these terms: