

An American National Standard

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

Sponsor

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

Reaffirmed 25 March 2010

Approved June 13, 1985

IEEE-SA Standards Board

Reaffirmed 24 March 2005

Approved November 21, 1985

American National Standards Institute

Corrected Edition

ISBN 0-471-60205-1

Library of Congress Catalog Number 87-045994

©Copyright 1987

**The Institute of Electrical and Electronics Engineers, Inc.
345 East 47th Street, New York, NY 10017 USA**

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.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied “**AS IS**.”

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; (978) 750-8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Foreword

(This Foreword is not a part of ANSI/IEEE Std 352-1987, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety 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 safety 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 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 safety system designs.

This document was originally 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. In the intervening years, Standard 279 has been superseded by Standard 603, and in March, 1984, Standard 279 was withdrawn. This standard has been expanded in revisions since 1971 to include many technical areas as they have become important. In accord with the current version of Standard 603, IEEE Std 603-1980, it has been generalized to apply to safety systems.

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

The current revision of this document contains much updated information and clarification, but adheres to the general principles put forth in previous editions.

The IEEE will update this document as the state of the technology changes. Comments and suggestions for additional material to be added should be addressed to the Secretary of the IEEE Standards Board.

This document was prepared by Subcommittee 5, Reliability, of the Nuclear Power Engineering Committee of the IEEE Power Engineering Society. The members of the working group and other major contributors were as follows:

R. L. Olson, *Chair*

F. J. Baloh
R. G. Easterling
W. C. Gangloff
S. H. Hanauer

I. M. Jacobs
H. T. Martz
E. Nomm
J. R. Penland
F. Rosa

B. M. Tashjian
M. I. Temme
I. B. Wall
J. J. Wroblewski

At the time this guide was approved, the members of the subcommittee were follows:

W. C. Gangloff, Chair

P. F. Albrecht	P. Hass	J. W Pegram
A. Barchas	W. Hannaman	J. R. Penland
L. E. Booth	B. W. Logan	J. Pittman
F. Chamow	W. J. Luckas, Jr.	S. Reizenstein
K. Comer	R. Miles	F. Rosa
W. I. Crowley	S. P. Mitra	B. M. Tashjian
D. Finnicum	P. K. Niyogi	M. I. Temme
J. R. Fragola	R. L. Olson	E. Wittry
J. F. Fussell	E. S. Patterson	J. J. Wroblewski

At the time this guide was approved, the members of the Nuclear Power Engineering Committee were as follows:

R. E. Allen, Chair

B. M. Rice, Vice Chair

G. R. Leidich, Secretary

J. T. Bauer, Vice Chairman and Standards Coordinator

J. F. Bates	W. C. Gangloff	J. R. Penland
T. M. Bates, Jr.	J. B. Gardner	N. S. Porter
F. D. Baxter	L. Hanes	W. S. Rautio
R. G. Banham	I. M. Jacobs	H. V. Redgate
J. T. Boettger	R. F. Karlicek	A. R. Roby
D. F. Brosnan	A. Laird	W. F. Sailer
W. Buxton	D. C. Lamken	W. G. Schwartz
D. G. Cain	P. G. Lyons	A. J. Spurgin
F. W. Chandler	L. C. Madison	L. Stanley
C. M. Chiappetta	T. J. McGrath	D. F. Sullivan
R. P. Daigle	W. E. O'Neal	P. Szabados
E. F. Dowling	R. W. Pack	L. D. Test
J. J. Ferencsik	M. Pai	J. E. Thomas
E. P. Fogarty	A. Petrizzo	T. R. Vadaró
J. M. Gallagher	E. S. Patterson	F. J. Volpe

The following persons were on the balloting committee that approved this document for submission to the IEEE Standards Board:

R. E. Allen	R. E. Hall	N. S. Porter
J. T. Bauer	L. Hanes	W. S. Rautio
F. D. Baxter	G. K. Henry	H. V. Redgate
R. G. Benham	R. F. Karlicek	B. M. Rice
D. F. Brosnan	J. T. Keiper	A. R. Roby
W. E. Buxton	T. S. Killen	Z. Sabri
F. W. Chandler	A. Laird	W. F. Sailer
R. P. Daigle	D. C. Lamken	A. J. Spurgin
E. F. Dowling	G. R. Leidich	L. Stanley
J. J. Ferencsik	P. C. Lyons	D. F. Sullivan
E. P. Fogarty	W. E. O'Neal	P. Szabados
J. M. Gallagher	R. W. Pack	W. G. Schwartz
W. C. Gangloff	M. Pai	L. D. Test
J. B. Gardner	J. R. Penland	J. E. Thomas
L. C. Gonzalez	C. A. Petrizzo	T. R. Vadaró
B. Grim		F. J. Volpe

...

Authorized licensed use limited to: Tsinghua University. Downloaded on March 07, 2026 at 02:44:37 UTC from IEEE Xplore. Restrictions apply.

When the IEEE Standards Board approved this standard on June 13, 1985, it had the following membership:

John E. May, *Chair*
John P. Riganati, *Vice Chair*
Sava I. Sherr, *Secretary*

James H. Beall
Fletcher J. Buckley
Rene Castenschiold
Edward Chelotti
Edward J. Cohen
Paul G. Cummings
Donald C. Fleckenstein

Jay Forster
Daniel L. Goldberg
Kenneth D. Hendrix
Irvin N. Howell
Jack Kinn
Joseph L. Koepfinger*
Irving Kolodny
R. F. Lawrence

Lawrence V. McCall
Donald T. Michael*
Frank L. Rose
Clifford O. Swanson
J. Richard Weger
W. B. Wilkens
Charles J. Wylie

* Member emeritus

CLAUSE	PAGE
1. Introduction and References	1
1.1 Introduction	1
1.2 References	1
2. Definitions	4
3. Objectives and Methods	5
3.1 Consideration of the Human Factor	5
3.2 Qualitative Analysis	6
3.3 Quantitative Analysis	6
3.4 Applications of Reliability Methodology	7
4. Qualitative Analysis Principles	9
4.1 Failure Mode and Effects Analysis (FMEA)	9
4.2 Fault Tree Analysis	14
4.3 Reliability Block Diagram	19
4.4 Example	21
4.5 Extended Qualitative Analysis for Common-Cause Failures	22
5. Quantitative Analysis Principles	28
5.1 Mission Definition	28
5.2 Mathematical Modeling	31
5.3 Tabular Reference to Popular Logic Configurations	45
5.4 Trial Calculations	46
5.5 Credibility Check of Results	46
6. Guides for Data Acquisition and Use	48
6.1 Input Parameters	48
6.2 Probability Distributions, Parameters, and Estimation	50
6.3 Established Data Programs	56
6.4 Developing Field Data Programs	60
7. Application of Reliability Methods	65
7.1 Introduction	65
7.2 Numerical Goals	66
7.3 Selection of the Modeling Technique	67
7.4 Fault Tree Techniques	68
7.5 The Markov Process as a Reliability Model	69
7.6 Equipment and System Testing	72
8. Annex (Informative)	77

An American National Standard

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

1. Introduction and References

1.1 Introduction

This guide was prepared to provide the designers and operators of nuclear power plant safety systems and the concerned regulatory groups with the essential methods and procedures of reliability engineering that are applicable to such systems. By applying the principles given, systems may be analyzed, results may be compared with reliability objectives, and the basis for decisions may be suitably documented.

The quantitative principles are applicable to the analysis of the effects of component failures on safety system reliability. The principles are applicable during any phase of the system's lifetime. They have their greatest value during the design phase. During this phase, reliability engineering can make the greatest contribution toward enhancing safety.

These 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, in the preparation or revision of operating or maintenance procedures, and in improving test programs. Although not inherently limited, these principles are intended for application to systems covered in the scope of ANSI/IEEE Std 603-1980 [5]¹

1.2 References

The following publications shall be used in conjunction with this standard:

[1] ANSI/ANS 51.1-1983, American National Standard for Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants.

[2] ANSI/ANS 52.1-1983, American National Standard for Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants.²

¹ The numbers in brackets correspond to those of the references listed in 1.2.

² ANSI/ANS publications can be obtained from the Sales Department, American National Standards Institute, 1430 Broadway, New York, NY 10018, or from the American Nuclear Society, 555 North Kensington Avenue, La Grange Park, IL 60525.

- [3] ANSI/IEEE Std 500-1984, IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations.³
- [4] ANSI/IEEE Std 577-1976 (R 1986), IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations.
- [5] ANSI/IEEE Std 603-1980, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.
- [6] APOSTOLAKIS, G. E. and BANSOL, P. P. Effect of Human Error on the Availability of Periodically Inspected Redundant Systems. *IEEE Transactions on Reliability*, vol R-26, 1971, pp 220-225.
- [7] *Automatic Reliability Mathematical Model (ARMM)*. Report NA66-838, North American Aviation, Inc.
- [8] BAIN, L. J. *Statistical Analysis of Reliability and Life Testing Models*. New York: Dekker, 1978.
- [9] BAZOVSKY, I. *Reliability Theory and Practice*. Englewood Cliffs, N J: Prentice-Hall, 1961.
- [10] BEYER, W. H., Ed. *CRC Handbook of Tables for Probability and Statistics*. Cleveland, OH: The Chemical Rubber Co.
- [11] BUSH, S.H. A Reassessment of Turbine-Generator Failure Probability. *Nuclear Safety*, vol 19, Nov-Dec 1978, pp 681-698.
- [12] Conference Record Bibliography, 1979 *IEEE Standards Workshop on Human Factors and Nuclear Safety*. Sponsored by the Institute of Electrical and Electronics Engineers, the United States Nuclear Regulatory Commission, and Brookhaven National Laboratory.
- [13] CRELLIN, G. L., *et al.* Markov Analyses of Nuclear Plant Failure Dependencies. *Proceedings 1979 Annual Reliability and Maintainability Symposium*.
- [14] CROSSETTI, P. A. *Computer Program for Fault Tree Analysis*. Report DUN5508, Douglas United Nuclear.
- [15] *Data Collection for Nonelectronic Reliability Handbook*. Report RADC-TR-68-114, Rome Air Development Center, Rome, NY.
- [16] DUNCAR, A. J. *Quality Control and Industrial Statistics*. American Society for Quality Control, 3rd ed, 1965.
- [17] EDWARDS, G. T. and WATSON, I. A. *A Study of Common-Mode Failures*. Safety and Reliability Directorate, United Kingdom Atomic Energy Authority, July 1979.
- [18] GATELY, W. V. and WILLIAMS, R. L. *GO Methodology—Overview*. EPRI NP-765-1978a, Electric Power Research Institute, Palo Alto, CA
- [19] GATELY, W. V. and WILLIAMS, R. L. *GO Methodology—System Reliability Assessment and Computer Code Manual*. EPRI NP-766-1978b, Electric Power Research Institute, Palo Alto, CA
- [20] GREEN, A. E. and BOURNE, A. J. *Safety Assessment with Reference to Automatic Protective Systems for Nuclear Reactors, Part 3*. Report AHSB (S) R117, United Kingdom Atomic Energy Authority, 11 Charles II Street, London, SW 1, England, 1966.
- [21] HAHN, G. J. and SHAPIRO, S.S. *Statistical Models in Engineering*. New York: Wiley, 1967.

³ANSI/IEEE publications can be obtained from the Sales Department, American National Standards Institute, 1430 Broadway, New York, NY 10018, or from the Institute of Electrical and Electronics Engineers, Service Center, 445 Hoes Lane, Piscataway, NJ 08854-4150.

- [22] HENLEY, E. J. and KUMAMOTO, H. *Reliability Engineering and Risk Assessment*. Englewood Cliffs, N J: Prentice-Hall, 1981.
- [23] HILLARY, R. D. *Failure Mode and Effects Analysis*. Paper presented at the Penn State Reliability Engineering Seminar, Aug 1968.
- [24] KEMENY, J. G. and SNELL, J. L. *Finite Markov Chains*, Princeton, NJ: Van Nostrand, 1960.
- [25] Liquid Metal Engineering Center. *Failure and Problem Reporting for Nuclear Reactors*. USAEC Report LMEC-MEMO-69-6, 1969.
- [26] MANN, N. R., SCHAFER, R., and SINGPURWALLA, N. D. *Methods for Statistical Analysis of Reliability and Life Test Data*. New York: Wiley, 1974.
- [27] MARTZ, H. F. and MC WILLIAMS, T. P. Human Error Considerations in Determining the Optimum Test Interval for Periodically Inspected Standby Systems. To appear in *IEEE Transactions on Reliability*.
- [28] NELSON, W. Hazard Plotting for Incomplete Failure Data. *Journal of Quality Technology*, vol 1, Jan 1969, pp 27-52.
- [29] NUREG-0460. *Anticipated Transients Without Scram for Light Water Reactors*. Apr 1978, vols 1 and 2, Dec 1978, vol 3.
- [30] NUREG-0492. VESELY, W. E., et al. *Fault Tree Handbook*. Jan 1981.
- [31] NUREG/CR-1278. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*. Final Report, Aug 1983.
- [32] NUREG/CR-2254. BELL, B. J., and SWAIN, A.D. *A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants*. May 1983.
- [33] NUREG/CR-2300. HICKMAN, J. W. *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*. Jan 1983.
- [34] NUREG/CR-3010, BNL-NUREG-51601. HALL, R. E., FRAGOLA, J. R., and WREATHALL, J. *Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation*. Brookhaven National Laboratory, Nov 1982.
- [35] ORBACK, S. *Generalized Effectiveness Methodology Analysis Program (GEM)*. Electronics Division, US Naval Applied Science Laboratory, Brooklyn, NY.
- [36] SHAPIRO, S.S. and WILK, M. B. An Analysis of Variance Tests for the Exponential Distribution (Complete Samples). *Technometrics*, vol 14, May 1972, pp 355-370.
- [37] SHOOMAN, M. L. *Probabilistic Reliability—An Engineering Approach*. New York: McGraw-Hill, 1968.
- [38] STEPHENS, M. A. On the *W* Test for Exponentiality with Origin Known. *Technometrics*, vol 20, Feb 1978, pp 33-35.
- [39] VESELY, W. E. *Analysis of Fault Trees by Kinetic Tree Theory*. Report IN-1330, Idaho Nuclear Corporation, Idaho Falls, ID.
- [40] WOODCOCK, E. R. *The Calculation of Reliability Systems—The Program Notes*. Report AHSB (S) R153, Authority Health and Safety Branch, United Kingdom Atomic Energy Authority, 11 Charles II Street, London, SW 1, England.

2. Definitions

availability: The probability that an item or system will be operational on demand.

- 1) **steady-state availability** is the expected fraction of the time in the long run that an item (or system) operates satisfactorily.
- 2) **transient availability** (or instantaneous availability) is the probability that an item (or system) will be operational at a given instant in time. For repairable items, this will converge to steady-state availability in the long term.

break-in period: That early period, beginning at some stated time, during which the failure rate of some items may be decreasing rapidly. Also called “early-failure period” and “infant mortality.”

common-cause failures: Multiple failures attributable to a common cause. (Sometimes called “common mode failure,” but this term is becoming obsolete.)

failure: The termination of the ability to perform a required function (see **item failure** and **mission failure**). 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). The failure rate of an item is often a function of time, although dependence upon number of operations, environmental conditions, etc, may also occur.

human error rate: The frequency of occurrence of human error given the number of opportunities (that is, demands) for that event.

item failure: The termination of the ability of an item to perform its required function.

mean time between failures (MTBF): The average, or expected value, of operating times between failures of a repairable item.

mean time to failure (MTTF): The expected life of a nonrepairable item. Also, the mean or expected value of time to failure of an item.

mean time to repair (MTTR): The average, or expected value, of times required to complete a repair activity.

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

mission failure: The inability to complete a stated mission within stated limits.

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

mutually exclusive events: Events that cannot exist simultaneously.

probability distribution function: The mathematical function that gives $\text{Prob}(X \leq x)$, where X is a random variable and x is a particular value of X .

reliability: The characteristic of an item or system 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 on a given item per unit of time.

risk: A measure of the probability and severity of undesired effects. Often taken as the simple product of probability and consequence.

sensitivity analysis: An analysis that assesses the variation in the value of a given function caused by changes in one or more arguments of the function.

test frequency: The number of tests of the same type per unit time interval; the reciprocal 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 systems or the parts of a system. In general, there are two patterns of interest:

- 1) **simultaneous.** Redundant items or systems are tested at the beginning of each test interval, one immediately following the other.
- 2) **perfectly staggered.** Redundant items or systems are tested such that the test interval is divided into equal subintervals.

unavailability: The probability that an item or system will not be operational at a future instant in time. Unavailability may be a result of the item being repaired (repair unavailability) or it may occur as a result of malfunctions. Unavailability is the complement of availability.

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

3. Objectives and Methods

This guide 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 with an identification of the various failure modes of the parts of a system that contribute to the system unreliability. It also indicates ways to increase the probability that the system will perform its intended function for the environments and time periods of interest. Quantitative analysis utilizes the operating experience of the system's components and provides the designer with a numerical estimate of the system's reliability. The output of the analysis may be used to determine the adequacy of the system and to establish operating procedures such as testing requirements.

3.1 Consideration of the Human Factor

Historically, the focus of reliability analysis has been on equipment failure and success. This neglects the fact that in most systems human interaction and interface with the equipment is an important and sometimes critical element in the overall success or failure of that system. There have been instances, historically, where the human element has been the weakest link in the system and conversely where it has been the strongest. Consequently, when performing system reliability analyses, the system can only be modeled accurately if the human element is considered. This is true for both qualitative and quantitative analyses. In particular, computer software should be investigated thoroughly, because it contains prior human decisions that may be inaccurate.

Even though the human factors engineering discipline has been in existence for some time, the inclusion of human factors engineering in nuclear power plant system reliability analyses is a fairly recent concept. As such, the methodology and data available are not as refined as those that are used to model the contributions of equipment and components to system reliability. Because there has been increased activity in both human factors modeling and human factors data, and since it is likely that this will result in advances in the state of the art in the near future, the reader is advised to refer to recent publications in human reliability analyses. The following sources (also given in the reference section) are listed to provide a starting point for those who are incorporating the human factor into system reliability analysis:

- 1) Bibliography contained in the Conference Record for *1979 IEEE Standards Workshop on Human Factors and Nuclear Safety*, sponsored by the Institute of Electrical and Electronics Engineers, the United States Nuclear Regulatory Commission, and Brookhaven National Laboratory [12].
- 2) NUREG/CR- 1278. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*. Final Report, August 1983 [31].
- 3) Bell, B. J. and Swain, A.D., Sandia National Laboratories. *A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants*. US NRC Report NUREG/CR-2254, May 1983 [32].

- 4) Hickman, J. W., American Nuclear Society. *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*. US NRC Report NUREG/CR-2300, January 1983 [33].
- 5) NUREG/CR-3010. *Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation*, November 1982 [34].

3.2 Qualitative Analysis

Qualitative reliability analyses are used to identify possible ways in which a system can fail 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 imbalances 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 and interfaces between systems
- 5) To provide a systematic compilation of data as a preliminary step to facilitate quantitative analyses

This type of analysis should become an integral part of the normal system design process. The designer is usually the most qualified person 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 the functional required performance of the system
- 2) Identify the system boundaries and components
- 3) Identify significant failures and their consequences (generally called *failure mode and effects analysis—FMEA*)
- 4) Display the above information in a table, chart, fault tree, or other format
- 5) Evaluate overall system reliability relative to the information above and identify potential problems

Each of these steps requires different types of documentation and methods. In the first three steps, special forms are useful for documenting an FMEA. Failure modes are identified by design and operating personnel, but it is usually the job of the design engineer to document these modes. An experienced reliability analyst should be consulted to define the level of detail to be pursued in identifying failures.

In the fourth general step, failure logic forms of various types such as fault trees, system functional diagrams, and block diagrams are used to develop and document the interaction of components within the system. In the last step the analyst is required to estimate the reliability of the system and point out areas where improvements can be made.

3.3 Quantitative Analysis

In quantitative analysis, the analyst represents the system by a mathematical model, apportions the reliability and availability goals among parts of the system, assigns probabilities to each failure mode of concern, and reconciles the calculated estimates of reliability and availability with the over-all 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 operation stages of a plant's life.

This analysis helps the designer to be cognizant of the characteristics of the components selected and to provide a reliability 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 faded 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 influence of the input parameters on the analysis. The relative significance of each component's failure rate in the reliability and availability prediction for the safety system can also be determined.

3.4 Applications of Reliability Methodology

In Sections 4. and 5. of this guide various reliability methods will be introduced. The intent of this subsection is to provide an outline of ways in which these methods can be applied to enhance system reliability. Each method will be discussed in greater detail in Section 7. Although a broad spectrum of reliability methodology exists, all methods have one common feature—they are intended to provide a *systematic* approach to evaluating some aspect of a design's failure potential. Reliability assessments can range from detailed numerical calculations of the failure rate to simple listings of the potential failure modes. It is important to recognize, however, that the methodology itself is only a tool and will provide outputs that reflect, and are limited by, the quality of data input and the assumptions used. If the analyst does not have a thorough understanding of all design functions, the output may be superficial and may have little chance of correctly assessing or improving reliability.

The following discussion will provide reliability methodology in four categories:

- 1) Failure modes and effects analysis (FMEA)
- 2) Logic tree analysis
- 3) System modeling
- 4) Reliability testing

As in other design disciplines, in actual application the results of one methodology serve as input to others with the final design evolving after many iterations.

3.4.1 Failure Modes and Effects Analysis (FMEA)

The FMEA is usually the first reliability activity performed to provide a better understanding of a design's failure potential. It can be limited to a qualitative assessment, but may include numerical estimates of a failure probability.

Important applications of the FMEA include the following:

- 1) The specification of future tests that are required to establish whether or not design margins are adequate relative to the specific failure mechanisms that have been identified in the FMEA.
- 2) Identification of "safe" versus "unsafe" failures for use in the quantitative evaluation of safety-related reliability.
- 3) Identification of critical failures that may dictate the frequency of operational test or maintenance intervals if these failure modes cannot be eliminated from the design.
- 4) The establishment of the level of parts quality (particularly true in electrical systems) needed to meet allocated reliability goals.
- 5) The identification of the need for design modifications to eliminate unacceptable failure mechanisms. These failures could produce unacceptable safety or operational conditions.
- 6) Identification of the need for failure detection.

3.4.2 Logic Trees

Logic trees provide a powerful tool for evaluating the effect of multiple failures (or successes) of components throughout the system being evaluated. They are particularly useful for establishing the level of redundancy (or lack thereof) for various system functions. They also provide a graphic display of events that can be easily reviewed by all design disciplines for completeness and adequate representation of features in their areas of expertise. Applications of logic trees yield the following benefits:

- 1) They identify single point failures. These are single (or multiple dependent) failures that can prevent the system from performing its intended function.
- 2) By focusing attention on critical path failure modes, they provide a structure for evaluating the effect of human performance, which should be considered at important branches of the failure scenario.
- 3) They aid in establishing the frequency of operational tests by identifying those system components that may be required to have high “demand availability.”
- 4) They identify the need for system configuration changes because of inadequate redundancy or diversity to meet allocated reliability goals.
- 5) They provide a systematic method for quantifying the relative probability of various failure scenarios. Thus, even if data available is inadequate for an “absolute” assessment of failure probability, priorities can be established for the efficient allocation of available resources.

3.4.3 System Modeling

In the computation of system reliability or availability, a mathematical expression interrelating logic and components is used. Depending on the complexity of the system and the importance of considerations such as maintenance or testing, different approaches are employed. Two modeling techniques that are often used are success/failure state modeling and Markov modeling. The latter method is particularly useful when maintenance activities are important to the overall prediction.

Applications that require the use of system models include the following:

- 1) The comparison of reliability estimates for various proposed system configurations to provide input to concept selection. It is important to recognize, however, that reliability is only one design consideration, and other factors may dictate that a concept with adequate, not necessarily optimum, reliability may be finally chosen.
- 2) Sensitivity studies to identify the component failures or human errors, or both, having the greatest impact on system reliability. This information can be used to take action to improve the reliability of individual components or to provide a basis for modifying the system configuration.
- 3) Evaluation of operational test intervals that have a direct impact on predicted system reliability. By evaluating the effect on predicted reliability of changing the test interval, a meaningful balance between test frequency and the adverse effect of human interaction can be established.
- 4) Apportionment of reliability goals by establishing reasonable contributions to the overall system goal of lower level subsystems or components.
- 5) Evaluation of the degree to which predicted system reliability satisfies apportioned goals.
- 6) Establishment of the amount of testing required for various system elements (or the system itself) to confirm meeting established goals.

3.4.4 Reliability Testing

Reliability testing can be divided into two broad categories:

- 1) Testing to confirm adequate system reliability prior to placing the system in operation.
- 2) Testing of the system at established intervals after it has been placed in operation to assure high demand availability.

3.4.4.1 Confirmation Testing

This category of testing has as its objective the demonstration that chosen components will meet established reliability requirements in the system configuration in which they are placed. Confirmation testing is a straightforward process when the components or systems are inexpensive, so that a significant number may be tested to failure, although extremely high reliability requirements may make reasonable test plans impractical. In some cases confirmation testing may entail the establishment of component or system reliability estimates by analytical methods; in other cases it may entail confirmation of adequate design margins to defend against the significant failure modes. This latter approach is often necessary when the specific component being tested is large and expensive, which makes testing to establish absolute levels of reliability highly impractical. Examples in this category would be main or auxiliary transformers, reactor shutdown systems (combined mechanical and electrical components), and other large components or systems. For these circumstances, failure tests are often performed to establish margins to failure for significant failure modes identified by analysis, rather than attempting to quantify the actual probability of failure. When practical, for example, for electrical components, testing of a statistically meaningful sample of components can be done under prototypical conditions to estimate reliability. This is usually done at the module or subsystem level with higher level system reliability estimates obtained through the use of mathematical models. In some cases it may be possible to utilize results from tests of, or experience with, similar equipment if differences can be adequately quantified.

3.4.4.2 Operational Test Intervals

Operational 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.

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. 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 draft characteristics of the components have been adequately accounted for when exposed to the expected operating conditions.

In-service assessment 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 safety 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 system goals.

4. Qualitative Analysis Principles

As mentioned in 3.2, the first general step of a reliability analysis is the identification of failure modes. A specific method for accomplishing this step, the FMEA, is discussed, along with fault tree and reliability block diagram analyses that pictorially represent the relationships of important events. Other methods, such as the GO method, are more suited to quantitative computerized analyses, and are discussed in Section 5.

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. The essential function of an FMEA is to consider each major part of the system, how it may fail (the *mode* of failure), and what the effect of the failure on the system would be (the failure *effect*). Usually, the analysis is organized by creating a format like that shown in Table 1.

4.1.1 Purposes of Failure Mode and Effects Analysis [23]

The purposes of an FMEA are as follows:

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

When considering the 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.

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 $P_M > P$ 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 "	

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)
5. DC Power Supply PQ-1, 2, 3	Provide Power For Analog Current 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

By confining the scope of an analysis to determining how the article can fail and what the consequences would be if it should fail, it is usually not necessary to be concerned about stresses and strengths. This limited-scope analysis is a preliminary FMEA, which does not do the whole job, but does provide some early answers when they are needed, and also provides a basis for later studies and analyses. The FMEA provides acceptable documentation of the failure characteristics considered in the design and, if followed through the design process, the way they were reconciled. A suggested form for documenting an FMEA is shown in Table 1.

4.1.2 Timing of a Failure Mode and Effects Analysis (FMEA)

The FMEA should be an integral part of the conceptual design process 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 should be developed throughout the entire design process, from concept selection through documentation of the final design.

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 (FMEA)

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 for the given missions
- 3) Identification of failure categories
- 4) Description of the environmental conditions

The system should be described to the extent that it delineates the boundaries of the system and clearly defines its mission. Interfaces should be clearly defined. One may use a similarly detailed product specification, parts list, or sales agreement. 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 mentioned 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 for a Failure Mode and Effects Analysis (FMEA)

A partial FMEA has been performed on a typical reactor trip system to demonstrate the procedure. Table 1 documents the FMEA for the typical reactor trip function shown in Fig 1 and described in 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. Documentation requirements for analysis of nuclear power plant safety systems are described in ANSI/IEEE Std 577-1976 (R 1986) [4].

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 appropriate to the purposes 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 schematic 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).

Each failure mode that 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, including 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.

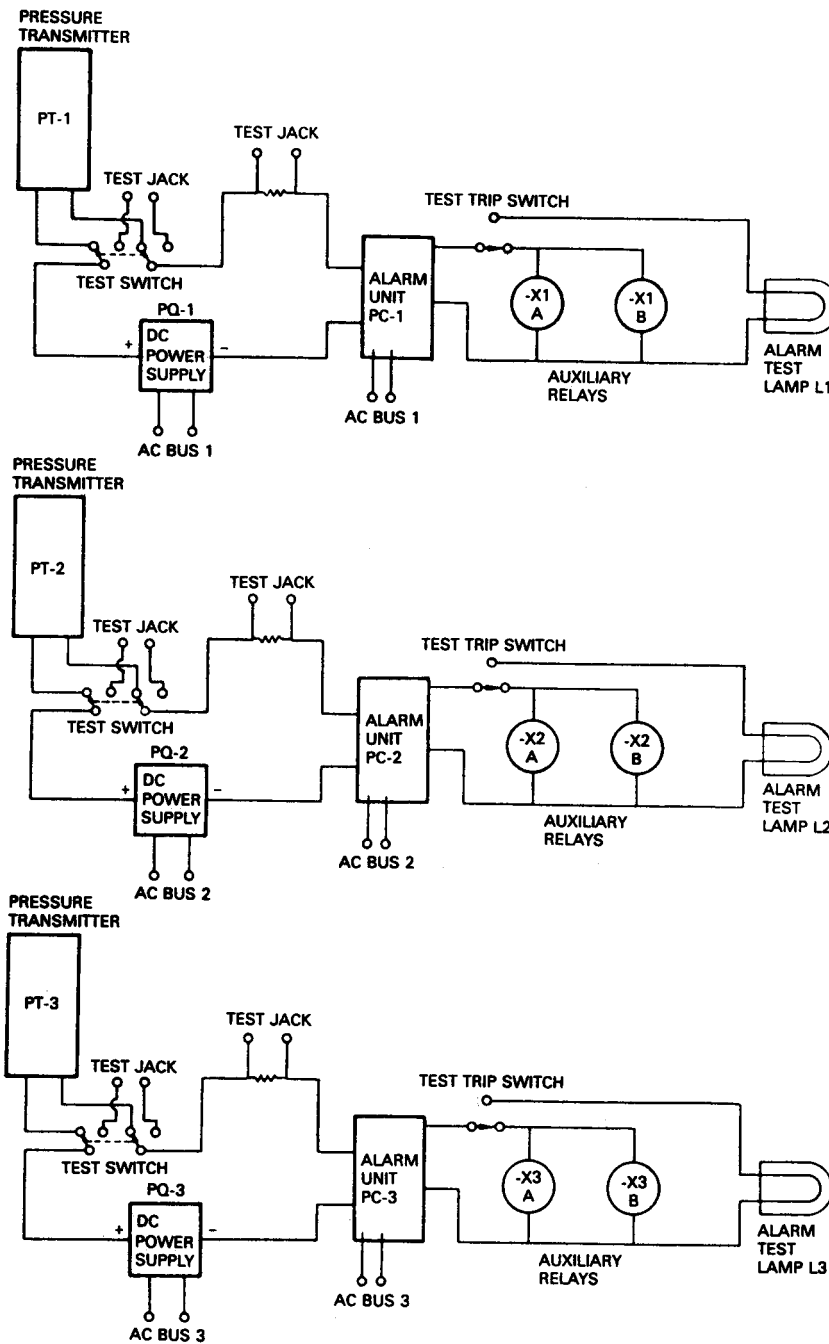
Column 5 describes the effects of the failure on the overall system. It is at this point that a reliability logic block diagram or other tool can be helpful to trace system logic and interconnections. Apparent redundancies may not protect against a single failure for a particular system mode of operation.

Column 6 describes the ways that failure can be detected. 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, particularly whether the failure is acceptable or unacceptable.

4.2 Fault Tree Analysis

Fault tree analysis is a technique, either qualitative or quantitative, by which failures that can contribute to an undesired event are organized deductively in a logical process and represented pictorially. It is one way to diagram and communicate the information developed in a failure mode and effects analysis (FMEA). The resulting arrangement is a tree-like structure with information flow from the branch tips, and the single-most undesired event at the convergence of the branches. A fault tree diagram is illustrated in Fig 2. The symbols used are defined in 4.2.2.



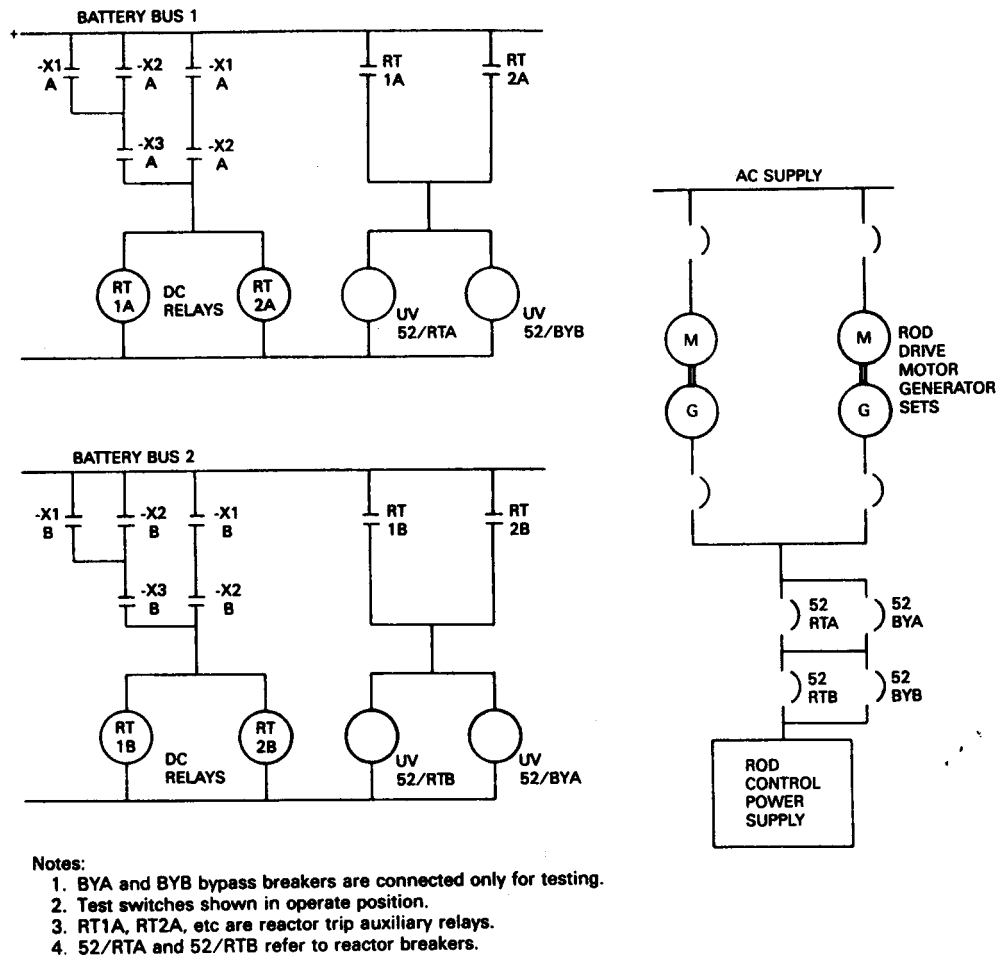


Figure 1—Schematic of a Typical Reactor Trip Function

4.2.1 Functions and Benefits of Fault Tree Analysis

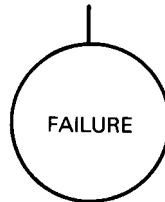
The primary features of the technique are as follows:

- 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 for an 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 progressing to a quantitative analysis
- 6) It provides consistent and clear documentation of the consideration of failure characteristics in the design process
- 7) It provides a basis for identifying multiple failures and common-cause failure mechanisms for the system

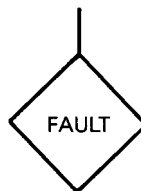
4.2.2 Representation of Events and Operations in a Fault Tree

Because the basic elements of a fault tree are the same regardless of the types of events or systems being analyzed, a standard terminology 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:

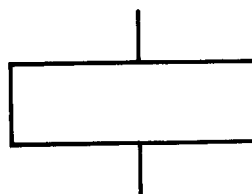
- 1) *Circle*. The circle represents a basic fault event that requires no further dissection because the probability of such events is derived from empirical data or physics of failure analysis. This probability is an input to the fault tree when quantitative analysis is performed.



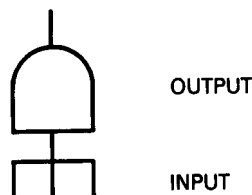
- 2) *Diamond*. The diamond represents a fault event that is assumed to be basic in a given fault tree. This event could be divided further to show how it can result from more basic failures, but is not developed because of lack of significance in such a fault, lack of sufficient details to develop it further, or because empirical data exists at this level.



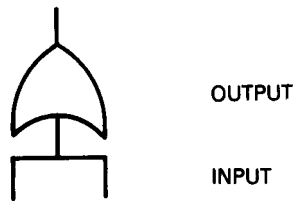
- 3) *Rectangle*. The rectangle represents an intermediate event that results from the combination of events of the types described above through the input of a logic gate.



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



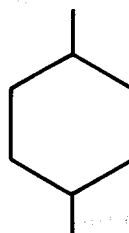
- 5) *OR Gate*. The OR gate is the union operation of sets; that is, an output event occurs if one or more of the input events occur.



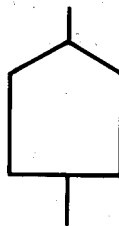
- 6) *Transfer Gates.* The transfer symbol provides a tool to avoid repeating sections of the fault tree. The *transfer-out* gate represents the full branch that follows it, represented by a symbol, say I , and indicates that the branch is repeated somewhere else. The *transfer-in* gate represents the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



- 7) *INHIBIT Gate.* The INHIBIT gate is a special type of AND gate. The output of this gate is caused by a single input, but some qualifying condition must be satisfied before the input can produce the output. The condition that must exist is the conditional input.



- 8) *The External Event, or House.* The house is used to signify an event that is normally expected to occur, such as a phase change in a dynamic system. Thus, the house represents events that are not in themselves faults. This event acts as a switch by being set to 0 or 1 to reflect boundary conditions.



4.2.3 Procedure for Constructing a Fault Tree

The general steps in constructing a fault tree are as follows:

- 1) Define system boundaries, success criteria, and initial conditions.
- 2) 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 be clear. 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.

- 3) 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 details of the system can be developed by subsequent branches.
- 4) Select one of the branches and deduce its next level of subbranches. The manner of deducing the subbranches 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.

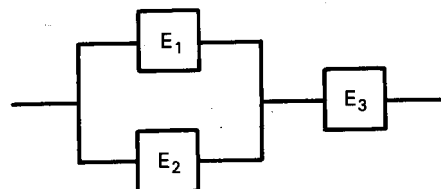
These general steps can be carried out after an FMEA, or concurrently with a formal or informal FMEA. Once the fault tree is prepared, it may be possible to assign numerical values to the probabilities of the events and conditions and, by using methods discussed later, to determine the probability of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

The value of a fault tree, other than to provide a detailed understanding of the system, is that the combinations of failures that will lead to the top event can be identified, either by careful study or by computerized algorithms. Such a combination of failures is called a *cut set*. A minimal cut set is one that will no longer be a cut set if any one failure is removed. Obviously, a knowledge of the minimal cut sets of a fault tree is valuable to understanding the reliability of a system. Computer codes that will find minimal cut sets are referenced in 5.2.2.

4.3 Reliability Block Diagram

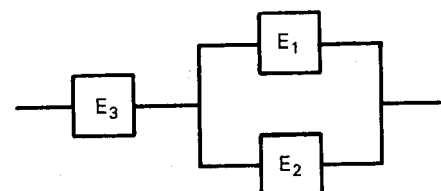
The reliability block diagram (RBD) is a success-oriented diagram that represents the logic of a system. Reliability block diagrams are developed through analysis of the functional relationships among items shown by functional block diagrams and circuit schematics. The interrelation of events needed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

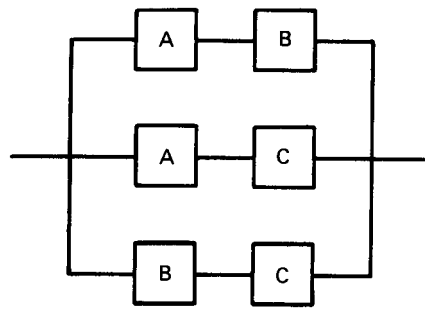


If either path is good, that is, made up of unfailed components, the system is good or successful.

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

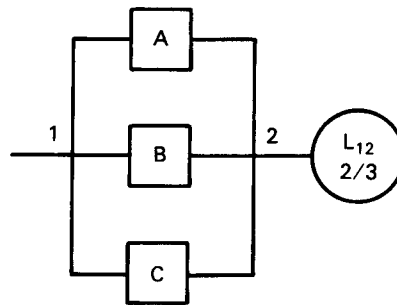


The system logic may be shown in different ways. For example, a 2-out-of-3 system of logic with success paths A - B , A - C , and B - C may be shown as follows:



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 following diagram:



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

The general procedure for constructing a reliability block diagram (RBD) 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) Define system boundaries and initial conditions.
- 3) 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.)
- 4) 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 the paths to successful system function. 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 by using 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 the 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-cause failures and events. The reliability block diagram corresponds closely to a system functional diagram and allows for 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.

The complement to a reliability block diagram can be constructed by considering failure rather than success. Such a diagram is called a *failure state model*, and has the disadvantage of being very unlike a process diagram or system wiring diagram in appearance. Conversely, the reliability block diagram is very similar to a system diagram and is therefore less difficult to construct.

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, process pressure is below the pressure transmitter 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 2-out-of-3 logic, connect dc voltage to two pairs of dc control relays (*RT-1* and *RT-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 and from the rod drive motor-generator (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 in which the process pressure exceeds the setpoint, the three alarm units switch off power, deenergizing the ac control relays. When two out of the three normally open contacts of these ac relays are 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 open the 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 4.4.1.

4.4.3 Fault Tree Analysis

Figure 2 is a fault tree for the typical trip function described in 4.4.1. This tree presents the possible combinations of failures or basic events that can generate the ultimate system failure to trip on demand.

4.4.4 Reliability Block Diagram

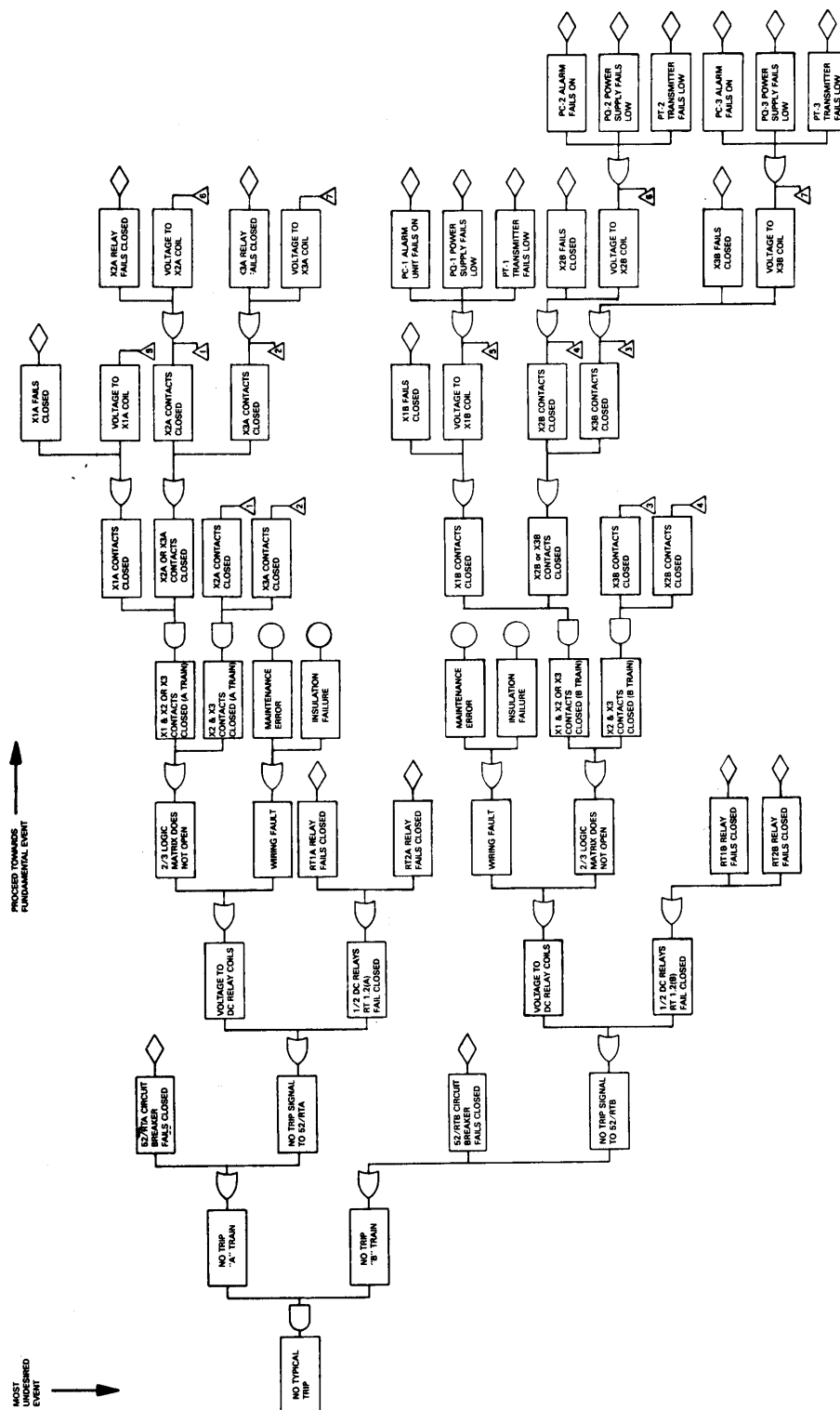
Figures 3 and 4 illustrate two possible reliability block diagram representations of the trip function described in 4.4.1.

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 for Common-Cause Failures

In evaluating the reliability and availability of highly reliable systems such as safety-related systems for nuclear power plants, it is often necessary to extend the qualitative analysis beyond that which is done for failure modes and effects analysis (FMEA) or fault tree analysis by considering common-cause failures of redundant components. The concern for common-cause failures stems from operating experience with nuclear reactor safety systems and other systems that employ a high level of redundancy [29]. The data in [17] show that common-cause failures are a significant proportion of system failures and could be the dominant contributor to the probability of system failure, especially in systems designed against the effects of independent failures. This section describes an extended qualitative analysis procedure, based on the FMEA, that is designed to suggest to the analyst possible common-cause failure mechanisms not normally considered in an analysis of independent component failures. The procedure for common-cause failure analysis is flexible and can be molded to suit the needs of the analyst. It is not presented as a standard, nor as an ideal method of analysis. Rather, it is intended to be a general guide or a possible design and analysis tool.

While the definition of common-cause failure is very general, the analysis is usually intended to find multiple failures of components in two or more separate channels of a redundant system, leading to a failure of this system to perform its intended function. The analysis is applicable when the redundancy is provided by either identical channels or diversely configured channels, or both. In either case, the multiple features are dependent on a common event or condition, for example, a single initiating cause. The following discussion identifies three types of statistical dependence that are helpful in identifying and categorizing common-cause failures. One is a dependence among failure events themselves. The failure of one component can increase the stress on a second component, and the probability of failure of the second component is thus greater than it would be if the first had not failed. A second type of dependence is the dependence of failure events on the occurrence of a separate initiating cause. For example, given an initiating cause that is not catastrophic, such as a temporarily elevated temperature, the probability of early but not simultaneous failure of several components is greater than it would be if the initiating event had not occurred. A third type of dependence could appear when all components experience the same extreme conditions simultaneously, such as during an earthquake. There are many other classifications for common-cause failures that may be useful to the analyst for identifying common-cause failure initiators.



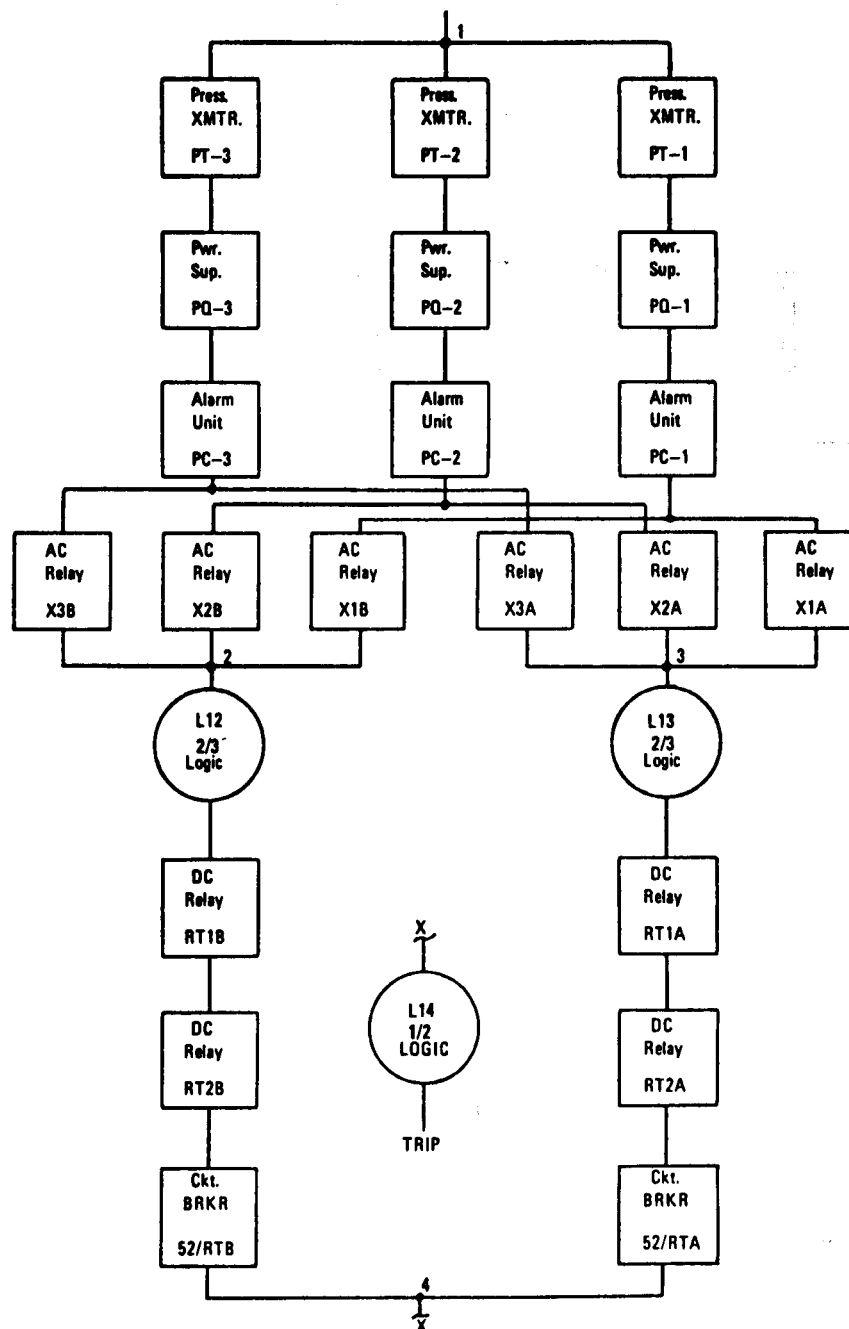


Figure 3—Reliability Block Diagram of a Typical Trip Function

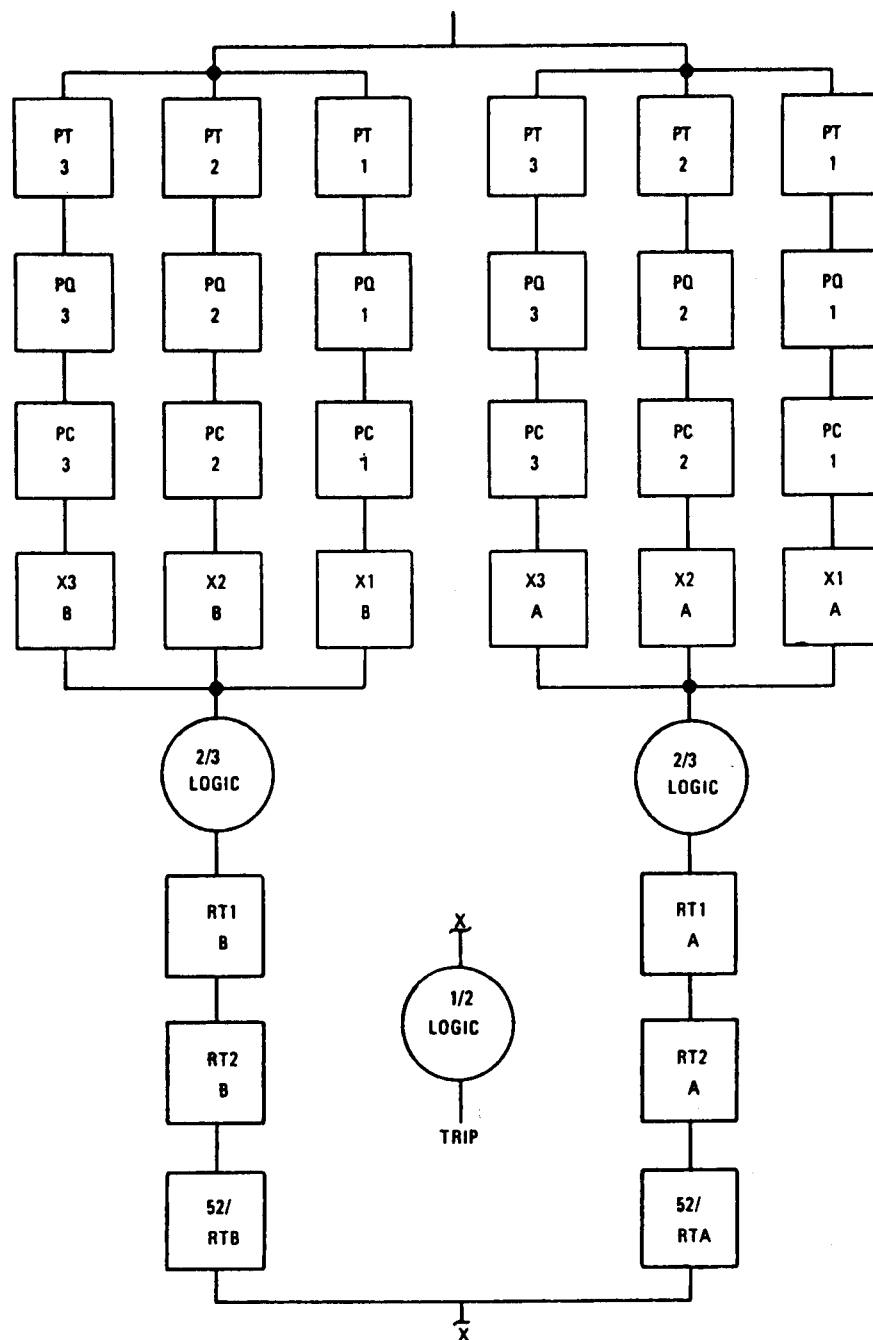


Figure 4—Alternative Reliability Block Diagram of a Typical Trip Function

The common-cause failure analysis (CCFA) is designed to identify modes and mechanisms of failures of components that are considered to be redundant. For example, this extension of the analysis should have identified a situation in which a number of control rods could fail to operate due to a single obstructed pipe.

Sometimes failure events occur in chain-like fashion, where one failure of a component leads to an overstressed condition for another component and thereby causes it to fail. The second failure in turn leads to a third, etc. Usually several different areas or systems in a plant are affected. Failure sequences of this type are called cascade failures.

These are distinguished from common-cause failures, because they need not involve a critical number of failure events in redundant channels of a system. An example of a cascade-failure sequence would be one 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. Cascade failures should be identified directly from the FMEA without recourse to extended qualitative analysis. The FMEA includes a list of the effects on the primary system under evaluation or other systems that may interact with the primary system, or both. These listings should suggest possible cascade failure sequences. Of course, the success of a cascade failure analysis depends on the thoroughness of the analysis and the skill and experience of the analyst. Because cascade failures may not be apparent in the previous analyses, they are included in the extended qualitative analysis.

4.5.1 Extension of the FMEA

The analyst may vary the depth and scope of this analysis to suit his purpose and the system being studied. The following procedural steps may be useful as a basis for the CCFA:

- 1) *Define the System and System Boundaries.* This step is normally completed in the FMEA; however, it is stated here again to emphasize the need for particular care in the definition of system boundaries. Paths of intersystem communication (pipes, wires, relays, etc) and other interactions (environmental conditions, people, etc) must be completely specified and listed. Some interactions may be quite subtle. In one case, the control system and the protection system interacted in an undesirable way through the controlled process itself.
- 2) *Define All Anticipated System Operation Modes.* Typically, the operation modes would include automatic, manual, test, and bypass. 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 ways under unusual, but foreseeable, operating conditions. A definition of the system and system boundaries for each operating mode is often useful in identifying possible common-cause failure events.
- 3) *Describe the Operation of System and Environmental Conditions Applicable to All Operating Modes.* The environmental description should include any conditions that can be credibly expected to occur within the life of the plant, in addition to those normally anticipated.

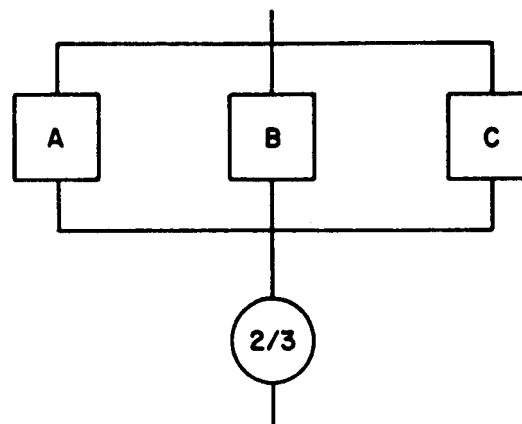


Figure 5—Basic 2-Out-of-3 (2/3) System

- 4) *Prepare a Critical Items List.* From the list of all system components and modules (made for the FMEA), identify and list those that comprise redundant channels in the system. Pay special attention to those items that are not completely diverse. Also make a list of any nonredundant subsystems that are composed of components and modules that are identical or similar in design or construction. This list may reveal additional dependencies not readily detected.

- 5) *Prepare a List of Failure Modes.* Determine and list all possible failure modes of the channels or subsystems identified above. When appropriate, the failure modes of a component or module should not be limited to upscale or 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.
- 6) *Document Results.* Using Fig 4 or 5 as a guide, determine and list all means by which the failures may occur. The following questions may be helpful in recognizing potential failure causes.
 - a) Were elements of redundant channels made by a single manufacturer? What are credible sources of failure in the manufacturing processes?
 - b) What environmental factors (dust, humidity, radiation, temperature, liquid spillage, etc) could cause the failure?
 - c) Can test, calibration, maintenance, or installation errors cause simultaneous failures of elements of redundant channels? Installation and maintenance procedures should be evaluated realistically to determine what can happen, rather than what should occur.
 - d) What possible operator interactions could produce multiple channel failures?

4.5.2 Extended Fault Tree Analysis

For a small system, common-cause failures can be identified in theory by constructing a fault tree, finding the minimal cut sets, and examining the minimal cut sets to determine if any cause can produce failure of all of the components in a minimal cut set. This procedure is extremely difficult in practice because fault trees are seldom produced in sufficient detail to allow discovery of subtle common causes, they are frequently unmanageably large and must be broken into subtrees or modules, and because it may be difficult to identify common causes that might affect all of the components in a minimal cut set. A hypothetical example that would be difficult to identify by fault tree methods is a safety system that upon starting causes a water hammer to rupture a pipe in a distant part of a building, spraying water on and disabling an instrument that would have actuated a redundant safety system after a time delay. While the example might seem farfetched, similar failures have occurred. This potential multiple failure would be detected by fault tree methods only if the modeler had suspected that it could occur, and had arranged for the location of the piping to be coded in the fault tree. Also, the fault tree approach requires careful definition of the top event. Common-cause failures may produce unforeseen, but severe, top events.

Despite the difficulties described above, several computer codes have been written to detect potential common-cause failures in fault tree models, and many unsuspected common-cause failure combinations have been detected with them. The codes and the methods that they use are discussed in [8]. While these computer codes cannot guarantee that all credible common-cause failure situations will be identified, the same must be said of any other technique.

4.5.3 Termination of the Analysis

An inordinate amount of time could be spent in applying the outlined procedures 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 multiple failures, consequences should be analyzed once.
- 4) If the causes of failure are obviously incredible, detailed study of the consequences is unnecessary. For example, the analyst could estimate the rate of occurrence of a transient and the fraction of time F the system is in the mode being analyzed. If $\lambda F \geq 10^{-6}$ 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 $\lambda F < 10^{-6}$ per year, the probability of occurrence of such postulated events may be so small as to be negligible, irrespective of the consequences. The numerical value of 10^{-6} per year is used here only as an example. The actual value used will vary with application. For example, if there were a large number of independent postulated occurrences for a system, the failure rate could be large even though each occurrence had a very low probability.
- 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 probability of individual component parts and failure characteristics of the system to predict the failure probability of the system. A mathematical model for system success or failure 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 schedules. In practice the validity of quantitative results may be limited by the quality and quantity of the data; however, useful comparative results and sensitivity analyses do not depend on the availability of extensive data. The following sections describe the principles of quantitative analyses.

5.1 Mission Definition

A detailed description of what the system must do for the success of 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, used to express mission success, reliability, and availability are discussed in the following sections.

5.1.1 Reliability

The reliability of an item is the probability that it will perform a required mission under stated conditions for a stated mission 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 should be accompanied by a statement of time. Two examples of valid reliability missions are as follows:

- 1) A pressure switch monitoring reactor pressure is inaccessible for maintenance during reactor operation. Its mission is to operate correctly for one complete fuel cycle (a stated time).
- 2) A safety system is initiated and must continue to operate without failure for 100 hours.

The reliability of any continuously operating item for a mission time t_m may be calculated exactly by the expression

$$R(t_m) = \exp - \int_0^{t_m} \lambda(t) dt \quad (1)$$

where

- $R(t_m)$ = reliability (probability of mission survival)
 $\lambda(t)$ = failure rate
 t_m = mission duration; mission begins at time $t=0$

The failure rate can be thought of as an instantaneous failure probability. This is because $\lambda(t)dt$ is the probability of failure in the time interval, $(t, t + dt)$, given survival of the item to time t . In the above expression for $R(t_m)$, the assumption is that the item is functioning at the beginning of the mission. Further discussion of the relationships among reliability, failure rate, and the probability distribution of an item's lifetime is given in the references listed in 1.2.

The failure rate may be any arbitrary function. For many types of equipment, a "bathtub-shaped" function is thought to be appropriate. Early in life, the failure rate may be large, but it usually decreases as early failures occur. This is followed by a period in which the failure rate is relatively constant, followed by a period of increasing failure rate as "wearout" occurs. If the mission occurs over a period of time in which the failure rate can be taken as a constant, Eq 1 reduces to

$$R(t_m) = \exp(-\lambda t_m) \quad (2)$$

where λ is the constant value of $\lambda(t)$ over the mission's duration.

The exponential form can be expressed as a Taylor series expansion:

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

For small values of the product λt ,

$$R(t) \approx 1 - \lambda t \quad (3)$$

Where t is equal to 0.1, the error when using Eq 3 is approximately 0.5%. For the range of values of λt normally encountered, the error is trivial. The table below shows some values of the result and the percentage error.

λt	$1 - \lambda t$	$e^{-\lambda t}$	% Difference
0.01	0.99	0.99005	0.005
0.02	0.98	0.9802	0.02
0.05	0.95	0.95123	0.13
0.10	0.90	0.9048	0.54
0.15	0.85	0.8607	1.26

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

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

Not all items have a reliability that is a function of mission time. For example, some items do not operate continuously, but only "on demand". Their success or failure may be only a function of the stress imposed by the demand, not the time at which the demand occurred or the age of the item. Thus, their reliability is defined as their probability of success, on demand, not with respect to some mission time.

Components may have significantly different failure rates depending upon their state, such as in operation, installed but not operating, or in storage. The importance of such differences depends on the magnitude of the differences and the time spent in each state. It is most important to realize that a replacement component may not be in the "fresh" state.

5.1.2 Availability (Steady-State)

The concept of steady-state availability is applied to a repairable or replaceable item, although the repair time can be allowed to become infinite in calculations to simulate nonrepairable cases. Such an item operates until failure, is then repaired, operates until it fails again, is repaired, operates, fails, is repaired, etc. Conceptually, this sequence continues forever. In this discussion, "repair" can mean either the repair or the replacement of a part or parts. Instantaneous availability is defined as the probability that at a point in time the item is in the operating state. In the limit, this probability is related to the average operating and repair times over an infinite time period by

$$\text{Availability} = \frac{\text{Average up time}}{\text{Average up time} + \text{Average down time}} \quad (5)$$

Two situations need to be distinguished. In the first, the failure of an item is known when it occurs, and repair is initiated. In this case, assuming there is no logistic delay time, “down time” equals repair time. In the other situation, the failure is not self-annunciating and can only be discovered by periodic testing. In this case, down time is the period from time of failure to the next test, plus repair time.

In general, availability is a complicated mathematical function, depending on the test interval and the probability distributions of operating time and repair time. In the following situation, though, a simple approximation is possible. Suppose:

- 1) The item has a constant failure rate.
- 2) Failures are detectable only by periodic testing.
- 3) The time between tests is a constant, T .
- 4) λT is small enough to warrant approximating the probability of failure during the test interval by $R(T) = \lambda T$.
- 5) Down time (repair time plus any logistic delay time) is quite small relative to T .
- 6) The item is in operating condition at the beginning of each test interval. This means that the test is certain to detect a failed item and that repair is perfect. It also means that testing does not induce the item to fail or alter its failure rate.

Rewriting Eq 5 as

$$\text{Availability} = \frac{U}{U + D}$$

and recognizing that

$$U + D = T$$

then

$$\text{Availability} = \frac{T - D}{T} = 1 - \frac{D}{T}$$

The probability of failure during T is λT , and on average the down time is one-half the interval, so that

$$\text{Down time} = D = \lambda T \cdot \frac{T}{2}$$

and, thus Eq 5 reduces to

$$\text{Availability} \cong 1 - \frac{\lambda T}{2} \quad (6)$$

If condition 1 above is dropped and it is assumed that the item has reliability $R(t)$, then availability equals the average reliability over the test interval:

$$\text{Availability} = \frac{1}{T} \int_0^T R(t) dt \quad (7)$$

This expression is exact. In the special case of $R(t) = \exp(-\lambda t)$,