352-87 4805702 0008128 0
ANSI/IEEE Std 352-1987
R-34-11

IEEE GUIDE FOR GENERAL PRINCIPLES OF RELIABILITY ANALYSIS OF NUCLEAR POWER GENERATING STATION SAFETY SYSTEMS

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

352-87 4805702 0008129 2
R-34-71

An American National Standard

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



Published by
The Institute of Electrical and Electronics Engineers, Inc



Distributed in cooperation with
Wiley-Interscience, a division of John Wiley & Sons, Inc

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

352-87 4805702 0008130 9

ANSI/IEEE
Std 352-1987
(Revision of ANSI/IEEE
Std 352-1975)

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

Approved June 13, 1985

IEEE Standards Board

Approved November 21, 1985

American National Standards Institute

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

352-87 4805702 0008131 0

ISBN 0-471-60205-1

Library of Congress Catalog Number 87-045994

© Copyright 1987 by

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.

October 13, 1987 *SH11296*

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

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, *Chairman*

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 as follows:

W. C. Gangloff, *Chairman*

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

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

R. E. Allen, *Chairman*

B. M. Rice, *Vice Chairman* **G. R. Leidich,** *Secretary*

J. T. Bauer, *Vice Chairman and Standards Coordinator*

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

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

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

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

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

John E. May, *Chairman* **John P. Riganati,** *Vice Chairman*
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

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

IEEE Standards documents are developed within the Technical Committees of the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Board. Members of the committees serve voluntarily and without compensation. They are not necessarily members of the Institute. The standards developed within IEEE represent a consensus of the broad expertise on the subject within the Institute as well as those activities outside of IEEE which have expressed an interest in participating in the development of the standard.

Use of an IEEE Standard is wholly voluntary. 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 once 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.

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.

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 all 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 technical 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 on standards and requests for interpretations should be addressed to:

Secretary, IEEE Standards Board
345 East 47th Street
New York, NY 10017

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Contents

SECTION PAGE

1. Introduction and References 13
   1.1 Introduction 13
   1.2 References 13

2. Definitions 17

3. Objectives and Methods 19
   3.1 Consideration of the Human Factor 19
   3.2 Qualitative Analysis 20
   3.3 Quantitative Analysis 21
   3.4 Applications of Reliability Methodology 21
      3.4.1 Failure Modes and Effects Analysis (FMEA) 22
      3.4.2 Logic Trees 22
      3.4.3 System Modeling 22
      3.4.4 Reliability Testing 23

4. Qualitative Analysis Principles 25
   4.1 Failure Modes and Effects Analysis (FMEA) 25
      4.1.1 Purposes of Failure Mode and Effects Analysis 28
      4.1.2 Timing of a Failure Mode and Effects Analysis 28
      4.1.3 Preparatory Steps for a Failure Mode and Effects Analysis 29
      4.1.4 Procedure for a Failure Mode and Effects Analysis 29
   4.2 Fault Tree Analysis 32
      4.2.1 Functions and Benefits of Fault Tree Analysis 32
      4.2.2 Representation of Events and Operations in a Fault Tree 34
      4.2.3 Procedure for Constructing a Fault Tree 35
   4.3 Reliability Block Diagram 37
   4.4 Example 37
      4.4.1 Description of a Typical Reactor Trip Function 37
      4.4.2 Failure Mode and Effects Analysis 38
      4.4.3 Fault Tree Analysis 38
      4.4.4 Reliability Block Diagram 38
   4.5 Extended Qualitative Analysis for Common-Cause Failures 38
      4.5.1 Extension of the FMEA 42
      4.5.2 Extended Fault Tree Analysis 43
      4.5.3 Termination of the Analysis 44

5. Quantitative Analysis Principles 45
   5.1 Mission Definition 45
      5.1.1 Reliability 45
      5.1.2 Availability (Steady-State) 47
   5.2 Mathematical Modeling 48
      5.2.1 Manual Calculation 48
      5.2.2 For Computer Calculation 59
   5.3 Tabular Reference to Popular Logic Configurations 63

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

SECTION PAGE

5.4 Trial Calculations 64
5.4.1 Manual Calculations 64
5.4.2 Computer Calculations 64
5.5 Credibility Check of Results 64
5.5.1 Comparison for Prior Analysis 64
5.5.2 Sensitivity Analysis 64
6. Guides for Data Acquisition and Use 67
6.1 Input Parameters 67
6.1.1 Failure Rates 67
6.1.2 Mean Time to Repair 67
6.1.3 Mission Time 68
6.1.4 Test Interval 68
6.1.5 Test Schedule 68
6.2 Probability Distributions, Parameters, and Estimation 69
6.2.1 Exponential Distribution 70
6.2.2 Poisson Distribution 73
6.2.3 Binomial Distribution 73
6.2.4 Weibull Distribution 75
6.2.5 Combining and Updating Data 75
6.3 Established Data Programs 76
6.3.1 Failure Rate Data Program (FARADA) 76
6.3.2 Government-Industry Data Exchange Program 76
6.3.3 Nonelectric Parts Reliability Data (NPRD-1) 77
6.3.4 Energy Technology Engineering Center (ETEC) 77
6.3.5 United Kingdom Atomic Energy Authority Data Program (UKAEA), National Center of Systems Reliability (SYREL) 77
6.3.6 Nuclear Plant Reliability Data System (NPRDS) 77
6.3.7 Generating Availability Data System (GADS) 78
6.3.8 Licensee Event Report 79
6.3.9 Operating Units Status Report (NUREG-0020) 79
6.3.10 Reactor Safety Study, WASH-1400 (NUREG-75/014) 79
6.3.11 Failure Incident Report Review (FIRR) 79
6.3.12 IEEE Survey by Industrial and Commercial Power Systems 79
6.3.13 Nuclear Power Experience Reports 80
6.3.14 IEEE Nuclear Reliability Data Manual—ANSI/IEEE Std 500-1984 80
6.4 Developing Field Data Programs 80
6.4.1 Failure Analysis 81
6.4.2 Failure Data Analysis 83

7. Application of Reliability Methods 87
7.1 Introduction 87
7.2 Numerical Goals 87
7.2.1 Bases for Establishing Numerical Goals 88
7.2.2 Specific Goals 88
7.2.3 Procedures 89

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

SECTION PAGE

7.3 Selection of Modeling Technique 89
7.3.1 Model Requirements 89
7.3.2 Model Limitations 90
7.4 Fault Tree Techniques 90
7.4.1 Characteristics 90
7.4.2 Recommended Uses 91
7.5 The Markov Process as a Reliability Model 91
7.5.1 Constant Failure and Repair Rate Components 94
7.5.2 Constant Repair or Switching Time Components 94
7.5.3 Constant Success/Failure on Demand 94
7.6 Equipment and System Testing 95
7.6.1 Acceptance Sampling 96
7.6.2 Initial Test Intervals 99
7.6.3 In-Service Adjustment of Test Intervals 101

APPENDIX

A1. Introduction 103
A2. Procedure 103
A2.1 System Definition 103
A2.2 Failure Mode and Effects Analysis (FMEA) (Qualitative Analysis) 104
A2.3 Common-Mode-Failure Analysis 104
A2.4 Reliability/Availability Prediction (Quantitative) 104
A2.4.1 Determination of Test Interval 104
A2.4.2 Reconciliation of System Goals 104
A3. Illustrative Examples 104
A3.1 System Definition 104
A3.2 Qualitative Analysis—FMEA 106
A3.2.1 Uses of the FMEA 106
A3.2.2 Mechanics of the FMEA 106
A3.2.3 Results of FMEA 120
A3.3 Common-Mode-Failure Analysis 123
A3.3.1 Failure Combinations 123
A3.3.2 Causative Factors 124
A3.3.3 Preventative Measures 124
A3.3.4 Evaluation of System Susceptibility to Common-Mode Failure 124
A3.4 Quantitative Analysis 128
A3.4.1 Fault Tree Analysis 128
A3.4.2 System Goals and Test Intervals 130
A4. Bibliography 138

FIGURES

Fig 1 Schematic of a Typical Reactor Trip Function 30-31
Fig 2 Fault Tree for a Typical Trip Function 39

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

FIGURES PAGE

Fig 3 Reliability Block Diagram of a Typical Trip Function 40
Fig 4 Alternative Reliability Block Diagram of a Typical Trip Function .. 41
Fig 5 Basic 2-Out-of-3 (2/3) System 43
Fig 6 Venn Diagram for Basic (2/3) System 52
Fig 7 Reliability Block Diagram of a Simple 2/3 System 55
Fig 8 Improved Model of a 2/3 System 56
Fig 9 Sensitivity Study on Model of Fig 8 65
Fig 10 Distribution Graphical Evaluation 84
Fig 11 Transition Rate Diagram 93
Fig 12 Transition Rate Matrix 94

TABLES PAGE

Table 1 Typical Failure Mode and Effects Analysis Documentation 26-27
Table 2 Unavailability as a Function of Logic Configuration and Testing Schedule (Adapted from [20]) 63
Table 3 Some Typical Failure Modes and Mechanisms 82
Table 4 Two-Point Design of a Single-Sampling Plan with α Approximately 0.05 and β Approximately 0.10 98
Table 5 Test Interval as a Function of Logic Configuration and Unavailability Design Goal G 100

APPENDIX FIGURES PAGE

Fig A1 One Function Diagram for a Typical Reactor Trip Function 105
Fig A2 Fault Tree for No Typical Trip Function 129
Fig A3 Fault Tree for Limit Consequences 135

APPENDIX TABLES PAGE

Table A1 Generic Part Failure Rate and Failure Mode Classification 107
Table A2 Principal Design Components and Their Primary Function 109
Table A3 Failure Mode and Effects Analysis 111-119
Table A4 Summary of Failure Modes and Effects 121
Table A5 Summary of Results 122
Table A6 Nonannunciating Failures Detectable by Test 123
Table A7 Minimum Number of Like Functional Blocks Required to Suffer Common-Mode Failure to Prevent Automatic Reactor Trip 125
Table A8 Common-Mode-Failure Preventative Measures 126
Table A9 Common-Mode-Failure Matrix Relating Causative Factors to Equipment Required Failure Modes in Reactor Protection System 127
Table A10 Logic and Boolean Expressions for Events in a Fault Tree .. 132-133

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

..... 141

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.

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

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

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

[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, NJ: 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 DUN-5508, Douglas United Nuclear.

---

[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 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.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

[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.

[22] HENLEY, E. J. and KUMAMOTO, H. *Reliability Engineering and Risk Assessment.* Englewood Cliffs, NJ: 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.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

[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.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

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.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

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 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.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

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].

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

(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.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

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 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 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 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 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

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

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:

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

(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.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

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.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

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.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

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	Makes Trip 1/1	Monthly Test	
			UV Trip Attachment Mechanism Stuck	"	"	
			Fuse Main Contacts	"	"	
		Fail Open	Loss of DC Control Power	Spurious Trip	Spurious Trip	Immediate Detection
			UV Coil Failure	"	"	
			Worn Trip Latch	"	"	
2. DC Control Relay	Break Ckt. To Trip Breaker UV Coil on Trip (DE-EN To Trip)	Fail Closed	Contacts Shorted or Fused	Makes Trip 1/1	Monthly Test	
			Armature Jammed	"	"	
			Wiring Fault	"	"	
		Fail Open	Loss of DC Control Power	Spurious Trip	Spurious Trip	Immediate Detection
			Coil Failure	Spurious Trip if 2/2 Fail	"	
			Broken Contacts	"	"	
			Broken Wire or Loose Connec.	"	"	
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	Makes 1 Train 2/2 vice 2/3	Monthly Test	
			Armature Jammed	"	"	
			Wiring Fault	"	"	
		Fail Open	Loss of AC Power (Instr. Bus)	Spurious Trip if 2/3	Spurious Trip	
			Coil Failure	"	"	
			Broken Contacts	"	"	
			Broken Wire or Loose Connec.	"	"	

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

352-87 4805702 0008154 1

Table 1 (*continued*)

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)
4. Alarm Unit PC-1, 2, 3	Remove AC Power To Relays For $P_M > P$ set	Fail Off	Transformer Failure	Makes Both Trains 1/2	Spurious Trip if 2/3 Fail	Partial Trip Alarm
			Open Circuit in Output Sect.	"	"	
			Setpoint Drift	"	"	
		Fail On	Short in Output Section	Makes Both Trains 2/2	Monthly Test	
			Setpoint Drift	"	"	
5. DC Power Supply PQ-1, 2, 3	Provide, Power For Analog Current Loop	Fail Low or Off	Transformer Failure	Makes Both Trains 1/2	Spurious Trip if 2 Fail	Partial Trip Alarm
			Diode Failure	"	"	
		Fail High	Heat Effects	Makes Both Trains 2/2	Monthly Test	
			Misadjustment	"	"	
6. Pressure Transmitter PT-1, 2, 3	Convert Pressure To Analog Current	Fail Low	Corrosion	Makes Both Trains 2/2	Monthly Test and Comparison with Redundant Channel Indicators	Possible Immediate Detection
			Wear	"		
			Mechanical Damage	"		
			Heat Effects	"		
		Fail High	Misadjustment	Makes Both Trains 1/2	Spurious Trip if 2 Fail	Partial Trip Alarm

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

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

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

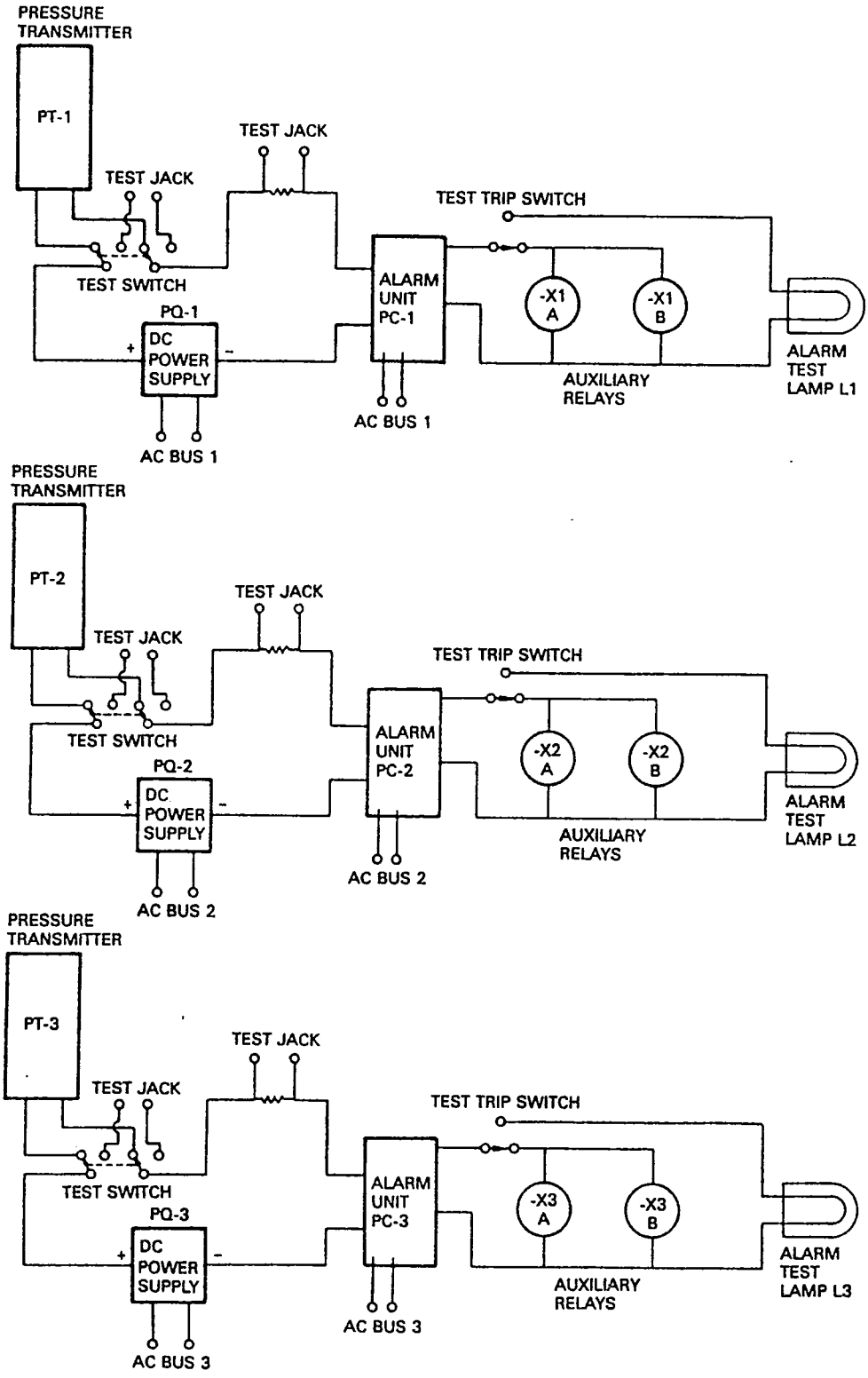
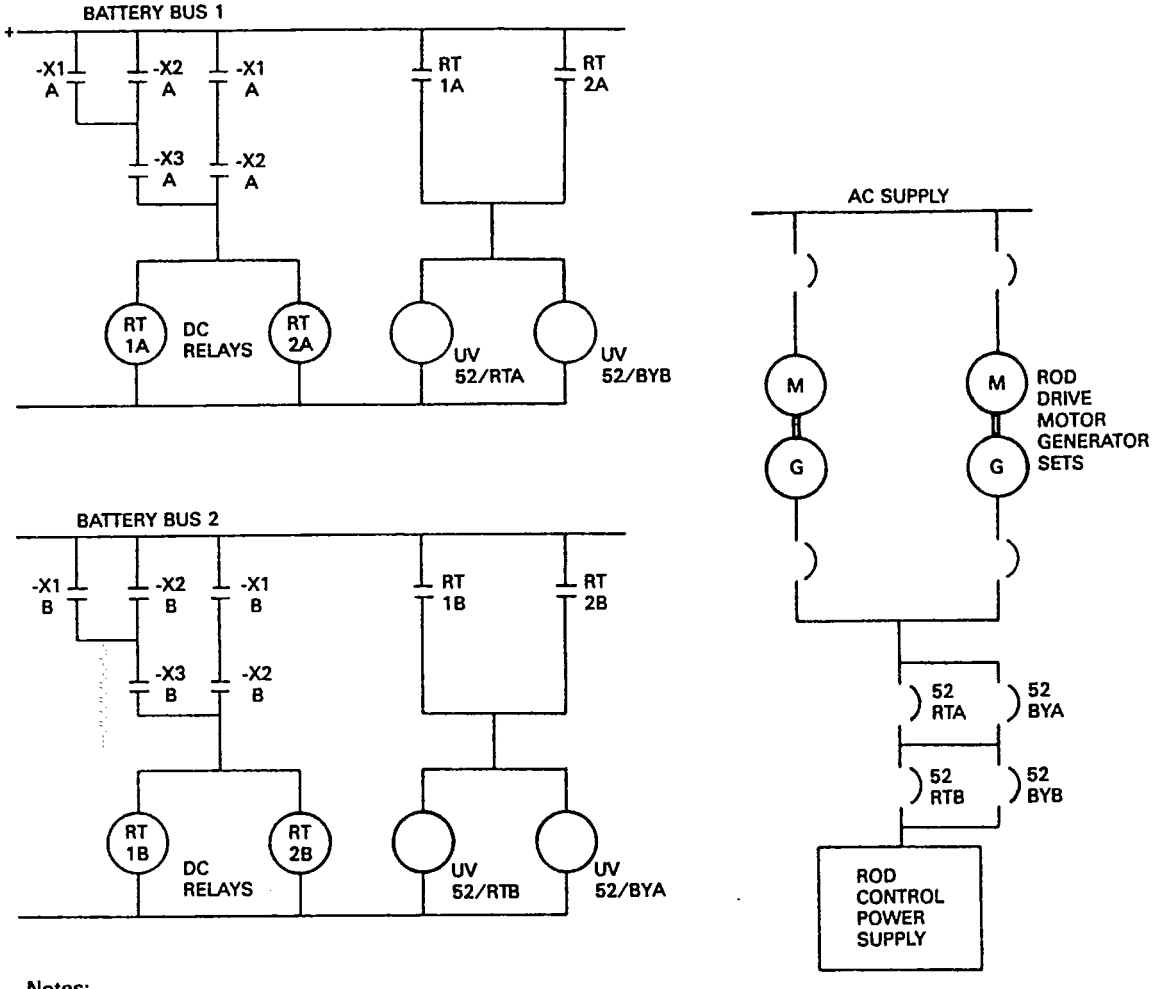


Fig 1
Schematic of a Typical Reactor Trip Function

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale



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 (*continued*)

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

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.

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

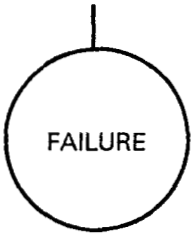
(5) It provides a systematic basis for progressing to a quantitative analysis

(6) It provides consistent and clear documentation of the consideration of failure characteristics in the design process

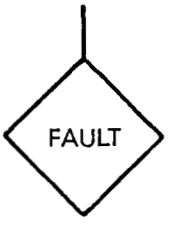
(7) It provides a basis for identifying multiple failures and common-cause failure mechanisms for the system

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.



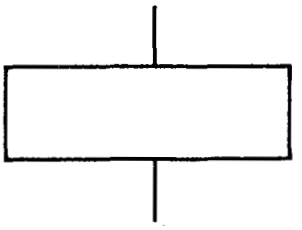
(2) *Diamond.* The diamond represents a fault event that is assumed to be basic in a given fault tree. This event could be divided further to show how it can result from more basic failures, but is not developed because of lack of significance in such a fault, lack of sufficient details to develop it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



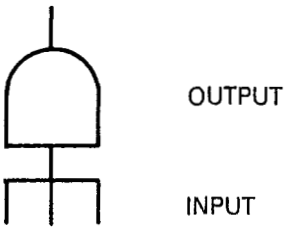
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

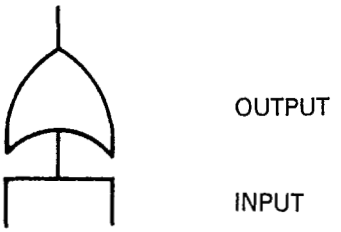
(3) *Rectangle.* The rectangle represents an intermediate event that results from the combination of events of the types described above through the input of a logic gate.



(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.



TRANSFER-OUT

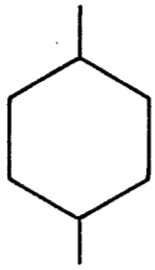


TRANSFER-IN

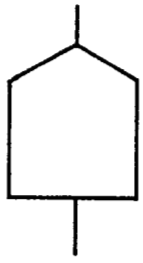
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

(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 subbranch of a tree occurs when the event being considered is a fundamental event

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

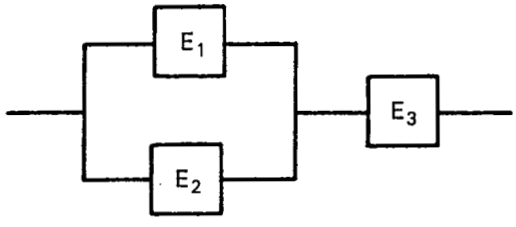
(basic fault) or when a transfer gate can be used for another subtree already developed.

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.

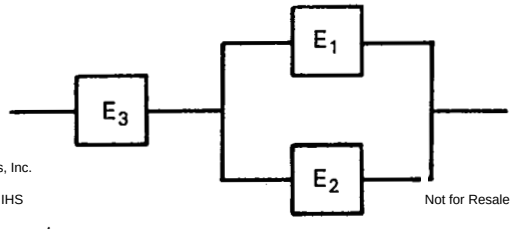
4.3 Reliability Block Diagram. The reliability block diagram (RBD) is a success-oriented diagram that represents the logic of a system. Reliability block diagrams are developed through analysis of the functional relationships among items shown by functional block diagrams and circuit schematics. The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



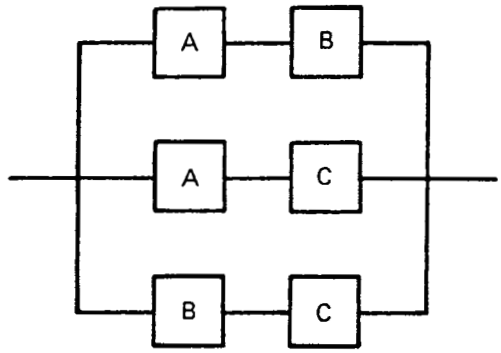
If either path is good, that is, made up of unfailed components, the system is good or successful.

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



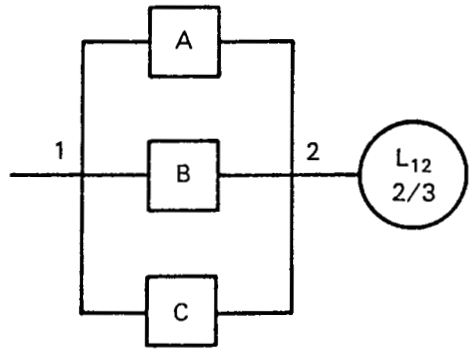
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

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

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

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

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

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

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

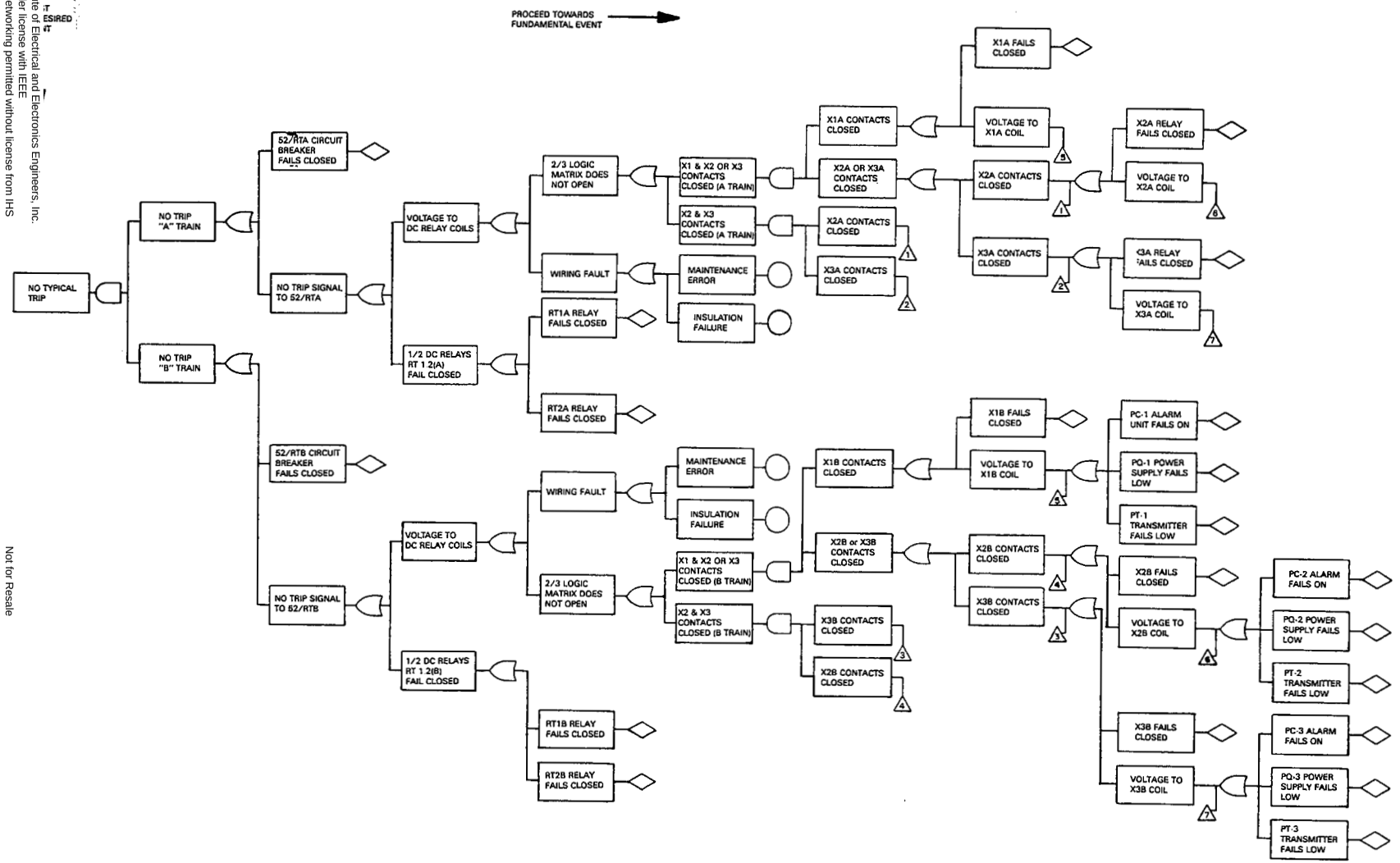


Fig 2
Fault Tree for a Typical Trip Function

352-87 4805702 0008168 1

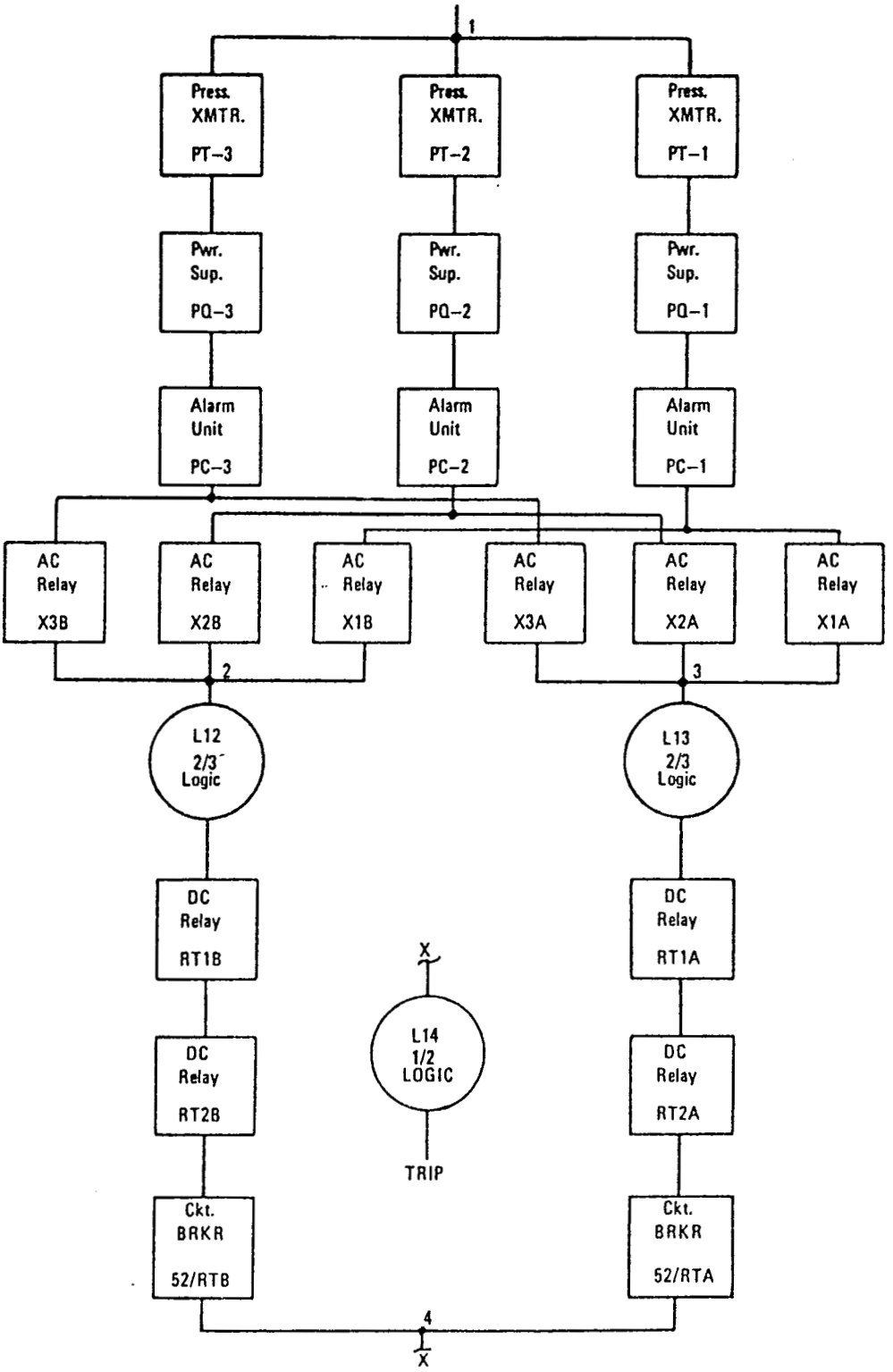


Fig 3
Reliability Block Diagram of a Typical Trip Function

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

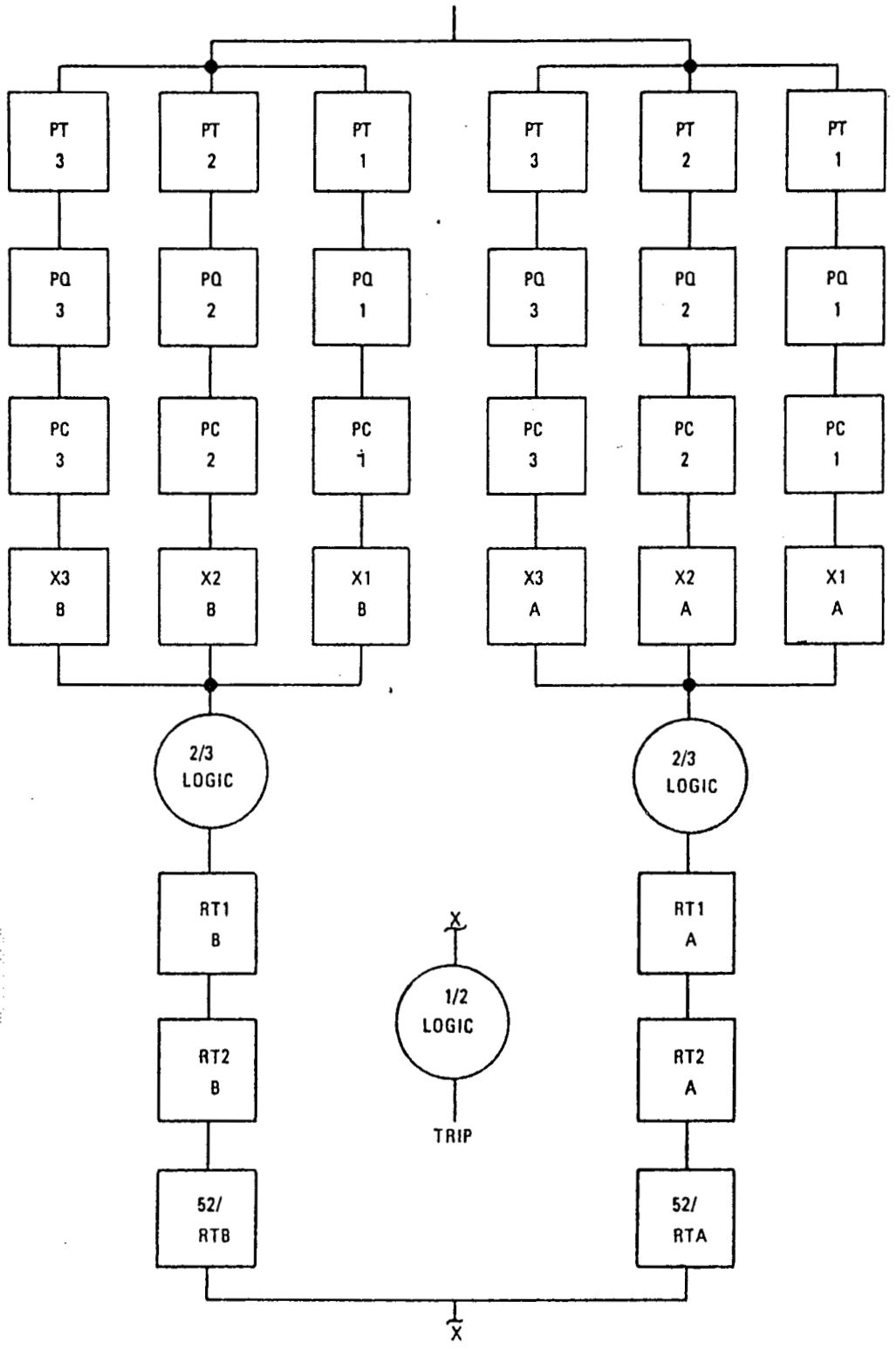


Fig 4
Alternative Reliability Block Diagram of a Typical Trip Function

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

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.

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 undesireable 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.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

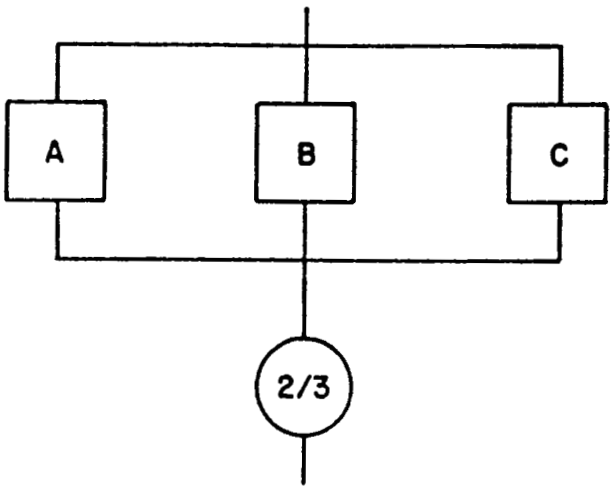


Fig 5
Basic 2-Out-of-3 (2/3) System

(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

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

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

$$R(t_m) = \exp -\int_0^{t_m} \lambda(t)\,dt \qquad \text{(Eq 1)}$$

where

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

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

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

$$R(t_m) = \exp(-\lambda t_m) \qquad \text{(Eq 2)}$$

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:

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

For small values of the product λt,

$$R(t) \cong 1 - \lambda t \qquad \text{(Eq 3)}$$

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,

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

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.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

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

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

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

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

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

and, thus Eq 5 reduces to

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

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:

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

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

$$\text{Availability} = \frac{1 - e^{-\lambda T}}{\lambda T}$$

If the series expansion of the numerator is carried out to the second-order term, the approximate result of Eq 6 is obtained.

Equation 7 is applicable to either a component or a system. For a system, it may be necessary to use the mathematical techniques of Section 5.2 to derive $R(t)$ from the failure rates or probabilities of the components in the system.

Alternative expressions for availability can be derived by other techniques. Section 5.2.2.1 shows the expressions derived by Markov modeling.

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, although the same principles are applied.

5.2.1 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. This means that the system operates successfully if at least two of the three channels operate. 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:

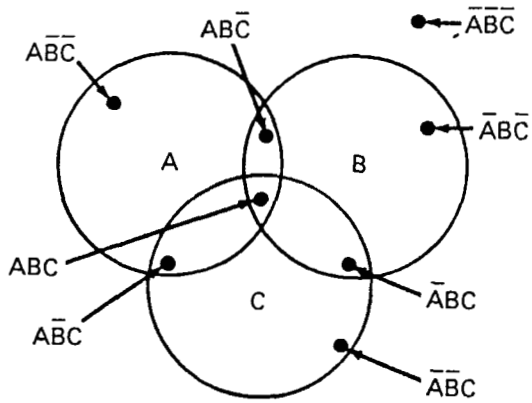
	A	B	C	System	Term
(0)	0	0	0	0	$\bar{A}\,\bar{B}\,\bar{C}$
(1)	0	0	1	0	$\bar{A}\,\bar{B}\,C$
(2)	0	1	0	0	$\bar{A}\,B\,\bar{C}$
(3)	0	1	1	1	$\bar{A}\,B\,C$
(4)	1	0	0	0	$A\,\bar{B}\,\bar{C}$
(5)	1	0	1	1	$A\,\bar{B}\,C$
(6)	1	1	0	1	$A\,B\,\bar{C}$
(7)	1	1	1	1	$A\,B\,C$

where a 1 represents the successful operation of the component, and a 0 represents the failure of the component to operate. The success of component A is denoted by A, and $\bar{A}$ denotes its complement, the failure of A. The system fails if two or more

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

channels fail, so success or failure can be determined for each line in the truth table. Furthermore, each term in the truth table is mutually exclusive of all other terms as is illustrated in the following Venn diagram:



Thus the success probability is equal to the sum of the probabilities of entries (3), (5), (6), and (7) of the truth table:

$$\text{System } P(S) = P(\bar{A}BC) + P(A\bar{B}C) + P(AB\bar{C}) + P(ABC) \qquad \text{(Eq 8)}$$

Suppose now that the three events in each of these probabilities are statistically independent. That is, suppose the probability of one component failing is unaffected by whether the other two components failed or not. Then, for example, $P(\bar{A}\bar{B}C) = P(\bar{A})P(\bar{B})P(C)$, and similar equations hold for the other terms. For example, suppose $P(\bar{A}) = P(\bar{B}) = P(\bar{C}) = 0.01$, so that $P(A) = P(B) = P(C) = 0.99$. Then the probability of system failure is

$$P(F) = (0.01)\ (0.01)\ (0.01) + (0.01)\ (0.01)\ (0.99) + (0.01)\ (0.99)\ (0.01)$$
$$+ (0.99)\ (0.01)\ (0.01) = 0.000298$$

The system reliability is $1 - P(F) = 0.999702$.

This demonstrates a typical characteristic of such calculations—that it is usually more practical to calculate failure probabilities than success probabilities because of the number of digits that may have to be carried. It is important, however, to design for success, and this section will stress success.

The truth table, though very convenient for simple systems, generates so many terms for a complex system that it is cumbersome to use. It may be more convenient in some situations to use Boolean algebra to solve reliability problems. The technique that will be illustrated here is how to manipulate the Boolean expression into a series of mutually exclusive terms[4] so that the probability equation may be written directly.

---

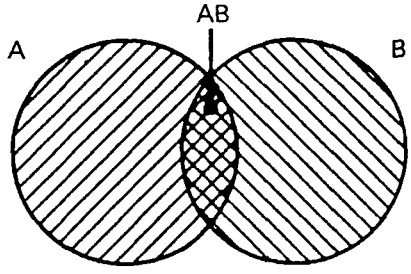
[4] The terms will then represent events such that the occurrence of one precludes the occurrence of ev are *mutually exclusive.*

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

First, a few simple ideas from Boolean algebra will be illustrated by the Venn diagram. Let success be defined as

$$S = A + B \qquad \text{(Eq 9)}$$

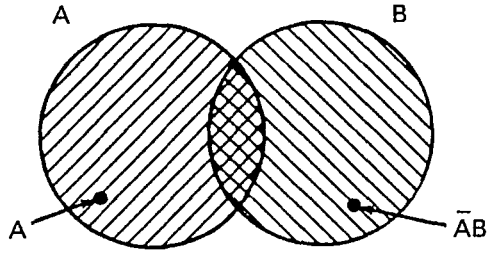
The plus sign is the Boolean notation for the union of events, called the OR function, meaning the event "success" is equivalent to the event A OR B. The total shaded area of the Venn diagram may be used to represent S thus:



The double shaded area is designated "AB," which means "A AND B," and is called the intersection of A and B. If "$\bar{A}$" is the shaded area within the circle A, "$\bar{A}$" or "not A" is the area outside circle A. A new success equation can be written

$$S = A + \bar{A}B \qquad \text{(Eq 10)}$$

represented by the Venn diagram:



where the double shaded area is eliminated because the intersection $\bar{A}B$ does not include any part of A. Equation 10 is now in mutually exclusive form and the probability of success can be written directly as

$$P(S) = P(A) + P(\bar{A})\,P(B) \qquad \text{(Eq 11)}$$

Note that $S, A, \bar{A}$, etc, are used to describe events and are not numeric. $P(S), P(A), P(\bar{A})$, etc, are used to describe the probability of an event, and are numerical quantities.

The probability equation can be written directly from the Boolean expression only when all the terms of the Boolean expression are mutually exclusive. This expression is not necessarily unique. For example, S could also be expressed as $S = B + A\bar{B}$.

One Boolean method will be illustrated using the same 2-out-of-3 (2/3) logic problem used in the truth table derivation. In a 2-out-of-3 (2/3) system, if any two

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

components are good, the system is good. Consequently, if any two channels fail, the system fails. In Boolean algebra, the event "success" is described as

$$S = AB + AC + BC \quad \text{(Eq 12)}$$

meaning that the event S is equivalent to the joint events A AND B OR A AND C OR B AND C. Although this is a valid and succinct expression for success, it must be manipulated into mutually exclusive form before the probability expression can be written directly. In order to do this, first break the expression into two terms with parentheses:

$$S = AB + (AC + BC) \quad \text{(Eq 13)}$$

Now, without changing the meaning of the expression, the terms in the parentheses are intersected with the negation of the first term, as was done to make Eq 9 equal Eq 10. Thus

$$S = AB + \bar{A}\bar{B}\,(AC + BC) \quad \text{(Eq 14)}$$

where $\bar{A}\bar{B}$ means not "A AND B." This operation is performed to assure that no event already contained in AB is allowed to remain in the balance of the equation.

Similarly, the two terms inside the parentheses can be treated in exactly the same way without changing the value of the expression:

$$S = AB + \bar{A}\bar{B}\,(AC + \bar{A}\bar{C}\,(BC)) \quad \text{(Eq 15)}$$

Of all the rules of Boolean algebra, only three, plus de Morgan's theorem, are needed to treat this problem:

$AA = A$

$A\bar{A} = \Phi$ = null set (NOTE: $P(\Phi) = 0$)

$A + A = A$

$\overline{AB \cdots N} = \bar{A} + \bar{B} + \cdots \bar{N}$ (de Morgan's theorem)

$= \bar{A} + A\bar{B} + AB\bar{C} + \cdots + ABC \cdots (N-1)\bar{N}$ (mutually exclusive form)

By using these rules of Boolean algebra it can be shown that

$$\bar{A}\bar{B} = \bar{A} + \bar{B} = \bar{A} + A\bar{B} \quad \text{(Eq 16)}$$

and

$$\bar{A}\bar{C} = \bar{A} + \bar{C} = \bar{A} + A\bar{C} \quad \text{(Eq 17)}$$

Substituting Eqs 16 and 17 in 15 gives

$$S = AB + (\bar{A} + A\bar{B})\,(AC + (\bar{A} + A\bar{C})\,(BC)) \quad \text{(Eq 18)}$$

and clearing from the innermost parentheses gives

$$S = AB + (\bar{A} + A\bar{B})\,(AC + \bar{A}BC) \quad \text{(Eq 19)}$$

since $CC = 0$. Further clearing leaves

$$S = AB + \bar{A}BC + A\bar{B}C \quad \text{(Eq 20)}$$

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

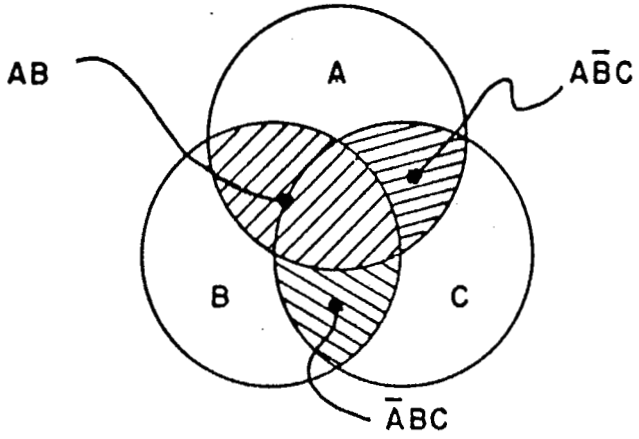


Fig 6
Venn Diagram for Basic (2/3) System

The events AB, $\bar{A}BC$, and $A\bar{B}C$ are mutually exclusive as a result of the foregoing manipulation. This is apparent from the Venn diagram of Fig 6, which identifies all the areas wherein two events intersect, but no area is overlapped. Therefore, the probability of failure is the sum of the joint probabilities

$$P(S) = P(AB) + P(\bar{A}BC) + P(A\bar{B}C) \quad \text{(Eq 21)}$$

$$P(S) = P(A)P(B) + P(\bar{A})P(B)P(C) + P(A)P(\bar{B})P(C) \quad \text{(Eq 22)}$$

Numerically, if $P(A) = P(B) = P(C) = 0.99$, then

$$P(S) = (0.99)\ (0.99) + (0.01)\ (0.99)\ (0.99) + (0.99)\ (0.01)\ (0.99)$$

$$P(S) = 0.999702$$

Note that the term ABC could have been included in Eq 12 as a success condition, and would have been eliminated in Eq 14. It is usually apparent by inspection that such terms are not mutually exclusive.

This method may be further illustrated in the following example. Consider a 3-out-of-4 (3/4) logic configuration. Success is defined as "any three of the four components are good."

(1) Write the Boolean expression that is the union of all possible success paths, utilizing the minimum number of variables in each term:

$$S = ABC + ABD + ACD + BCD \quad \text{(Eq 23)}$$

(2) Insert in parentheses all terms except the first term as follows:

$$S = ABC + (ABD + ACD + BCD) \quad \text{(Eq 24)}$$

(3) Intersect the negation of the first term with the term within the parentheses:

$$S = ABC + \bar{A}\bar{B}\bar{C}\ (ABD + ACD + BCD) \quad \text{(Eq 25)}$$

(4) Continue similarly with the terms inside the parentheses until only a single term is contained within the innermost parentheses:

$$S = ABC + \bar{A}\bar{B}\bar{C}\ (ABD + \bar{A}\bar{B}\bar{D}\ (ACD + \bar{A}\bar{C}\bar{D}\ (BCD))) \quad \text{(Eq 26)}$$

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

(5) Express each negated success as the union of mutually exclusive events by using de Morgan's theorem expressed in mutually exclusive form

$$\overline{AB \cdots N} = \bar{A} + A\bar{B} + AB\bar{C} + \cdots + ABC \cdots \bar{N},$$

as follows:

$$S = ABC + (\bar{A} + A\bar{B} + AB\bar{C})\ (ABD + (\bar{A} + A\bar{B} + AB\bar{D})\ (ACD + (\bar{A} + A\bar{C} + AC\bar{D})\ (BCD))) \quad \text{(Eq 27)}$$

(6) Starting with the innermost parentheses, clear the expression using the relationships $A\bar{A} = 0$, $A + A = A$, and $AA = A$, as follows:

$$S = ABC + (\bar{A} + A\bar{B} + AB\bar{C})\ (ABD + (\bar{A} + A\bar{B} + AB\bar{D})\ (ACD + (\bar{A}BCD)) \quad \text{(Eq 28)}$$

$$S = ABC + (\bar{A} + A\bar{B} + AB\bar{C})\ (ABD + \bar{A}BCD + A\bar{B}CD) \quad \text{(Eq 29)}$$

$$S = ABC + \bar{A}BCD + A\bar{B}CD + AB\bar{C}D \quad \text{(Eq 30)}$$

(7) The probability of success is equal to the sum of the probabilities of the mutually exclusive events:

$$P(S) = P(ABC) + P(\bar{A}BCD) + P(A\bar{B}CD) + P(ABCD) \quad \text{(Eq 31)}$$

The preceding example dealt with a Boolean success equation. Alternatively, a Boolean failure equation could have been used. The 2-out-of-3 system treated earlier in this section has symmetry (the system succeeds if at least 2-out-of-3 components succeed; it fails if at least 2-out-of-3 components fail), so exactly the same analysis could have been carried out interchanging the roles of success and failure. Thus,

$$F = \bar{A}\bar{B} + \bar{A}\bar{C} + \bar{B}\bar{C}$$

and after reexpression in terms of mutually exclusive events becomes

$$F = \bar{A}\bar{B} + \bar{A}B\bar{C} + A\bar{B}\bar{C}$$

For the example numbers,

$$P(F) = (0.01)\ (0.01) + (0.99)\ (0.01)\ (0.01) + (0.01)\ (0.99)\ (0.01)$$
$$= 0.000298$$
$$= 1 - P(S)$$

Generally, the Boolean manipulation is easier for a failure equation than for a success equation because there will be more ways for a well-defined system to succeed than to fail. Also, if a fault tree is used, it leads naturally to a Boolean failure equation and therefore, that form has been illustrated here.

One reason for using a system failure equation is to check a system failure probability calculation. That is, if there is no rounding off, one can check that $P(S) + P(F) = 1.0$. The failure equation also has the advantage that, in the case of fairly reliable components, one can calculate an approximate system failure probability

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

from the original Boolean expression and not have to reexpress the equation in terms of mutually exclusive events. The error in the approximation will be conservative in that the system failure probability will be overstated. For the 2-out-of-3 system illustrated here,

$$P(F) \cong P(\bar{A}\bar{B}) + P(\bar{A}\bar{C}) + P(\bar{B}\bar{C})$$
$$= (0.01)\ (0.01) + (0.01)\ (0.01) + (0.01)\ (0.01)$$
$$= 0.0003$$

which is negligibly different from the exact result, $P(F) = 0.000298$.

To further illustrate these methods, consider the system shown in Fig 7.

The system succeeds if the 2-out-of-3 portion succeeds and if D or E succeeds. Thus

$$S = ABD + ACD + BCD + ABE + ACE + BCE \quad \text{(Eq 32)}$$

is the Boolean success equation for this system. By converting this relationship to one in terms of mutually exclusive events, one of the possible reexpressions yields

$$P(S) = P(ABD) + P(\bar{A}BCD) + P(\bar{A}BC\bar{D}E)$$
$$+ P(A\bar{B}CD)$$
$$+ P(A\bar{B}C\bar{D}E) + P(AB\bar{C}\bar{D}E) + P(ABC\bar{D}E) \quad \text{(Eq 33)}$$

Alternatively, a simpler solution is to take advantage of the fact that the 2/3 logic is independent of the 1/2 logic so that the Boolean success equation can be written

$$S = (AB + AC + BC)\ (D + E) \quad \text{(Eq 34)}$$

Now, since the first set of parentheses does not include any terms within the second set of parentheses, and vice versa, each set of parentheses only needs to be made mutually exclusive within itself; thus,

$$S = (AB + \bar{A}BC + A\bar{B}C)\ (D + \bar{D}E) \quad \text{(Eq 35)}$$

and

$$P(S) = P(ABD) + P(\bar{A}BCD) + P(AB\bar{D}E) + P(A\bar{B}CD)$$
$$+ P(\bar{A}BC\bar{D}E) + P(A\bar{B}C\bar{D}E) \quad \text{(Eq 36)}$$

Although this result appears to be different from Eq 33, it really is not, since there are many ways of describing the chosen area in a Venn diagram. They all yield the same numerical result. Substitution of the same numerical probabilities used in evaluating Eq 33 into Eq 36 yields the identical result.

Nevertheless, using the example of Fig 7, the Boolean failure expression is

$$F = \bar{D}\bar{E} + \bar{A}\bar{B} + \bar{A}\bar{C} + \bar{B}\bar{C} \quad \text{(Eq 37)}$$

The conversion to mutually exclusive form gives as a result

$$P(F) = P(\bar{D}\bar{E}) + P(\bar{A}\bar{B}D) + P(A\bar{B}\bar{C}D) + P(\bar{A}B\bar{C}D)$$
$$+ P(\bar{A}\bar{B}\bar{D}E) + P(A\bar{B}\bar{C}\bar{D}E) + P(\bar{A}B\bar{C}\bar{D}E) \quad \text{(Eq 38)}$$

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

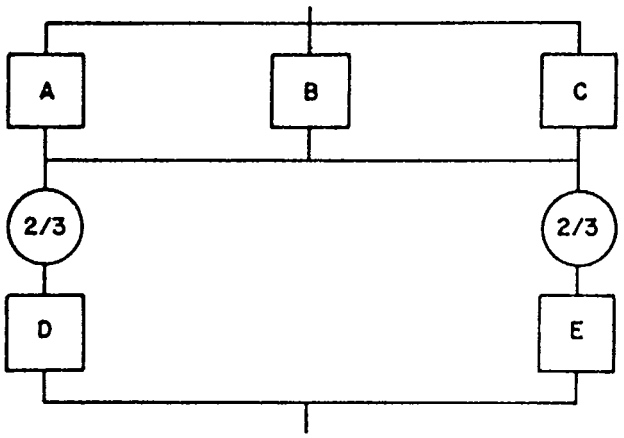


Fig 7
Reliability Block Diagram of a Simple 2/3 System

Although the end result is no less complicated, the manipulation generated fewer intermediate terms and is somewhat easier. In general, there is an advantage in calculating the probability of failure (assuming $P(F) \ll 1$) because less precision is demanded in the numerical solution to achieve a result with a given accuracy. Substitution of the same numerical probabilities used in evaluating Eq 33 yields $P(F) = 0.000299$.

As another example of manual calculation on another system model, consider Fig 8. This is the same as Fig 7 except that six additional components are introduced that are not uniquely paired with A or B or C. An exact solution to this problem by the Boolean method generates so many terms that it is exceedingly cumbersome, and in most cases the accuracy of the exact solution does not warrant the effort. An approximate method known as *minimal cut sets* is used as a basis for some computer solutions and is also useful for manual methods.

A *cut set* is a collection of components belonging to a model such that if all those components fail, then all success paths are interrupted. A *minimal cut set* is a unique set of failed components such that restoring any one of the set to operation restores a success path.

The manual calculation method is performed in the following manner. First, decide on an order of components, usually with the least redundant components first and the most redundant components last. For this case consider the components in the order $D, E, A, B, C, F, G, H, J, K, L$. Consider D failed, and then fail E. This qualifies as a minimal cut. Now restore E, fail A, and then fail B. The combination $\bar{D}\bar{A}\bar{B}$ does not constitute a minimal cut because restoring D does not restore a success path. The next valid minimal cut is $\bar{D}\bar{A}\bar{K}$ and $\bar{D}\bar{A}\bar{L}$. Then A is restored, and the next minimal cuts are $\bar{D}\bar{B}\bar{J}$ and $\bar{D}\bar{B}\bar{L}$, and so on. When all of the minimal cuts involving D are written, D is permanently restored, E is failed, and the chain is searched again.

Eventually there will be enough components permanently restored so that failure is not possible and the list is completed. It is relatively easy to write all the terms by inspection:

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

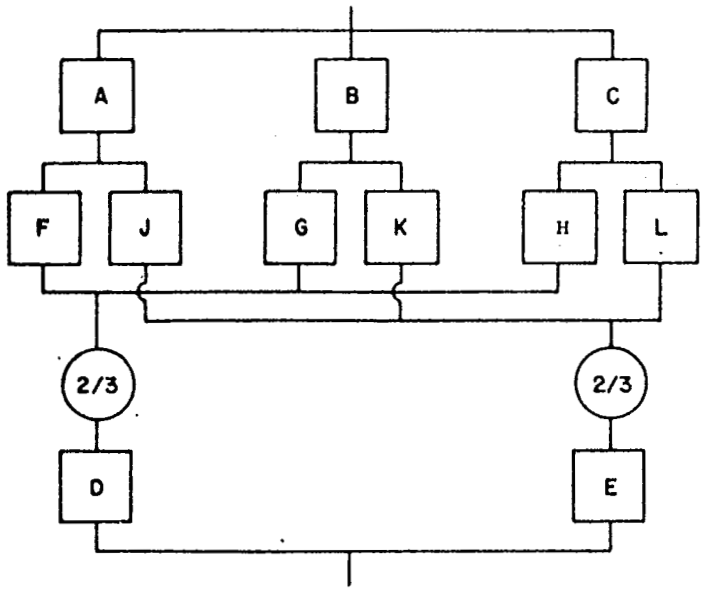


Fig 8
Improved Model of a 2/3 System

$$
\begin{aligned}
F = {} & \bar{D}[\bar{E} + \bar{A}(\bar{K} + \bar{L}) + \bar{B}(\bar{J} + \bar{L}) \\
& + \bar{C}(\bar{J} + \bar{K}) + \bar{J}(\bar{K} + \bar{L}) + \bar{K}\bar{L}] \\
& + \bar{E}[\bar{A}(\bar{G} + \bar{H}) + \bar{B}(\bar{F} + \bar{H}) + \bar{C}(\bar{F} + \bar{G}) \\
& + \bar{F}(\bar{G} + \bar{H}) + \bar{G}\bar{H}] \\
& + \bar{A}[\bar{B} + \bar{C} + \bar{G}(\bar{K} + \bar{L}) + \bar{H}(\bar{K} + \bar{L})] \\
& + \bar{B}[\bar{C} + \bar{F}(\bar{J} + \bar{L}) + \bar{H}(\bar{J} + \bar{L})] \\
& + \bar{C}[\bar{F}(\bar{J} + \bar{K}) + \bar{G}(\bar{J} + \bar{K})] \\
& + \bar{F}\ [\bar{G}\ (\bar{J}\bar{K} + \bar{J}\bar{L} + \bar{K}\bar{L}) + \bar{H}\ (\bar{J}\bar{K} + \bar{J}\bar{L} + \bar{K}\bar{L})] \\
& + \bar{G}\ [\bar{H}\ (\bar{J}\bar{K} + \bar{J}\bar{L} + \bar{K}\bar{L})]
\end{aligned}
\qquad \text{(Eq 39}
$$

To calculate $P(F)$ approximately, one simply inserts the probability for each item represented by an alphabetical symbol.

This method is described more fully in [21]. Note that some of the terms represent the product of two factors, such as $\bar{D}\bar{E}$, others three factors, such as $\bar{C}\bar{F}\bar{J}$, and still others as four factors such as $\bar{G}\bar{H}\bar{J}\bar{K}$. In numerical substitution, it may be reasonable to eliminate the four-factor terms as insignificant if the four events are independent and their probabilities are reasonably low.

The logical nature of the fault tree lends itself naturally to the direct writing of the Boolean expression for failure. Once obtained, this may be reduced by standard Boolean techniques to obtain a result suitable for numerical substitution. Fault tree models are very prolific in the generation of terms, and it may be necessary to apply good judgment in simplifying the model for manual calculation. Nevertheless, the

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

reliability model and the fault tree model yield identical results for the same input information, and they may be used interchangeably.

5.2.1.1 Numerical Substitution; Reliability Calculations. Once the mathematical model is obtained in a form similar to Eq 22, a numerical substitution must be made in order to obtain a numerical result. If the model represents the reliability of the system for mission time T, substitute for the reliability (probability of success) of a component:

$$R_n = \exp [-\lambda_n T]$$

and

$$\bar{R}_n = 1 - \exp [-\lambda_n T]$$

where $\bar{R}_n$ is the reliability of component n. For example,

$$P(A) = R_A = \exp [-\lambda_A T]$$

$$P(B) = R_B = \exp [-\lambda_B T]$$

$$P(C) = R_C = \exp [-\lambda_C T]$$

If $\lambda_n T \ll 0.1$, one may use the approximations $R_n = 1 - \lambda_n T$ and $R_n = \lambda_n T$ with negligible error.

One must be careful to avoid rounding off numbers near unity, or the true significance of the numerical result may be erroneous. For this reason, it is usually more desirable to calculate the probability of failure ($\ll 1.0$) than to calculate the probability of success.

5.2.1.2 Numerical Substitution; Availability Calculations. Numerical substitutions for availability model calculations fall into three general classifications, depending on the relative importance of the repair rate and test interval.

(1) If the mean time to repair is very short compared to the test interval, it may be reasonable to neglect the effect of the repair time, and an adequate approximation to the availability calculation is based solely on failure rates and test intervals. This condition may be characteristic of systems that are tested manually once every week or more and have modular construction that allows failed components to be replaced in a matter of minutes once the failure is detected.

In this case, substitute

$$A_n = 1 - \lambda_n (T/2)$$

and

$$\bar{A}_n = \lambda_n (T/2)$$

in the mathematical model for the availability of the system, where $(T/2)$ is one-half the average test interval. This numerical substitution yields a good approximation to the availability period $\lambda_n (T/2) \ll 1.0$.

(2) If the mean time to repair is very long compared to the test interval, the test interval may be neglected and the availability calculation based solely on the component failure rates and the repair rates. This condition may be characteristic of some systems that test automatically in a very short period.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

In this case, substitute

$$A_n = 1 - \lambda_n \tau_n$$

and

$$\bar{A}_n = \lambda_n \tau_n$$

in the mathematical model for availability, where τ_n is the mean time to repair (see 5.4.2). This substitution yields a good approximation provided $\lambda_n \tau_n \ll 1.0$ and the time to repair is exponentially distributed.

(3) If the mean time to repair and the test interval are the same general order of magnitude, accurate modeling for manual calculation becomes more difficult and is beyond the scope of treatment in this guide. Frequently, manual methods can be used to bound the results satisfactorily for purposes of estimation. Many of the computer programs referenced can adequately model this more difficult problem.

5.2.1.3 Common-Cause Failures. In the examples of 5.2.1, statistical independence of component failures and events was assumed. Often this assumption cannot be justified. For example, two components may be subject to the same environment simultaneously, and if this environment is degrading, both will have higher failure probabilities than under a more benign environment. As will be shown, this means the unconditional probabilities of each component failing cannot be multiplied to give the probability of both failing. In a given situation, there may be a variety of "common causes" that affect multiple components, and it is necessary that the mathematical model reflect this situation.

Let $C_1, C_2, \cdots, C_m$ be the common environments or conditions under which two components, A and B, operate. These conditions must be mutually exclusive (no two can be present at the same time) and exhaustive (no conditions are left out). Let $P(C_1), P(C_2), \cdots, P(C_m)$ be the probabilities of each of the conditions occurring. Suppose the event of interest is $\bar{A}\bar{B}$, both components failing, and let $P(\bar{A}\bar{B} \mid C_i)$ denote the conditional probability of that event, given the occurrence of condition C_i. Then the unconditional probability of $\bar{A}\bar{B}$ is

$$P(\bar{A}\bar{B}) = \sum_{i=1}^{m} P(\bar{A}\bar{B} \mid C_i)\, P(C_i) \qquad \text{(Eq 40)}$$

Similarly, the unconditional probabilities of failure of each component are given by

$$P(\bar{A}) = \sum_{i=1}^{m} P(\bar{A} \mid C_i)\, P(C_i)$$

and

$$P(\bar{B}) = \sum_{i=1}^{m} P(\bar{B} \mid C_i)\, P(C_i)$$

In general, $P(\bar{A}\bar{B})$ will not equal $P(\bar{A}) \cdot P(\bar{B})$, and in fact may exceed it substantially. Thus, it is important to recognize and properly model common-cause failures.

For numerical illustration, suppose there are just two causes, say, *normal environment*, C_1, and *abnormal environment*, C_2. Suppose

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

$$P(\bar{A} \mid C_1) = P(\bar{B} \mid C_1) = 0.01$$

$$P(\bar{A} \mid C_2) = P(\bar{B} \mid C_2) = 0.50$$

$$P(C_1) = 0.95$$

$$P(C_2) = 0.05$$

and suppose further that conditional to C_1 or C_2, $\bar{A}$ and $\bar{B}$ are statistically independent. Let system failure be the failure of both $\bar{A}$ and $\bar{B}$. Then

$$P(\bar{A}\bar{B} \mid C_1) = (0.01)\ (0.01) = 0.0001$$

$$P(\bar{A}\bar{B} \mid C_2) = (0.5)\ (0.5) = 0.25$$

so

$$P(F) = P(\bar{A}\bar{B}) = (0.0001)\ (0.95) + (0.25)\ (0.05) = 0.012595$$

Also,

$$P(\bar{A}) = P(\bar{B}) = 0.01\,(0.95) + 0.5\,(0.05) = 0.0345$$

Their product, which would give the desired probability under the assumption of independence, is

$$P(\bar{A}) \cdot P(\bar{B}) = (0.0345)\ (0.0345) = 0.00119025,$$

which is about a factor of ten less than the actual probability of both components failing.

The situation of common-cause failures is just one in which multiple component (or system) failures are nonindependent events. Another is *cascade failures*, described in the following section.

5.2.1.4 Other Dependent Failures. In some situations, failure of one item may increase the stress on another, thus altering its failure probability. This dependence needs to be modeled in much the same way as common-cause failures were in the previous section. Suppose the sequence, or *cascade*, of failures of concern is $\bar{A}$, then $\bar{B}$, then $\bar{C}$. Then,

$$P(\bar{A}\bar{B}\bar{C}) = P(\bar{A}) \cdot P(\bar{B} \mid \bar{A}) \cdot P(\bar{C} \mid \bar{A}\bar{B})$$

where the last probability is the conditional probability of C failing, given the previous failures of $\bar{A}$ and $\bar{B}$. Depending on the stress introduced to C by these failures, this probability might be quite different from the unconditional probability of C failing. In some situations, cascade and common-cause failures may have to be considered simultaneously in order to have a realistic model.

5.2.2 For Computer Calculation. Several computer codes have been described in the references. To a large extent, the development of the model should anticipate the type of input required by the computer. For example, if a fault tree type of code is to be used, the model should be developed along the lines of the fault tree.

The code must be suited to the type of analysis required. The various codes have different abilities for dealing with reliability, availability test intervals, test schedules, and repair rates. The code capability must be commensurate with the desired result. Most codes yield approximate solutions and the residual error allowed in

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

the calculation is partly a function of allowable computer costs. Therefore, the analyst may choose to make a simplified manual calculation before using the computer in order to estimate the run time and cost.

The various types of reliability models available as computer codes are discussed in Section 7 and are described in detail in [7], [14], [18], [19], [35], [39], and [40].

Two types of models that have not been discussed are the Markov model and the Monte Carlo model. They are briefly introduced in the following sections.

5.2.2.1 Markov Models. Markov models are important mathematical tools that are particularly useful in the study of reliability. The basic concepts of a Markov model are those of the *state* of a system and *transitions* between such states. The system under consideration is said to occupy a certain *state* whenever it satisfies the conditions that define the state. The dynamic changes in the state of the system are referred to as state *transitions*. An excellent elementary introduction to Markov models is given in [17].

There are two basic classes of Markov models. The first is the class of discrete time models, or *Markov chain* models. The second is the class of continuous time models, or *Markov process* models. In reliability applications, the primary concern is with Markov process models since events such as the failure of a component or system can occur at any point in time. However, Markov chains have also been used to model certain systems such as standby safety systems since such systems are typically inspected at known fixed points in time (see [27]).

Any Markov model is defined by a set of probabilities p_{ij}, which define the probability of transition from any state i to any state j. In the case of a Markov chain, p_{ij} is the probability of transition from state i to state j during the time interval used to index the chain, such as the period of time between inspections of a standby safety system. In the case of a Markov process, p_{ij} is the probability that the system will undergo a transition from state i to state j in the time period t to $t+t$. The probabilities p_{ij} are usually arrayed in a matrix for ease in subsequent matrix manipulations.

Markov chains and processes derive their name from the so-called "Markov property," which requires, in effect, that the future behavior of the system depends only on present and not on past behavior. Thus, in the case of a Markov chain, the probability of a transition to state j depends only on state i, the present state, and not on the past history leading to state i.

The desired solution of a Markov model is the set of unconditional probabilities that the system is in each of the various possible states at any discrete time point (for the case of a Markov chain) or at any time t (in the case of a Markov process). These probabilities may be found by performing certain matrix multiplications in the case of a Markov chain, or by solving a certain set of differential equations in the case of a Markov process. For the many realistic reliability problems for which Markov models may be employed, the solution to the set of differential equations could be difficult to obtain. In such cases, it may be sufficient to do the calculation by considering only the "steady-state solution," which is obtained by taking the limit as t tends to infinity. That is, the transient behavior of the system is ignored. The practical basis for this decision is the fact that for most reliable systems the steady-state behavior is reached rather quickly in time and steady-state results provide rather good approximations.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

During certain conditions the limiting unconditional probabilities that the system is in each state do not depend on the initial starting conditions. Such a Markov model is said to be *ergodic*, or to have no *absorbing* states. A further discussion of this important class of models may be found in [24].

If the p_{ij} terms are all independent of time and depend only on constants and perhaps Δt, the Markov process is called *homogeneous*. For a homogeneous process, the resulting differential equations have constant coefficients, and the solutions are of the form $\exp(-\lambda t)$ or $t^n \exp(-\lambda t)$.

Example. In order to illustrate the use of Markov models in reliability analyses, consider the following example of a homogeneous Markov process. Consider a single system that can only be in either of two states, which we label "0" (up) or "1" (down) at any time t. Furthermore, suppose that repair is possible and that the failure rate λ and repair rate μ are known constants. Assuming that the Markov property holds, the transition probabilities p_{ij} are given by

$$p_{00} = 1 - \lambda \Delta t \qquad p_{01} = \lambda \Delta t$$

$$p_{10} = \mu \Delta t \qquad p_{11} = \mu \Delta t$$

which leads to the system of two differential equations given by

$$\frac{dp_0(t)}{dt} = -\lambda p_0(t) + \mu p_1(t), \; t > 0$$

$$\frac{dp_1(t)}{dt} = -\mu p_1(t) + \lambda p_0(t), \; t > 0$$

where $p_0(t)$ and $p_1(t)$ are the desired unconditional probabilities that the system is up or down, respectively, at time t. If we specify the initial condition that the system was up at time $t = 0$, that is, $p_0(0) = 1$, and using the fact that $p_0(t) + p_1(t) = 1$, the solution is easily computed to be

$$p_0(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} \exp\left[(-\lambda+\mu)t\right]$$

$$p_1(t) = \frac{\lambda}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} \exp\left[(-\lambda+\mu)t\right]$$

Also, the steady-state solution is easily seen to be

$$p_0 \equiv \lim_{t\to\infty} p_0(t) = \frac{\mu}{\lambda+\mu} = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}$$

$$p_1 \equiv \lim_{t\to\infty} p_1(t) = \frac{\lambda}{\lambda+\mu} = \frac{\text{MTTR}}{\text{MTTF} + \text{MTTR}}$$

It is noted that $p_0(t)$ is the availability of the system at time t and that p_0 is the steady-state availability. The expression for $p_0(t)$ is known as the "transient availability" of the system. Numerous additional illustrations of Markov models for solving reliability problems may be found in [37].

5.2.2.2 Monte Carlo Methods. Monte Carlo methods are so named because a random number generator, such as a roulette wheel, is used to determine the state

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

of components. In practice, a mathematical random number generator is used.

A Monte Carlo model of a system can take the form of a fault tree or any other format that relates the success or failure of the system to the success or failure of its components.

As a simplistic example, the mean time to failure (MTTF) of a complex system could be determined from the known reliability of its components by conducting repeated trial runs. In each run, the success or failure of the system is determined, hour by hour, by "spinning the roulette wheel" for each component until component failures cause the system to fail. The average of the times to failure for the different runs should converge to the mean time to failure if a sufficiently large number of runs is performed. The major drawback of the method has been that the large number of runs may be expensive and time-consuming, although the more recent computers may alleviate this. The references contain many methods for increasing the efficiency of the method, and detail the ways in which various probability distributions may be employed.

The major advantage of the method is that complex systems may be readily modeled and time constraints such as daily or weekly variations in output requirements and repair times may be included. It is also relatively easy to include distributions of parameters, such as a lognormal distribution of time to repair. Thus, the Monte Carlo method can be applied to systems that cannot be modeled in any other way, and is often combined with fault tree methods for this reason.

Examples of the use of Monte Carlo methods are given in [22].

5.2.2.3 GO Methodology. The GO method [18], [19], unlike fault tree analysis, is a success-oriented system analysis technique. Using an inductive logic to model system performance, the GO method determines system response modes, both successes and failures, and can treat man-machine interactions.

An advantage of the GO method is that a GO model can generally be constructed from engineering drawings by replacing elements (valves, switches, etc) with one or more GO symbols, which are combined to represent system function and logic. The GO computer code uses the GO model to evaluate system reliability and availability, identify fault sequences, and rank the relative importance of the constituent elements.

The GO symbols are operators that describe the operation, interaction, and combination of the physical equipment. The logic for combining the operators is contained as a set of algorithms in the GO computer code. The GO method lends itself readily to modularization, with small system models being combined into large system models by the computer code.

An advantage of the GO method is that it is easy to use the analysis as a continuing tool to estimate the effect of proposed system modifications, which can be as easily shown in the model as on the engineering schematics. A disadvantage is that the construction of the model does not require pessimistic seeking for failure possibilities and modes. Thus it is easy to overlook subtle failure possibilities. The GO method appears to be best suited to the analysis of systems for availability in which subtle interdependencies and very unlikely failure modes are of less importance than in risk analysis. The method does have the advantage of handling very large systems more efficiently than fault tree methods.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Table 2
Unavailability as a Function of Logic Configuration and Testing Schedule
(Adapted from Reference [20])

Logic	Unavailability	
	Simultaneous Testing	Perfectly Staggered Testing
1/2	$(1/3)\ (\lambda T)^2$	$(5/24)\ (\lambda T)^2$
2/2	λT	λT
1/3	$(1/4)\ (\lambda T)^3$	$(1/12)\ (\lambda T)^2$
2/3	$(\lambda T)^2$	$(2/3)\ (\lambda T)^2$
3/3	$(3/2)\ (\lambda T)$	$(3/2)\ (\lambda T)$
1/4	$(1/5)\ (\lambda T)^4$	$(251/7680)\ (\lambda T)^4$
2/4	$(\lambda T)^3$	$(3/8)\ (\lambda T)^3$
3/4	$(2)\ (\lambda T)^2$	$(11/8)\ (\lambda T)^2$
$(1/2) \cdot 2$*	$(2/3)\ (\lambda T)^2$	$(5/12)\ (\lambda T)^2$

*A special four-channel logic to satisfy the Boolean success expression, $S = (A + C)\ (B + D)$. This is an extension of the development in Reference [20].

5.3 Tabular Reference to Popular Logic Configurations. In the event that a system can be shown to meet the following criteria, Table 2 may be used to estimate the system unavailability. The criteria are as follows:

(1) The channels are the principal contributors to the system unavailability. (The balance of the system is designed, maintained, and tested in such a way that its unavailability contribution is negligible.)

(2) The various channels are identical and are expected to have identical failure rates.

(3) All safe failures reduce the logic to the next lower level of logic, which is safer, while the channel is being repaired. For example, a 2-out-of-3 logic is reduced to a 1-out-of-2 logic during repair.

(4) If an unsafe failure is discovered by the test at the beginning of a new test interval, the channel is either placed in its safe condition during repair as in (3), or the repair is completed in a time that is so short (compared to a test interval) that the contribution to unavailability due to repair is negligible.

(5) The test schedule is clearly identified as conforming to either the simultaneous or the perfectly staggered pattern.

The above criteria are not unduly restrictive and can frequently be met. Some designers may wish to consider the above criteria as an objective of good design.

If the above criteria are satisfied, the unavailability for several popular logic configurations may be estimated from Table 2. The failure rate λ is the failure rate of one complete channel. The test interval is T. The logic designation, 1/2, means

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

that one of the two channels is the minimum required for successful operation. Perfectly staggered testing is generally to be preferred to simultaneous testing because it leads to a lower unavailability for most logic configurations.

5.4 Trial Calculations. Once the mission is defined, the mathematical model generated, and the input parameters tabulated, a trial calculation may be performed to check out the manual procedure or the computer program. The following items should be monitored to reduce the chance of errors that might yield an erroneous result.

5.4.1 Manual Calculations

(1) If the assumption is made that λt is small compared to unity, check to see that it is, or provide a more exact mathematical model.

(2) If the procedure calls for calculating the reliability/availability, calculate the unreliability/unavailability by alternate means and see that they sum to unity with an insignificant error.

5.4.2 Computer Calculations. Use available techniques to establish that the computer is accepting the problem format and the data and producing results free of numerical errors.

5.5 Credibility Check of Results. The quantitative analysis is a tool of the designer, and it is imperative that the designer retain mastery over the tool and not vice versa. When the results are collected, the designer should review them critically for credibility. The techniques discussed in 5.5.1 through 5.5.3 are useful.

5.5.1 Comparison With Prior Analysis. If prior results on similar designs are available, they should be compared. In view of the differences in design and input data, is the difference in the result credible? Is the trend predictable? If the analysis identifies the principal contributors to failure, is this consistent with actual experience or best judgment? If the answer to any of these questions is "no," then the designer should reexamine his model and his data.

5.5.2 Sensitivity Analysis. A sensitivity analysis can be made to determine the relative importance of the various component failure rates, human error rates, test intervals, or repair times on the system's reliability/availability. In this way, the weakest elements in the system may be identified and reexamined for credibility.

5.5.2.1 Variable-Parameter—Wide Range Method. Vary the value of one key parameter over a wide range, noting the change in the systems unreliability/unavailability. A simple plot, usually on log-log paper, will show the range of values wherein a component is a major contributor to system unreliability/unavailability.

Example. Consider the model of a 2/3 system shown in Fig 8. Due to symmetry, A, B, and C are identical components and are expected to have the same failure rate. Similarly, D and E are identical, and F through L are identical. In this type of sensitivity study it is appropriate to consider all identical components as a group and vary their failure rates together. Let

$$P(\bar{A}) = P(\bar{B}) = P(\bar{C}) = \bar{X}$$

$$P(\bar{F}) = P(\bar{G}) = P(\bar{H}) = P(\bar{J}) = P(\bar{K}) = P(\bar{L}) = \bar{Y}$$

$$P(\bar{D}) = P(\bar{E}) = \bar{Z}$$

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

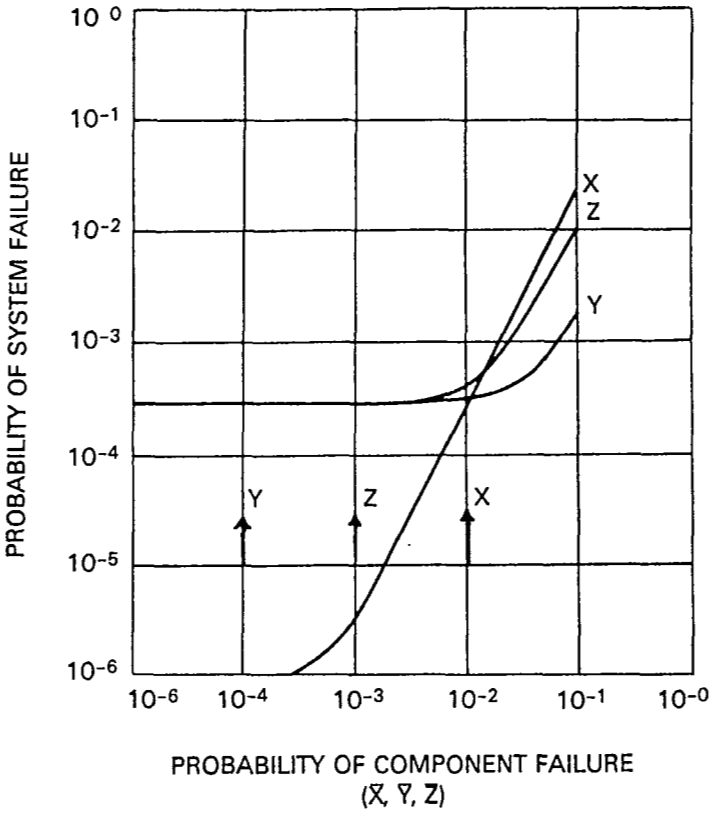


Fig 9
Sensitivity Study on Model of Fig 8

Making the above substitutions in Eq 39, which was derived by the minimal cut sets method for the reliability model of Fig 8, one obtains the probability of failures as

$$P(F) = \bar{Z}^2 + 6\bar{Z}(2\bar{X}\bar{Y} + \bar{Y}^2) + 3\bar{X}^2 + 12\bar{X}\bar{Y}^2 + 9\bar{Y}^4$$

For the purposes of this example, assume that the reference (expected) values are

$$\bar{X} = 0.01$$

$$\bar{Y} = 0.0001$$

$$\bar{Z} = 0.001$$

Fixing $\bar{Y}$ and $\bar{Z}$ at their reference values, compute $P(F)$ for the system as a function of $\bar{X}$ for a wide enough range of values to encompass the uncertainty in this reference value. This result is plotted as curve x in Fig 9. Repeat this procedure with $\bar{Y}$ and $\bar{Z}$ as the independent variables and plot curves $\bar{y}$ and $\bar{z}$.

The reference values of component probability of failure are indicated by arrows in Fig 9. Note that the reference value for $\bar{X}$ (A, B, and C) dominates the model. On the other hand, the reference values for $\bar{Y}$ and $\bar{Z}$ occur on the flat portion of their curves, indicating that components F through L and D and E have very little influence on the model. With this information, it is valid to represent the probability

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

of the failure of the system by the approximation

$P(\bar{F}) \cong 3\bar{X}^2$

5.5.2.2 Variable-Parameter—Narrow Range Method. This method involves calculating the system unreliability or unavailability for the reference values of the parameters. Then make a small percentage change in a given parameter, and another calculation of system unreliability or unavailability. The difference between these two results can be used as a sensitivity index provided the same percentage change is used each time.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

6. Guides for Data Acquisition and Use

Mathematical models of system reliability or unavailability, such as those described in the previous section, require numerical values for the various component failure probabilities and rates in order to assess the system reliability. Such numbers generally are not known with precision. However, if records have been kept on the components' past performance and if those data can be assumed to be applicable to present or future performance, then useful estimates may be obtainable. Obtaining estimates requires a knowledge of data sources and of the statistical methods by which estimates can be obtained. This section therefore addresses the following:

(1) Required input parameters
(2) Statistical methods for point and interval estimates of the failure rates or probabilities of components and systems
(3) Established data programs
(4) Development of field data programs
(5) Consideration for future data programs

6.1 Input Parameters. The number of input parameters required for reliability/availability analyses depends on the choice and sophistication of the mathematical model. Input parameters for the reliability model include failure rates, mission time, repair rates, test interval times, and surveillance test schedules.

The form of the input parameters will depend on the analyst's choice or model requirements. For example, failure information can be expressed in failure rates (number of failures per unit of time), as indicated above, or in MTBF (mean time between failures). Similarly, repair information can be expressed in repair rates (number of repairs per unit of time), or in MTTR (mean time to repair). However, for the purpose of this guide, failure rates and MTTR will be used.

6.1.1 Failure Rates. Any system is a collection of parts or components that are electrically or mechanically joined to perform a specific function. If a system can perform its function at some point in time, it will continue to perform that function until a change occurs in the operating characteristics of a part or group of parts. System failure can, therefore, be defined as having occurred when the operating characteristics, or a part or group of parts, change to the extent that the system can no longer satisfactorily perform its intended function.

It is evident that a key factor in making a system reliability analysis is in the selection of applicable part failure rates.

6.1.2 Mean Time to Repair. The mean time to repair (MTTR) parameter is primarily associated with the interface between the machine and human, or the

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

ease or speed with which a system or part can be kept in, or restored to, full functional operation. The MTTR parameter thus must reflect all aspects of the specific human-machine interface. Human performance and the effects of environmental, procedural, and personnel factors, referred to as performance shaping factors, should be considered, including the following:

(1) The physical and mental capabilities of those who are to operate and maintain the system
(2) The time required to identify and localize the failure
(3) The time required to isolate the part
(4) The disassembly time
(5) Availability of repair parts
(6) The interchange time
(7) The time to reassemble
(8) The alignment time
(9) Checkout time

In applying maintainability information to the mathematical model, the repair times may often be treated as constant or as being exponentially distributed. The desired depth of the analyses and sophistication of the model will determine the degree to which repair time information will affect the overall system availability results, as discussed in 5.2.1.2.

6.1.3 Mission Time. The mission time used in the system reliability analysis comes from the stated mission of the system and for nuclear power plants is usually bounded by major refueling outages or system test intervals. The mission time is measured in units compatible with the failure rate units such that the product of mission time and failure rate is dimensionless.

6.1.4 Test Interval. The test interval is the time from the start of one system test to the start of the next test of that system and is one parameter that can be readily adjusted to vary the predicted availability of a system.

Although this parameter may be adjusted to vary the predicted reliability/availability, the test interval should be subject to the following additional constraints:

(1) *Wearout.* Tests should not be so frequent that wearout is a dominant cause of failure.

(2) *Test Duration.* If the system is out of service while undergoing a test, then the tests should not be run too often, since the unavailability due to testing may become as high or higher than the unavailability due to undetected random failures.

(3) *Overriding Constraints.* A particular component may require exercise at regular intervals in order to keep it fit. For example, a machine may require operation periodically just to keep it adequately lubricated.

(4) *Fatigue.* There is no incentive to test for failures due to fatigue if all the fatigue is induced by the tests themselves. A system is not likely to be characterized solely by fatigue failures.

6.1.5 Test Schedule. The test schedule is used to designate the way in which redundant channels are tested during the test interval. If the channels are tested one immediately following another at the beginning of each test interval, this sched-

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

ule is known as *simultaneous*. If the tests are separated so that they divide one interval into equal times, the tests are *perfectly staggered* [9].

6.2 Probability Distributions, Parameters, and Estimation. In this section probability distributions associated with random variables, the parameters of those distributions, and estimation of the parameters are discussed.

The performance of an item, say its lifetime or its success or failure on demand, in general, will differ from the performance of other nominally identical items. The variability can be modeled by representing the performance characteristic, call it x, as a random variable. The variability of x is described by the function $F(x) = P(x \leq X)$, where X is a particular value of x. This function is called the *cumulative distribution function* of x. The derivative of $F(x)$, if it exists, is called the *probability density function* of x and is usually denoted $f(x)$. Thus,

$$f(x) = \frac{dF(x)}{dx}$$

and

$$F(x) = \int_{-\infty}^{x} f(s)\, ds$$

These relationships hold if x is a continuous random variable. If x is discrete, such as the number of failures in n tests, $F(x)$ is called the probability function of x and gives $P(x < X)$.

The analog of the probability density function for the discrete case is the cumulative distribution function, and is given by

$$F(X) = \sum_{x_i \leq X} F(x_i)$$

In general, the distribution function, and consequently the density function, involve one or more constants, which are called parameters. For example, if x is the probable lifetime of an item that has a constant failure rate λ, then x is exponentially distributed. That is, $F(x)$ is the exponential distribution characterized by a single parameter, λ. In most instances, the parameters of a distribution are not known. They must be estimated. The problem considered in this section is the estimation of parameters given data assumed to be a "random sample" from a distribution of a given functional form. In this subsection general estimation principles are discussed and then applied to illustrative probability distributions.

Suppose θ is the parameter of interest and suppose the data consist of n observations, $x_1, x_2, \cdots, x_n$. From the data, by applying certain statistical procedures, a point estimate or an interval estimate of θ can be calculated. A point estimate is a single value, usually chosen to satisfy a criterion such as unbiasedness. An estimate of θ is unbiased if its expected value is equal to θ. That is, if one could repeatedly obtain samples of size n and for each sample calculate the estimate of θ, then the average value of this estimate, over an infinite number of samples, would equal θ. Another desirable criterion for an estimate is that it have minimum variance—that is, that it vary less from sample to sample than any other estimate. Still another

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

criterion often used to obtain point estimates is maximum likelihood. The maximum likelihood estimate is that value that makes the probability of the observed data (called the likelihood function) a maximum.

A point estimate is the single value of θ most strongly suggested by the data according to some criterion. For example, if a coin is tossed 100 times yielding 52 heads, the point estimate of the probability of a head by most criteria is 0.52, but one cannot rule out the possibility that the coin and tossing methods are fair so that the true underlying probability of a head, call it θ, is 0.50. In general, for a given set of data, there will be a range of values that are consistent with the data, and within which one can be "confident" that θ lies. The statistical concept of confidence intervals provides a method for calculating these intervals and for quantifying the degree of confidence associated with an interval.

Let L and U be specific functions of the observed data, chosen such that in repeated sampling and repeated calculations of L and U, 95% of the time the interval L to U will contain θ. For the particular data observed, and the specific values of L and U obtained, one cannot know whether the observed interval is among the fortunate 95% or not. This uncertainty is conveyed by the statement that (L, U) is a 95% *confidence interval* on θ, which means it was calculated by a procedure that if repeated would capture θ 95% of the time.

Though the preceding discussion was in terms of 95% confidence, the confidence level can be specified at any one or many confidence levels. The usual notation used for the confidence level is $100(1 - \alpha)$%, and common used levels are 50%, 90%, 95%, and 99% (α = 0.5, 0.1, 0.05, and 0.01). The endpoints of the interval L and U are called the lower and upper confidence limits on θ, respectively. Conventionally, equal tail areas are usually selected so that, for example, L is a lower 95% confidence limit on θ, U is an upper 95% limit, and the interval between L and U is a 90% confidence interval on θ. In dealing with failure rates or failure probabilities, though, interest is usually in how large these parameters might be, so a one-sided confidence interval of the form $(0, U)$ would be used. U would be called the upper $100(1 - \alpha)$% confidence limit on θ and the interval $(0, U)$ would be called a one-sided $100(1 - \alpha)$% confidence interval on θ.

Confidence intervals tend to become narrower as the sample size increases. Thus they reflect the amount of data available for estimating θ, whereas point estimates do not. This feature can be one factor that influences the choice of a test program. Also, in doing sensitivity studies, as discussed in 5.6.2, confidence intervals provide guidance on what range of parameter values to explore.

6.2.1 Exponential Distribution. If it is assumed that the lifetime of a nonrepairable item is governed by a constant failure rate, then the random variable, the item's "lifetime," or "time until failure," has an exponential probability distribution. Similarly, if one assumes a constant failure rate for a repairable item and if the same failure rate applies after repair as before, the random variable, "time between failures," has an exponential distribution (6.4.2 describes data analyses that could lead to such an assumption). The exponential probability density function is

$$f(t) = \lambda \exp[-\lambda t] \qquad \text{(Eq 41)}$$

and applies only for $\lambda \geq 0$ and $t \geq 0$, where λ is the constant failure rate and t is

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

time. The cumulative distribution of time to failure (or time between failures, as the case may be) is

$$F(t) = 1 - \exp[-\lambda t] \qquad \text{(Eq 42)}$$

The component of $F(t)$, which is the reliability function because it gives the probability of not failing in the interval $(0, t)$, is

$$R(t) = \exp[-\lambda t]$$

Thus, the reliability of an item with exponentially distributed lifetimes is completely determined by the parameter.

The expected lifetime in an exponential distribution is $\theta = 1/\lambda$, which is often referred to as the MTTF, mean time to failure, or MTBF, mean time between failures, in the repairable case. Thus sometimes the exponential density function is written

$$f(t) = (1/\theta) \exp[-t/\theta]$$

Suppose that the available data are n observed lifetimes, $t_1, t_2 \cdots, t_n$. Then the maximum likelihood estimate of λ, denoted by $\hat{\lambda}$, is given by

$$\hat{\lambda} = n/T, \qquad \text{(Eq 43)}$$

where

$$T = \sum_{i=1}^{n} t_i$$

This same form applies to a variety of situations. For example, suppose n items are in use. Let t_i denote either a time to failure, if item i has failed, or a running time, if item i has not failed. Again, the total observed operating time is

$$T = \sum_{i=1}^{n} t_i$$

If in that collection of items r have failed, then

$$\hat{\lambda} = r/T$$

For the case of a repairable item, $t_1, t_2, \cdots, t_n$ would represent observed times between failure and the maximum likelihood estimate would again be

$$\hat{\lambda} = n/T \qquad \left(T = \sum_{i=1}^{n} t_i\right)$$

Alternatively, at the time the data are obtained, the individual interfailure times may not be available, but only the cumulated operating time of the item, say T^* time units, during which there have been n failures, where

$$\hat{\lambda} = n/T^* \qquad \text{(Eq 44)}$$

Thus, in general, the maximum likelihood estimate of λ is

$\hat{\lambda}$ = (number of failures)/(total running time)

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Confidence limits on λ depend on whether the total running time or the number of failures is the random variable. In the case of a fixed number, n, of lifetimes or times between failure, T is the random variable and $100(1 - \alpha)\%$ confidence intervals on λ are given by

$$\frac{\chi^2\,\alpha/2;2n}{2T} \leq \lambda \leq \frac{\chi^2\,1-\alpha/2;2n}{2T} \qquad \text{(Eq 45)}$$

where $\chi^2\,\alpha/2;2n$ is the $\alpha/2$ percentile of a chi-square distribution with $2n$ degrees of freedom. If the total running time T^* is fixed and the number of failures n is regarded as random, then a $100(1 - \alpha)\%$ confidence interval on λ is

$$\frac{\chi^2\,\alpha/2;2n}{2T^*} \leq \lambda \leq \frac{\chi^2\,1-\alpha/2;2n+2}{2T^*} \qquad \text{(Eq 46)}$$

Also, an upper $100(1 - \alpha)\%$ confidence limit on λ is given by

$$\lambda < \frac{\chi^2\,1-\alpha;2n+2}{2T^*}$$

This bound exists even in the case of zero failures and is given by

$$\lambda < -\frac{1n(\alpha)}{T^*} \qquad \text{(Eq 47)}$$

That is, the exponential distribution assumption and the knowledge that in T^* years, say, no failures have occurred permits an interval estimate of λ to be made.

In the situation where both the number of failures and the total running times are random variables, exact statistical confidence limits on λ are not obtainable. However, those based on T^* will provide a reasonable approximation.

An application of these results is given in [29]. From a tabulation obtained there, in 659 total reactor years of experience there had been one failure of a reactor scram system. Thus,

$$\hat{\lambda} = 1/659$$

$$= 1.5 \cdot 10^{-3} \text{ failures per reactor year}$$

In this case, the accumulated time, 659 reactor years is regarded as fixed, while the number of failures during that time is considered random; so, for example, the upper 99% confidence limit on λ is

$$\lambda_{99} = \frac{\chi^2\,4;0.99}{2T^*}$$

$$= \frac{13.3}{2(659)}$$

$$= 1.0 \cdot 10^{-2} \text{ failures per reactor year}$$

It should be stressed that the assumption under which these estimates are

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

obtained is that all reactor scram systems are governed by the same constant failure rate. This is quite a strong assumption, impossible to verify from the limited data available, so some caution in the use of such estimates is called for.

6.2.2 Poisson Distribution. The Poisson distribution, like the exponential, can be derived from the constant failure rate assumption. Consider a repairable item and the situation in which the repair time is negligible. Given a constant failure rate, the number of failures that occur in an interval of time $(0, t)$ is a random variable that has as its probability function the Poisson distribution. Under this distribution the probability of exactly r failures in time t is

$$f(r) = \frac{(\lambda t)^r e^{-\lambda t}}{r!}, r = 0, 1, \cdots \quad \text{(Eq 48)}$$

where λ is the failure rate.

The following example in which the reliability of a system is given directly by the Poisson distribution is given by Bazovsky [9]. Often it is not feasible or practical to operate components or units in parallel and "standby" arrangements must be applied; that is, when a component or unit is operating, one or more components or units are standing by to take over the operation if the first fails.

Standby arrangements normally require failure-sensing and switchover devices to put the next unit into operation. For this example it will be assumed that the sensing and switchover devices are absolutely reliable and that the operating component and the standby components have the same constant failure rate λ when operating. If one component is operating initially and $r - 1$ components are in standby, the system operates successfully for a mission of time t if $r - 1$ or fewer failures occur during that time. Thus

$$R(t) = P(\text{number of failures} \leq r - 1)$$

$$= \sum_{i=0}^{r=1} \frac{(\lambda T)^i e^{-\lambda t}}{i!} \quad \text{(Eq 49)}$$

Also, it should be apparent that the Poisson distribution provides the probability of r failures given a fixed cumulative running time of T^*, which is one of the situations discussed in the previous section. Thus, confidence intervals on λ given r failures over a fixed time of t time units are the same as in Eq 45, with t replacing T^* and r replacing n. The maximum likelihood estimate of λ is $\hat{\lambda} = r/t$.

6.2.3 Binomial Distribution. The binomial distribution is the probability distribution of the number of failures in n independent trials in which at each trial there are two possible outcomes—success or failure—and the failure probability; p is constant. This distribution is appropriate for situations in which an item is operated only "on demand," not continuously, and if the independence and constant p assumptions are appropriate. Under the binomial distribution, the probability of r failures in n trials is

$$f(r) = \binom{n}{r} p^r q^{n-r} \qquad r = 0, 1, \cdots, n \quad \text{(Eq 50)}$$

where

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

n = number of Bernoulli trials, or the number of demands to the item
r = number of failures
p = probability of failure, which is the same for each trial
q = $1 - p$
$\binom{n}{r}$ = number combinations of n things taken r at a time, and equals $\frac{n!}{r!(n-r)!}$

The binomial distribution provides an efficient way to calculate the reliability of a k-out-of-n system of identical components. Such a system succeeds if $n - k$ or fewer components fail. The probability of this event is

$$P(S) = \sum_{i=0}^{n-k} \binom{n}{i} p^i q^{n-i} \quad \text{(Eq 51)}$$

For the example of 5.2.1, a 2-out-of-3 system with $p = 0.01$,

$$P(S) = \binom{3}{0} (0.01)^0 (0.99)^3 + \binom{3}{1} (0.01)^1 (0.99)^2$$
$$= (0.99)^3 + (0.03)(0.99)^2$$
$$= 0.999702$$

The maximum likelihood estimate of p, also unbiased with minimum variance, is $\hat{p} = r/n$. For moderate to large n and small np, say $np < 5.0$, the binomial distribution can be adequately approximated by the Poisson distribution with λt replaced by np. Thus, approximate $100(1 - \alpha)\%$ confidence limits on p are given by

$$\frac{\chi^2\, \alpha/2; 2r}{2n} < p < \frac{\chi^2_1 - \alpha/2; 2r+2}{2n} \quad \text{(Eq 52)}$$

For np larger than 5.0, a normal approximation can be used:

$$\hat{p} - Z_{\alpha/2} \sqrt{\frac{\hat{p}(1-\hat{p})}{n}} < p < \hat{p} + Z_{\alpha/2} \sqrt{\frac{\hat{p}(1-\hat{p})}{n}} \quad \text{(Eq 53)}$$

where $Z_{\alpha/2}$ is the upper $\alpha/2$ percentile of the standard normal distribution. In the special case of zero failures, the upper $100(1 - \alpha)\%$ confidence limit on p is given exactly by $1 - (\alpha)^{1/n}$. Tables and computer programs are also available when given exact binomial confidence limits.

To illustrate, suppose a valve has failed 4 times in the last 10 000 demands and suppose the binomial assumptions are warranted. (This can be checked. For example, if it was found that the valve failed the first 4 times it was activated, never since, clearly the assumptions are suspect.) From these data, the maximum likelihood estimate is $p = 0.0004$ and the Poisson approximation yields an upper 95% confidence limit on p of

$$p \leq \frac{\chi^2\, 0.95; 10}{2(10\,000)}$$
$$= \frac{18.3}{20\,000}$$
$$= 0.0009$$

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

Suppose further that an event of interest is successful operation over the next 600 demands. This event has probability $(1-p)^{600}$. Substituting $\hat{p}$ for p yields a point estimate for this probability of 0.78 and substituting the upper confidence limit yields a lower 95% confidence limit of 0.58.

6.2.4 Weibull Distribution. One distribution often used as a model for the case of a nonconstant failure rate, termed the "hazard function," is the Weibull distribution. The Weibull hazard function is

$$h(t) = \frac{\beta}{\eta}\left(\frac{t-\nu}{\eta}\right)^{\beta-1} \quad \beta,\ \eta > 0,\ t \geq \nu \qquad \text{(Eq 54)}$$

If $\beta > 1$, $h(t)$ increases as t increases, while if $\beta < 1$, $h(t)$ decreases. The reliability function, from applying Eq 1 in 5.1.1 is

$$R(t) = \exp\left[-\left(\frac{t-\nu}{\eta}\right)^{\beta}\right] \qquad \text{(Eq 55)}$$

The three parameters of the Weibull distribution are referred to as the location parameter (ν), the scale parameter (η), and the shape parameter (β). The reader should be cautioned that different authors use different notation.

Note that if $\nu = 0$, $\beta = 1$, $\eta = 1/\nu$, the Weibull distribution reduces to the exponential distribution. In reliability applications, the minimum life, ν, is often assumed equal to zero. Estimation of the Weibull parameters is considerably more involved than for the exponential, Poisson, and binomial distributions. Maximum likelihood estimates must be obtained iteratively, but computer programs are available for obtaining these estimates. Another estimation method sometimes used is graphical [26]. Interval estimates of the parameters and of the reliability function can be obtained using the results of Bain [8]. Bush [11] gives an application of the Weibull distribution in estimating turbine failure probabilities.

6.2.5 Combining and Updating Data. A reliability analyst may be confronted with too much data, rather than too little, and must then combine data from different sources, or update a data set. Typical cases are those in which two different organizations have collected data on a class of components, but the two resulting sets are not equivalent, perhaps because of the number of observations involved, or perhaps one set has distributions while the other set has only point estimates. Another typical case is that in which a published data collection has a very large number of observations on generic components, say motors, while the plant being studied has a limited data collection on motors of a specific size. In either case, the data sets may be combined in many ways to achieve various purposes. A typical combination method is to adjust the magnitude of the distribution function of a large generic data set to conform to the mean (or perhaps median) of a smaller specific data set.

These problems may be treated in many ways, and a knowledge of the physical situation, the in-service testing program, and the operating and maintenance procedures should play a major role in the choice of data and handling of data. Whatever the method used, the logic and the results should be documented carefully to allow future modification as knowledge improves.

One systematic and defensible set of methods for combining and updating data sets are the Bayesian techniques, named after the work of the Reverend Thomas

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

Bayes in the 18th century. These techniques, discussed in [8], may be used to accomplish many desired ends in handling data, and are capable of thorough documentation. Further discussion is beyond the scope of this guide.

6.3 Established Data Programs. Of the many established reliability data banks or programs, most are within the United States, although some important ones are located in foreign countries. Established programs in the nonelectric utility industry tend to be of a specialized nature and are primarily concerned with military service and space application. The military and space application programs contain data related mostly to weapons, aerospace, and ground support component failure and performance evaluations.

At the present time, there is a shortage of directly usable data on human error and success in the nuclear industry. Work is continuing in an effort to identify or develop data sources. 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. References [12], [31], [32], and [33] are provided as a starting point for those who are incorporating the human factor into system reliability analysis.

A number of reliability data programs in the electric utility industry are in use in the US and in other countries. These programs contain data related mostly to equipment and events affecting unit performance or plant availability.

Some of the parts data are useful beyond these applications, and the use of these established data sources will benefit the analyst. One or more of these programs can provide a base or an order-of-magnitude range of failure data. A number of the more prominent data programs will be briefly discussed.

In general, each of the data programs provide sufficient failure rate back-up information to permit reasonable evaluations as to the suitability of the data for specific applications.

6.3.1 Failure Rate Data Program (FARADA). FARADA, jointly sponsored by the Army, Navy, Air Force, and NASA, comprises the collection, analysis, compilation, and distribution of failure rate and failure mode data. The program is currently under the sponsorship of the Government-Industry Data Exchange Program (GIDEP), described below.

6.3.2 Government-Industry Data Exchange Program (GIDEP). GIDEP is a cooperative activity between government and industry participants seeking to reduce or eliminate expenditures of time and money by making maximum use of existing knowledge. The program provides a means to exchange certain types of technical data essential in the research, design, development, production, and operational life-cycle phases of systems and equipment.

Participants in GIDEP are provided access to the four major data interchanges listed below. The proper utilization of the data associated with these interchanges can assist in the improvement of quality and reliability and reduce costs in the development and manufacture of complex systems and equipment. They are as follows:

(1) Engineering Data Interchange
(2) Metrology Data Interchange

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

(3) Reliability-Maintainability Data Interchange
(4) Failure Experience Data Interchange

Participation requirements or additional information about GIDEP may be obtained by contacting the GIDEP Operations Center.[5]

6.3.3 Nonelectric Parts Reliability Data (NPRD-1). The reliability information provided by this publication is described in [11]. The information, primarily from military and space applications, is provided in four sections as follows:

Section 1—Generic Level Failure Rate Data
Section 2—Detailed Part Failure Rate Data
Section 3—Part Data from Commercial Applications
Section 4—Failure Modes and Mechanisms

Additional information regarding this source of failure rate data can be obtained from the Reliability Analysis Center.[6]

6.3.4 Energy Technology Engineering Center (ETEC). Formerly called the Liquid Metal Engineering Center (LMEC), this test program is primarily concerned with equipment and parts used in liquid metals test and experimental reactor facilities. Provisions have been made, however, to allow for general nuclear reactor components to be integrated into the program. ETEC is operated by the Energy Systems Group of Rockwell International for the US Department of Energy.

Information on the now discontinued performance data collection program can be obtained from [25].

6.3.5 United Kingdom Atomic Energy Authority Data Program (UKAEA), National Center of Systems Reliability (SYREL). The UKAEA program is a comprehensive operating source of nuclear power reactor reliability data and general industrial data. The program information uses a data classification and coding format similar to that of the FARADA and GIDEP programs. The equipment service data for reactors come mostly from a long-standing equipment fault and incident reporting system used by UKAEA on approximately 900 components. The reliability data bank contains information on performance availability and generic reliability data, but contains data from industries other than nuclear power. Generic reliability data reports by category may be obtained by request from UKAEA.[7]

6.3.6 Nuclear Plant Reliability Data System (NPRDS). The American National Standards Institute Subcommittee N18-20 has developed and implemented the Nuclear Plant Reliability Data System (NPRDS). The NPRDS is designed to accumulate, store, and report failure statistics on systems and components in nuclear power plants related to nuclear safety.

The scope of reportable systems and components to NPRDS is, in general, limited to those classified as Safety Class 1 and Safety Class 2 in ANSI/ANS N51.1-1983 [1] and ANSI/ANS 52.1-1983 [2], which specify nuclear safety criteria for nuclear plant design and equipment designated as Electrical Class 1E in ANSI/IEEE Std

---

[5] Director, GIDEP Operations Center, Corona, CA 91720.

[6] Reliability Analysis Center, RADC/RBRAC, Griffiss Air Force Base, NY 13441.

[7] Systems Reliability Service (Data), UKAEA (SYREL), Wigshaw Lane, Culcheth, Warrington, Lancashire, WA3 4NE, United Kingdom.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

603-1980 [5]. The system, however, does not include all such equipment, and non-safety equipment data is often entered into the system at the discretion of the user.

Input information for the NPRDS is solicited from all organizations operating nuclear reactors used primarily for generating electric power within the US. The operating nuclear power plants licensed to operate prior to January 1967, and the La Crosse plant, were excluded from the program.

Four basic reports are used to input information to the NPRDS:

(1) Nuclear Unit Information Report, which provides general descriptive information about the nuclear unit, the owner-organization and the responsible utility contacts for use by NPRDS contractor.

(2) Report of Engineering Data, which provides specific engineering data for systems or components.

(3) Quarterly Operating Report, which provides the actual number of hours the reactor was in each of the three operating modes: critical, standby, and shutdown.

(4) Report of Failure, which provides detailed data on failures.

Eight basic output reports on system and component reliability are available to the industry:

(1) Quarterly Report of Engineering Data for Individual Reporting Organization (NPRD Report Q01), which supplies the reporting organization with a listing of all engineering data submitted for the quarter.

(2) Quarterly System and Component Failure Listing (NPRD Report Q02), which provides engineering and failure data for components reported as failed during the quarter.

(3) Quarterly Component Failure Listing (NPRD Report A01), which summarizes, by generic groups, similar component failures during the quarter.

(4) Annual Report of System Reliability (NPRD Report A02), which summarizes, by generic systems, operating statistics for safety-related systems.

(5) Annual Report of Cumulative Component Reliability (NPRD Report A03), which summarizes generic classification of operating statistics for components.

(6) Inventory Report of Similar Equipment in NPRD System Data Base (NPRD Report A04), which summarizes performance history each year of similar equipment.

(7) Annual Report of Systems Reliability for Individual Reporting Organizations (NPRD Report A05).

(8) Special Request Reports.

In addition to the routine NPRDS output reports described above, participating organizations may request special reports to be produced from the data base. These may be obtained at cost from the NPRD.[8]

6.3.7 Generating Availability Data System (GADS). GADS (formerly the Edison Electric Institute Equipment Availability Data System) operated by the National Electric Reliability Council (NERC) is primarily concerned with summary performance data on all types of electric power generating equipment. The data system is the primary electric utility industry source for the collection, processing, analyzing, and reporting of power plant outages and overall performance. The data

[8] NPRD Project Manager, INPO, 1100 Circle 75 Parkway, Atlanta, GA 30339.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

system provides statistics on outage availability and maintenance by unit size, arranged in tabular form and published in bound booklets. Additional information regarding this source of unit data can be obtained from the National Electric Reliability Council.[9]

6.3.8 Licensee Event Report. The report, prepared by the US Nuclear Regulatory Commission, provides a source of data for qualitative assessment of off-normal event and cause descriptive in the nuclear industry. Monthly computer listings are issued that provide information on facility identification and location, description of events, significance of events, operating conditions component details, radioactivity/location, and detection/correction.

Additional information regarding this source of qualitative data or special computer listings may be obtained from the Nuclear Regulatory Commission.[10]

6.3.9 Operating Units Status Report (NUREG-0020) (the Gray Book). The report, prepared by the US Nuclear Regulatory Commission, provides, on a monthly basis, a source of data on all operating commercial nuclear power plants in the US. The report summarizes, by units, inspection status, reports received from licensees, average daily power levels (MWC), operating status, and unit shutdown or power reduction for each operating unit.

Additional information regarding this source of operating data may be obtained from National Technical Information Services.[11]

6.3.10 Reactor Safety Study, WASH-1400 (NUREG-75/014). The study, an assessment of accident risk in US commercial nuclear power plants prepared by the US Nuclear Regulatory Commission, provides information on the methodology of data collection, failure rate data, and system model development for risk analysis. The report is prepared in ten appendices, and appendices III and IV provide the data source with tabular failure rate at the component level.

Additional information regarding this data source may be obtained from National Technical Information Services.[12]

6.3.11 Failure Incident Report Review (FIRR). The FIRR, an activity that is a subcommittee of the American National Standards Institute (ANSI), reviews problem areas to determine the need for changes in standards or new standards. Narrative reports prepared by the subcommittee are typical technical discourses on areas of current industrial interest, with quantitative sections as required.

Additional information regarding this source of information may be obtained from the IEEE Standards Office.[13]

6.3.12 IEEE Survey of Industrial and Commercial Power Systems. The IEEE survey by the Industrial and Commercial Power Systems Committee is a report on

---

[9] National Electric Reliability Council, Research Park, Terhune Road, Princeton, NJ 08540.

[10] Licensee Operation Evaluation Branch, DTS, Office of Management and Program Analysis, US Nuclear Regulatory Commission, Washington, DC 20555.

[11] National Technical Information Services, US Department of Commerce, 5285 Port Royal Road, Springfield, VA 22151.

[12] See footnote 11.

[13] Institute of Electrical and Electronics Engineers, Inc, 345 E 47th Street, New York, NY, 10017-2394.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

the reliability survey of industrial plants of equipment failures reported by 30 companies covering 68 plants in 9 industries. The report is prepared in six parts, covering electrical equipment, cost of outages, loss causes, types of failures, and other supplemental data.

Additional information regarding this survey may be obtained from the Institute of Electrical and Electronics Engineers.[14]

6.3.13 Nuclear Power Experience Reports. This is a privately funded business of data collection, and dissemination to subscribers is on a monthly basis. The data are collected from the many existing sources of operating experience information and formatted for filing in a multivolume, loose-leaf file system. Contents of reports provide summaries of data by experience, reactor, and so forth, concerning outages, defects, tests, and system descriptions in narrative, figure, and tabular form.

Additional information regarding this service may be obtained from Nuclear Power Experience, Inc.[15]

6.3.14 IEEE Nuclear Reliability Data Manual—ANSI/IEEE Std 500-1984 [3]. The manual offers a data base to be used for the performance of qualitative and quantitative systematic reliability analyses of nuclear power generating stations.

The reliability data presented include failure modes, failure rate ranges, and environmental factor information on generic components actually or potentially in use in nuclear power generating stations.

The data are given in ten chapters, with each data chapter dedicated to a major component area. Reliability data appears in the form of hourly and cyclic failure rates and failure mode information for over 1000 electrical, electronic, and sensing components. The data are arranged within each chapter in a hierarchical fashion by generic component type for easy data access. This approach gives data by section and subsection, including the applicable failure modes at each level. For each individual mode, low, recommended, high, and maximum failure rates are given.

Each chapter, devoted to a specific component type, contains the following information:

(1) A preface that describes unique characteristics or considerations of the specific component type, in addition to the hierarchical generic listing of component subtypes, failure mode matrix, and table of failure rate modifying factors to account for equipment environment.

(2) A tabular listing of component reliability data for applicable catastrophic, degraded, and incipient failure modes for each component type.

The listing includes failure rate ranges and recommended values for both cyclic and time dependent modes.

This data manual may be obtained from the IEEE Standards Office.[16]

---

[14] See footnote 13, p 79.

[15] Nuclear Power Experience, Inc (Data), PO Box 544, Encino, CA 91316.

[16] See footnote 13, p 79.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

6.4 Developing Field Data Programs. Field data programs are based on obtaining information by using various sampling techniques from the components of interest that are operated under known conditions. ANSI/IEEE Std 500-1984 [3] presents requirements for such programs in detail.

One technique is to simulate actual component operating conditions in a laboratory. This technique, if performed properly, can provide a good estimate of the expected component failure rate. In some cases, the results obtained by the simulation technique are more realistic than those obtained from actual field data gathered through an uncontrolled program. On the other hand, field failure data, if properly obtained through a controlled program, are considered superior to laboratory data because they represent actual operating conditions.

In selecting a sampling technique to use, the following factors should be considered and evaluated:

(1) The effort required to assure that the sample obtained reflects component failure experience in the field.

(2) The precision of estimates obtained from the sample data.

(3) The cost of obtaining the necessary data and related information.

When time, money, and other conditions permit, a combination of laboratory simulation and actual field experience techniques could be used.

Regardless of the sampling techniques used, certain information is required for a controlled data program. This basic information involves how failures are analyzed and how the corresponding failure rates are estimated. The statistical aspects of failure rate estimation are discussed in 6.1. Aspects of the practical problem are discussed herein.

6.4.1 Failure Analysis. The failure information input to the field data program is the most important portion of the data program. In order to provide adequate failure information, a comprehensive failure analysis and corrective action feedback system must be developed. This feedback information should answer the following questions:

(1) What failed?
(2) When did it fail?
(3) How did it fail? (mode)
(4) Why did it fail? (mechanism)
(5) What was the repair time and effect on plant operability?

A good failure record reporting system will have provisions for answering the first two questions. The last two may require additional information that can only be obtained from subsequent laboratory study of the failure condition. This will require a procedure that ensures that the laboratory information gets into the appropriate failure report. There are two general types of failure reporting systems: open loop and closed loop. *Open loop* is a system of reporting failures only. Subsequently, failure analysis may be performed to determine cause of failure. *Closed loop* is a system of reporting failures and keeping a status file of the reports. A reported failure is kept in the open status until corrective action is taken to close the file. The corrective action consists of the effort necessary to eliminate or to identify and accept the identified failure mode and mechanism.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Numerous failure reporting forms can be found in the reliability texts or handbooks in the references in 1.2. These reporting forms should contain, as a minimum, the following information:

(1) Time and date of failure
(2) Location
(3) Identification of components, module, etc
(4) Cause of failure, that is, identification of the failure mode and mechanism including any personnel error aspects (see Table 3)

Table 3
Some Typical Failure Modes and Mechanisms

Typical Modes of Failure	
Transistors	Intermittent High I_{CE} B-C Short Low BV_{EBO} High H_{FE}
Relays	Open or shorted (closed) contacts Open or shorted coils High contact resistance
Transformers	Open windings Shorted windings
Resistors	Open Short Drift
Capacitors	Short Open Leakage
Connectors	Misalignment Corrosion
Mechanical Systems	Corrosion Contamination Binding

Typical Mechanisms of Failure		
Adherence	Crosstalk	Noise
Arcing	Current overload	Piezoelectric effect
Backlash	Deterioration	Radiation damage
Bleeding	Dielectric breakdown	Secondary currents
Brinelling	Diffusion	Seizure
Carburization	Erosion	Silver migration
Composite behavior	Fatigue	Smearing
Contamination	Fretting or galling	Sputtering
Corona	Frequency effects	Sublimation
Corrosion	Leakage	Temperature shrinking
Creep	Magnetic hysteresis	Voltage breakdown
Creep rupture	Mass unbalance	Voltage overload
		Wear

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

(5) Operating time since last inspection and failure

(6) Other circumstances concerning the failure that would indicate if abnormal conditions had existed

The above, with the exception of item 4, are self-explanatory. This item, "cause of failure," is basic to proper failure reporting and is further explained.

When a component fails before the end of its expected lifetime, the underlying cause must be determined to ensure proper failure analysis. The cause of failures can be categorized into five areas:

(1) *Quality Defects.* Quality defects refer to those defects in the device that result from the manufacturing process. They are usually a function of assembly errors such as workmanship, improper assembly, or contamination. These defects can be partially avoided by quality control sampling and functional testing. However, both methods can allow "mavericks" to pass inspection. Sampling techniques allow the manufacturer to estimate the quality of his product; they do not necessarily eliminate all faulty components. Functional testing is of a much greater value in weeding out faulty components, but can have undesirable effects. As an example, burn-in techniques used to test high-reliability devices can force unrealistic failure modes, masking otherwise predominant modes. The advantage of accelerated testing methods lies in forcing early failures by accelerated stress. Since failure modes may be environment-dependent, accelerated testing at a more severe than expected temperature or other environmental parameter may cause an unrealistic failure mode to be dominant.

(2) *Design Faults.* Component design faults can result from the premature release of a design for fabrication. This error is difficult to control unless comprehensive testing is conducted before the assembly process.

(3) *Misuse.* Misuse is defined as: use of a device in environmental stresses beyond those intended; human errors, including improper installation operation, maintenance, and transportation; and use in a service never intended for the device. Misuse is hard to control since the human element is predominantly involved. Although this failure cause is hard to anticipate, failures usually show up early in the application.

(4) *Time/Environment Causes.* Time and normal environment-dependent failures are those more often termed "wear-out" failures. They are the result of progressive deterioration of the component due to stress and environment. In equipment that has been properly manufactured, handled, and applied, this is the fundamental cause of failures. Lifetime figures quoted by manufacturers are usually based on this failure cause.

(5) *Unknown Causes.* The phrase "unknown cause" is all too often abused and misapplied. As it becomes more difficult to pinpoint the cause of the failure and the mode and mechanism involved, it becomes much easier to cast away the problem with a "cause unknown." Properly used, unknown causes of failure are those that cannot be accurately determined from two or more suspected causes, due to the circumstances of the incident. This is particularly true in explosive-type incidents where the evidence is often destroyed. In a field data program these types of failures may be equally prorated to the other categories if they are a small percentage of the total.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

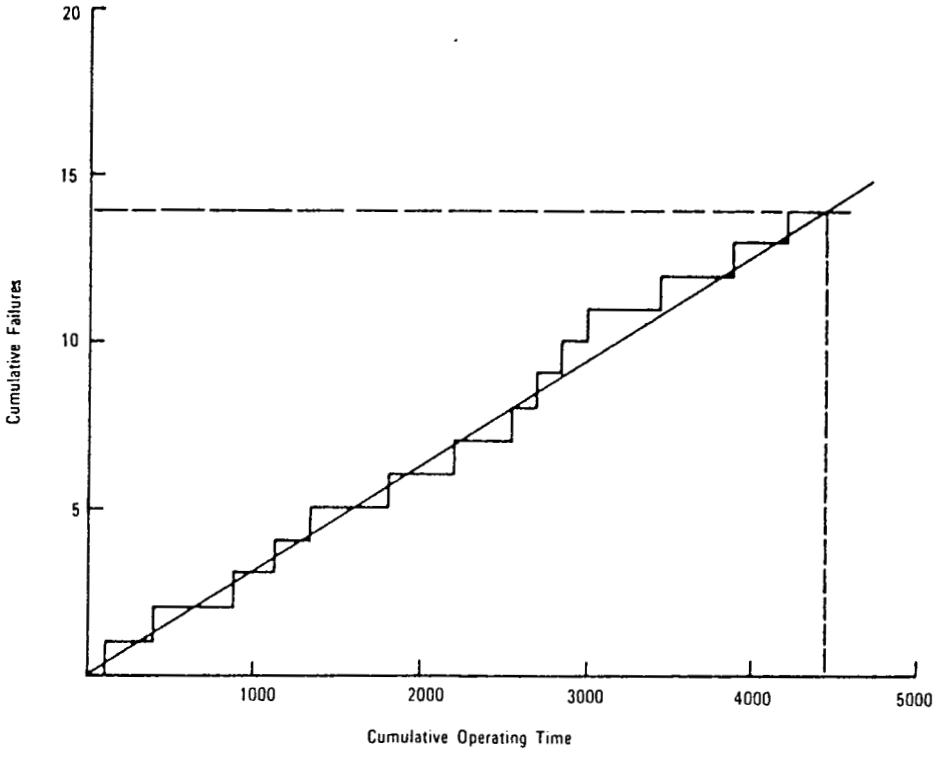


Fig 10
Distribution Graphical Evaluation

Whatever failure analysis techniques are used, they should be developed to provide a failure reporting system that best fits a particular plant or facility and yet fulfills the basic requirements as discussed in this section.

6.4.2 Failure Data Analysis. Data collected from any testing or field data program can be used to describe and summarize, via probability models, the performance of the items of interest. In using probability models and in making estimates, the statistical fundamentals presented in 6.1 must be kept in mind. In particular, the imprecision incurred by estimating parameters with limited data must be recognized and accounted for.

The analysis of failure data from a field data program can best be illustrated by examples. First, suppose that the field data program provides a set of operating times between failure for a single piece of equipment.

The first step in the analysis is to examine the data for trends. Does the distribution of times between failure appear to be changing with time, or not? One method of testing for trends is graphical. Simply plot the cumulative operating time versus the cumulative number of failures, as shown in Fig 10. If the distribution of time between failures is unchanging, the plot should look somewhat linear. A more formal quantitative test is provided by the statistic

$$Z = \left(\frac{\sum_{i}^{n} T_i}{nT} - \frac{1}{2} \right) \left(\sqrt{12/n} \right)$$

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

where

n = number of times between failures
T_i = cumulative operating time until the ith failure
T = total time the equipment has been in the field

If there is no trend, Z has approximately the standard normal distribution. Thus, by comparing a calculated Z to tables of the standard normal distribution [10], the assumption of no trend can be tested. For example, the probability the absolute value of Z exceeds 2.0 is about 0.05. Thus, an observed Z larger than 2.0 is fairly strong evidence against the assumption of no trend. This test is reasonably accurate for n as small as 3.

If there is evidence of a trend, analysis methods beyond the scope of this guide are called for (see [15] and [25]). If there is no strong evidence of a trend, the next step in the analysis is to determine a probability distribution that describes the distribution of the times between failures. The most convenient possibility is the exponential distribution. A "goodness-of-fit test" based on the ordered times between failures can be done graphically [21] or more formally [36], [38]. If the exponential assumption is supported by this test, the methods of 6.1 can be applied to estimate the failure rate λ.

The example in 6.1 was based on a failure history of one piece of equipment. Another possibility is that failure histories on more than one unit of that type of equipment are available. One then has the problem of ascertaining that these histories are consistent. (Comparison of two exponential distributions is discussed in [26].) If so, the cumulative operating times and failures can be pooled in order to estimate the common failure rate, λ.

In the case of nonrepairable equipment, the field data may be in terms of lifetimes of failed items and successful operating times for the remaining items in the field. Then the methods of Nelson [28] can be used to estimate the hazard rate and test the exponential assumption.

In all the cases just described, the actual times to failure, times between failure, or successful running times of individual items were available. Having these data available permits testing of the assumption of a constant failure rate or estimating the functional form of a nonconstant failure rate. Some data programs report only the cumulative operating time and the cumulative failures. About the only analysis permitted by these limited data is one based on an assumed constant failure rate. The reader should be aware that this may be a very misleading analysis. For example, the data reported on two systems might be 4 failures in 5 years of operation. One of them might have had all four failures the first year, the other, all four the fifth year. Clearly, different inferences are called for, but with only the cumulative data, this difference would not be detected. The constant failure rate assumption would yield identical results. Before such an analysis is done, there should be a realization that only very crude answers are required, or there should be good engineering reasons for assuming a constant failure rate.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

7. Application of Reliability Methods

7.1 Introduction. Qualitative methods are described in Section 4 and quantitative methods are described in Section 5. Because the application of the qualitative methods has been described, this section will deal primarily with quantitative methods. It should be remembered, however, that the qualitative methods can be very useful tools for furthering the understanding of a system design and for focusing attention on particular elements for further study. Among the other applications that do not require a quantitative goal, reliability analyses can be used to establish a hierarchy of alarms in the control room. Such a hierarchy, perhaps indicated by a gradation of the intensity of audible or visual signals, would allow operators to concentrate their attention on those alarms that indicate the most serious situations without being confused or distracted by relatively unimportant annunciators.

The product of a qualitative reliability analysis can be a powerful tool for the preparation of operating, testing, maintenance, or emergency procedures. The writer of a procedure should perform the necessary logical deductions to foresee the various actions or combinations of actions in the procedure, and is thus forced to reproduce a major part of the reliability analysis if it is not available to him. Similarly, a reliability analysis can be a major tool in trouble-shooting of equipment failures or spurious responses because the logical construction has already been performed.

7.2 Numerical Goals. In the application of quantitative analysis for safety systems of nuclear power generating stations, the design bases should include numerical goals for reliability/availability. Reliability goals as a part of the design basis establish allowable probabilities (or some equivalent numerical figures of merit) of failure of various parts of the system. It is important that these goals be established independently of the system analysis to prevent undue interactions between goals and analytical results.

Because of the wide variations among the components of the system, the influence of failures on the overall risk to the public, and the costs involved in achieving a specified reliability level, different goals may be established for different parts of the system. The combined effect of these goals must then be consistent with some overall goal. Although not solely responsible for specifying the overall goals, the system designer, because of his intimate knowledge of the plant and the interactions of the various subsystems, should contribute to the tradeoff process whereby individual goals, consistent with the overall goals, are established.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

7.2.1 Bases for Establishing Numerical Goals

7.2.1.1 Frequency of Demand. The expected frequency of occurrence (or probability of occurrence within a specified time interval) of conditions that require operation of a part of the safety system must be considered to establish the reliability of that part. These frequencies must be estimated, and they depend on many factors, among the most important of which are plant design, operating and maintenance techniques, control system capability, and the efficacy of the various echelons of protection, as well as the frequency of occurrence of external events such as loss of offsite power.

7.2.1.2 Consequence of Failure. To determine the reliability requirements of any safety system one must also consider the consequences of failure to perform. The consequences of failure of a safety device or subsystem when proper operation is required can vary quite widely, from equipment damage of varying severity to release of significant fission products into the environment. Some failures may require some other protection system components to operate properly to prevent unacceptable consequences.

7.2.1.3 Risk. The risk associated with a nuclear power plant accident is a function of the consequences of failure, the probability of failure, and the frequency of demand for safety system performance. For illustrative purposes, the risk associated with a given system may be taken as the simple product of the frequency of demand for system operation, the probability of system failure, and the magnitude of the consequences of the failure. In actuality, the magnitude of the consequences will have many multiplicative factors, each of which should be evaluated in a probabilistic manner. An example is the envelope of meteorological parameters that relate the release of a quantity of radioactive material to the radiation dose received by the public. The design basis parameters are statistical in nature, and with sufficient data can be estimated to any desired precision. They should be defined on a quantitative statistical basis, such as worst 50th percentile, so that the probability of their being exceeded can be known and applied to the consequence assessment.

The acceptable risk, on the other hand, is a function of society's response to the effect of the plant on their health and well-being. Logical units of measurement can be dose/year, dollars/year, injuries/year, or deaths/year. The acceptable risk becomes the basis of the goal for a given design. A given design may be considered satisfactory if the resultant risk is acceptable to society.

This concept of acceptable risk is a useful one, but society cannot be expected to make such a determination *a priori*, although their response may be inferred from history.

7.2.2 Specific Goals

7.2.2.1 Reactor Protective Action. An example of a protective function for which numerical goals may be established is the reactor emergency shutdown. Many situations with different rates of occurrence and different failure consequences necessitate such shutdowns. A very few cases may dominate the reliability requirements because of high frequency of occurrence or seriousness of consequences. If goals suitable for these cases can be established, and the effectiveness of engineered safety features are considered, it may be possible to show that the other

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

less severe or less frequent events do not appreciably change the requirements; although the validity of this conclusion should be demonstrated or corrections should be made to include the omitted situations. If the consequences of failure of the shutdown system for some situations include loss of engineered safety features, then the reliability goal of the shutdown system must take this into account.

7.2.2.2 Engineered Safety Features. In addition to the reactor shutdown system, engineered safety features are provided to mitigate the consequences of certain accidents. Containment closure systems and emergency cooling systems are examples. The numerical goals established for the reliability of these systems are determined in a way similar to that for the shutdown system. However, the rate of challenge as well as the consequence of failure of an engineered safety feature may depend on the reliability of some other engineered safety feature. In general, a reactor shutdown system is required to respond to an abnormality and to initiate an action, but the continued operation of the shutdown system is not required. Thus, the goal is usually one of "availability." However, for many engineered safeguards continued operation of certain equipment is required after initiation. In these cases reliability and availability are both of interest.

7.2.3 Procedures. Reliability goals must be assigned to the various subsystems to insure that the total continuous risk to the public is less than the acceptable risk for the plant if the goals are met. These goals then form the bases for reliability allocations to the smaller portions of the system. Each accident and the unreliability of the protection subsystems associated with limiting the consequences of the accident contribute to the risk. It is this total risk (that is, the sum of the risks associated with all accidents being considered) that is important, although a "worst case" situation that dominates may exist. The result will be assigned reliability goals for the various protection systems (or large subsystems). These goals become the yardsticks for evaluating the results of reliability analyses.

7.3 Selection of the Modeling Technique. The reliability modeling technique selected should be based on the reliability analysis requirements. Typical requirements are summarized below.

7.3.1 Model Requirements

(1) *Time Requirement.* Due to the nature of reliability data, sensitivity studies may be required to establish a level of confidence in the results. Therefore, economics may predicate that the time for the analysis be relatively short.

(2) *Replacement Time.* Some reliability models are capable of handling only failure modeling and are incapable of addressing repair. Repair or replacement, or both, is a critical factor of some safety systems since, due to long mission times, repair of failed components is possible. This can be a major consideration of the reliability model since repair may determine the spare parts requirements and the attendant logistics support.

(3) *Failure and Repair Modeling.* Although constant failure rate and constant repair times are convenient simplifying assumptions, it may be important that the model is capable of reflecting other component failure distributions. This could result if sensitivity to deviations from the exponential were to be studied.

(4) *Probability Distribution.* It may be necessary that the output of the model be a probability distribution function rather than just a point estimate or single

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

probability number, especially for a subsystem model whose output is to be used as input to a system model.

7.3.2 Model Limitations. The following paragraphs discuss the major features of the various types of reliability models.

(1) *Fault Tree/Cut Set.* The major drawbacks to use of this technique are excessive computer time, inability to handle multiple system states, and the attendant inability to generate probability functions. Modifications could be developed to handle multiple states, but the computer time would still be large compared to some other techniques.

(2) *Markov.* Such models can be adequate for all concerns listed in 7.3.1, although constant failure and repair rates must be assumed. The major drawbacks are the required mathematical sophistication and significant engineering time in model development.

(3) *Boolean.* Boolean techniques do not have the ability to adequately treat multiple states. In addition, application of Boolean models to any but the most simple systems becomes prohibitively complex.

(4) *Event Trees.* These techniques adequately model multiple system states, but are incapable of handling repair or replacement in any realistic manner.

(5) *Monte Carlo.* Such simulation techniques may be combined with several other methods, and can treat nonconstant failure and repair rates. The most widely utilized method is a combination of fault tree and Monte Carlo. Although such techniques are very easy to implement and understand, their computer run time may be much larger than that of other techniques.

7.4 Fault Tree Techniques. Fault tree analysis techniques are widely used for reliability evaluation in the nuclear industry. The use of the fault tree method has been described in 4.2 and is exemplified in the Appendix. Although frequently used, the fault tree technique is not the most advantageous for all purposes. Based upon the positive and negative attributes of fault tree analysis, as delineated below, recommended uses are detailed. Applications in which fault tree analysis should not be used are also described.

7.4.1 Characteristics. Fault tree techniques are directed at determining the causes and the probability of a single event as described in 4.2. The most undesired top event is specified and the system failure logic is established by tracing through the systems down to the level at which failures induce the top undesired event. The technique is not applicable to analysis of the multiple events of which most systems are capable. This is as compared to a failure modes and effects analysis for instance, in which the component failures are traced up through the system to define the multiple events that could occur. The fault tree technique is extremely powerful in its ability to trace through several interconnected systems to find the root causes of the top event. It provides a framework for interrelating complex interfaces among systems.

One of the most beneficial aspects of fault tree analysis is that it aids the analyst in understanding the failure characteristics of the system under examination. The technique does this by guiding the analyst through the pertinent features of the particular system as they relate to system failure. The technique aids the analyst in determining those aspects of the system that need not be examined in any detail

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

thereby providing an efficient means of examining the system. The technique further facilitates insight on the part of the analyst as to the functioning of the system.

Fault tree techniques are hampered in their application by several problems. The first of these is that fault tree techniques treat only binary states. That is, fault trees can address only whether the system is completely failed or completely good. A single fault tree is incapable of addressing degraded states of the system. For instance, a single fault tree could not be used to model the state of a utility grid in which differing levels of available generation capability occur at differing probability levels. A fault tree could only be used in this case to determine whether or not the system were capable of producing power at a rate above a given specified level.

Another difficulty in the use of fault tree techniques is in quantification, as typically done by computers. If cut sets are obtained, the available computer programs typically require very long run times. The long run time to determine the cut sets and to determine failure probabilities from the cut sets limits the application of the technique. For instance, if it is expected that many sensitivity runs will have to be performed, it is possible that the computer cost will be so high as to make the analysis prohibitively expensive. If the synthesis techniques, which do not require the use of defined cut sets, are used, the run time is not large. However, lower computer costs are obtained at the sacrifice of valuable information. For many problems, the cut sets are as or more important than the numerical estimate of the probability of the top event.

A third negative characteristic of fault tree techniques is their inability to handle any but the most simple models of repair. Fault tree techniques are incapable of handling the continuous change of state of components between failed and unfailed. Markov analysis techniques coupled with conditional probability methods are much superior to fault trees for this purpose. Additionally, fault tree techniques are typically incapable of adequately modeling sophisticated testing schemes for reactor protection systems. It is possible to synthesize a testing scheme using fault trees, but it is typically quite different and involves a large amount of the analyst's time to get an adequate simulation.

7.4.2 Recommended Uses. Fault trees are most useful in the analysis of complex systems where the failure logic leading to the top event cuts across many system boundaries. The technique is most applicable to situations in which multiple sensitivity runs will not be performed.

Fault tree techniques should not be utilized in analysis of systems for which development of complicated testing schemes is desired. Furthermore, if repair is expected to be an important parameter in the overall system evaluation, fault tree techniques present serious drawbacks. In situations where sensitivity studies or design tradeoff studies are desired, fault tree techniques again possess several negative features.

7.5 The Markov Process as a Reliability Model. A Markov process is defined as a finite stochastic (random) process that consists of a sequence of outcomes such that the outcome expected subsequently is dependent upon some random occurrence that occurs is one of a finite (countable) number of possible

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

outcomes. Each of the possible outcomes is called a system state, and the probability of an outcome in any trial is assumed to be independent of any except the immediately previous trial. This assumption is the reason that a Markov process is sometimes referred to as the "good as new" model, since if the probability of being in state i after having started in state j is constant, the likelihood of moving from an operational to a failed state (j to i) is constant. This is the result expected for the traditional reliability model, the constant failure/repair rate. Note, however, that the definition of a Markov process does *not* require constant failure or repair rates, only that the probability of transition from one state to another be defined purely in terms of a prior state.

Mathematically, the definition of a Markov process for a continuous stochastic variable $X(t), t > 0$ is that for any set of n time points, $(t_1, t_2 \cdots, t_n)$ in the index set of the process, and any real numbers, the following equality holds:

$$\Pr[X(t_n) \leq x_n \mid X(t_1) = x_1, X(t_2) = x_2, \cdots, X(t_{n-1}) = x_{n-1}]$$
$$= \Pr[X(t_n) \leq x_n \mid X(t_{n-1}) = x_{n-1}]$$

This equation is read as "the probability that the random variable X is less than or equal to the value x_n, at time t_n, conditional upon having been x_1 at $t = t_1$, x_2 at $t = t_2$, and x_{n-1} at $t = t_{n-1}$, is the same as the probability of X being less than or equal to x_n, conditional *only* upon having been equal to x_{n-1} at $t = t_{n-1}$.

The application of the concept of a Markovian process to equipment reliability and maintainability is achieved by consideration of the failure and repair/replacement process as in classical reliability theory. If one assumes a constant failure rate λ, and a constant repair rate μ, the probability of failure or repair in a time interval $(t, t+dt)$ is $\lambda\, dt$ or $\mu\, dt$, respectively, if the probability of more than one repair or failure in the time interval $(t, t+dt)$ is small. The failure or repair rate of a component is then the transition probability between one of two states for the equipment: state one is the unfailed condition, while state two is the failed condition. The transition probabilities for this process may be displayed in one or two forms: either the transition probability (or transition rate) matrix, or the transition probability (or transition rate) diagram.

As a simple example (taken from [13]), consider a system that can be in three different states, such as a system of two identical fully redundant and independent components, any one of which can be repaired upon failure without interrupting the operation of the good component. The system states may be defined as follows: State 0—both components work; State 1—one of the two components fails with failure rate λ and is being repaired with repair rate μ; and State 2—both components are failed and in repair. In State 2 both components may be in repair simultaneously (which is called *unrestricted* repair), or only one at a time is in repair (which is called *restricted* repair).

One is usually interested in knowing how this system will change its states due to the failure and repair processes, and in determining the probabilities of the system being in State 0, 1, or 2 after a time 5, if at time $t = 0$ the system starts in State 0 with both components being operational (any other initial state may also be specified). When both components are operational (State 0), the rate of transition of State 1 is 2λ; from State 1 the system may return to State 0 with a repair rate μ, or may

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

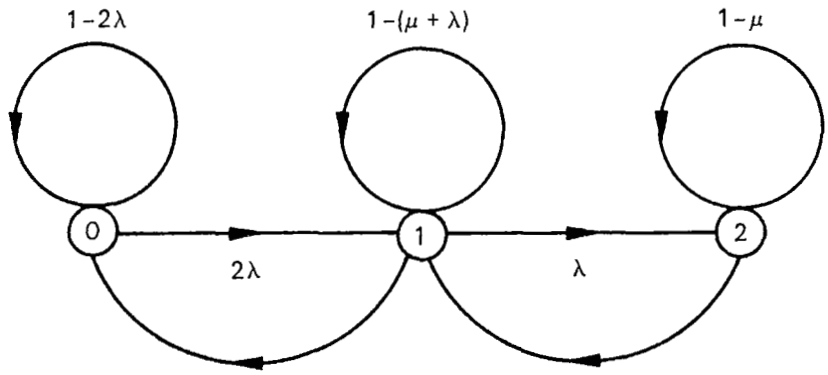


Fig 11
Transition Rate Diagram

transit to State 2 with a failure rate λ. It is assumed that the system may return from State 2 to State 1 with a repair rate μ_2 (for $\mu_2 = \mu$, while for unrestricted repair the rate would be restricted repair $\mu_2 = 2\mu$). In the following, the restricted repair case is assumed. Thus, the transition probabilities p_{ij} in a short interval dt are then as follows:

(1) From State 0 to State 1: $P_{01} = 2\lambda\, dt$
(2) From State 1 to State 0: $P_{10} = \mu\, dt$
(3) From State 1 to State 2: $P_{12} = \lambda\, dt$
(4) From State 2 to State 1: $P_{21} = \mu\, dt$

It is assumed that in the short time interval dt double transitions are not possible, so that P_{02} and P_{20} are zero. The complementary probabilities are those of no-transition. Thus, if the system is in State 0, the probability of remaining in that state in an interval dt is $P_{00} = 1 - 2\lambda\, dt$, which is the complement of the transition probability $P_{01} = 2\lambda\, dt$. The other no-transition probabilities are then $P_{11} = 1 - (\lambda + \mu)$, where $(\lambda + \mu)$ is the transition rate of the system going from State 1 either to State 2 or returning to State 0, and $P_{22} = 1 - \mu\, dt$. These result in the three self loops shown in the transition rate diagram of Fig 11 and the transition rate matrix shown in Fig 12.

Either representation is sufficient to set up the probability equations for the behavior of the system. First, the difference equations relating the probability of system state n at $(t + dt)$ back to the probability of system state n at t are written, using the earlier defined transition probabilities:

$$P_0(t + dt) = P_0(t)\,[1 - 2\lambda\, dt] + P_1(t)\,[\mu\, dt]$$

$$P_1(t + dt) = P_0(t)\,[2\lambda\, dt] + P_1(t)\,[1 - (\lambda + \mu)\, dt] + P_2(t)\,[\mu\, dt]$$

$$P_2(t + dt) = P_1(t)\,[\lambda\, dt] + P_2(t)\,[1 - \mu\, dt]$$

By performing the multiplications on the right side of this set of equations and rearranging the derivatives of the probabilities of $P_0(t)$ on the left side, $P_1(t)$ and

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

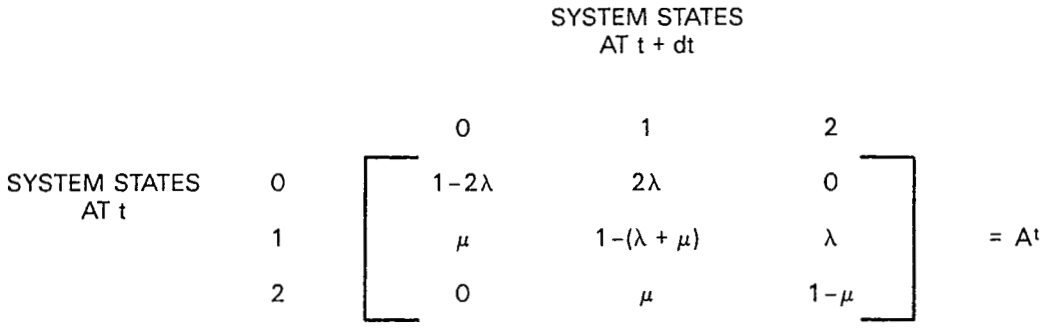


Fig 12
Transition Rate Matrix

$P_2(t)$ appear (in other words, the probabilities that the system will be in State 0, 1, or 2 at t for a specified initial condition at $t=0$, such as $P_0(0) = 1$):

$$\frac{P_0(t + dt) - P_0(t)}{dt} = -P_0(t)\,[2\lambda] + P_1(t)\,[\mu]$$

$$\frac{P_1(t + dt) - P_1(t)}{dt} = -P_0(t)\,[2\lambda] - P_1(t)\,[\lambda + \mu] + P_2(t)\,[\mu]$$

$$\frac{P_2(t + dt) - P_2(t)}{dt} = -P_1(t)\,[\lambda] - P_2(t)\,[\mu]$$

Changing from the explicit notation to matrix notation, the above set of equations can be written as

$$\underline{P}(t) = \underline{\underline{A}}\,\dot{\underline{P}}(t)$$

Here $\underline{\underline{A}}$ is the transpose of matrix A defined in Fig 12. There are various ways to solve such sets of differential equations including "canned" computer programs.

7.5.1 Constant Failure and Repair Rate Components. For those components that can be modeled adequately as constant failure/repair rate components, the system of equations to be solved are of the form given in the preceding section as the result of the sample application of the Markov process to reliability calculations. Redundant identical components may be specified either explicitly, or the same reliability data may be used for each redundant component.

7.5.2 Constant Repair or Switching Time Components. In some cases, it may be more accurate to consider a constant time period instead of constant rates for either failure or repair. For instance, standby equipment could be most accurately modeled as having a constant time period required to effect the switchover in case of failure of the normally operating component, since repair may be effected by the simple expedient of replacement of a failed component. Also, the time required for a spare pump to be valved into the flow path after switchover, since the valve requires a finite time to open, can be approximated as the ratio of the travel distance to the opening rate.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Terms of this type cannot be handled in the system of equations described so far. The introduction of a switching time introduces a delay term that prevents any transition from the temporary failed state until the time interval has elapsed. At the end of the interval, τ, the component is either repaired or switchover has been achieved and the state is now empty except for the probability of another transition into the state in the interval $(t, t+\tau)$.

The equation that describes the reliability R of a constant repair time component is $R(t) = -\lambda R(t) + \lambda R(t-\tau)$. Physically, this is intuitively correct since the repair rate at (t) hours is precisely the failure rate at $(t-\tau)$ hours, because the component that failed at $(t-\tau)$ *must* be repaired (probably replaced) at $t+\tau$, or the switchover must have been completed at τ hours after the failure. (In the case of switchover, the return may not be back to the original state, as will be explained in the next section.)

The system of equations to be solved must be modified if components with constant repair or switching times are to be considered since the terms in $(t-\tau)$ did not appear previously. By analogy to the equation for constant repair of a single component, the general form of the equations can now be written as

$$\underline{\dot{P}}(t) = \underline{\underline{A}}\,\underline{P}(t) + \underline{\underline{B}}\,\underline{P}(t-\tau)$$

where $\underline{\underline{B}}$ is another transition rate matrix similar to $\underline{\underline{A}}$ but describing only those states with constant delays, either due to switching or repair. The methods for developing $\underline{\underline{B}}$ are similar to those for $\underline{\underline{A}}$: one enumerates the possible states of the system and those components that are to be modeled as constant time terms rather than rates are identified as such.

7.5.3 Constant Success/Failure on Demand. Some components (particularly inactive standby) may have a probability of failure on demand as well as or instead of a probability of failure per unit time (passive or active). For example, a standby pump may fail to operate when attempts to activate it are made due to failure of electrical switches to open or close, or corrosion of the pump while in standby. This may be modeled by including the net probability of failure on demand as a multiplier on the transition rate between the success/failure branches leaving the state in the transition diagram. The incorporation of constant probabilities between selective states of the transition diagram does not require modification of the forms of the equations solved. However, care is required in the construction of the diagram to be sure that the sum of all probability branch paths leaving a state equals one, otherwise total probability will not be conserved.

7.6 Equipment and System Testing. The testing of equipment and systems to determine or assure reliability may be divided into three separate activities: acceptance or qualification sampling, initial in-serving testing, and experience-based in-service testing. While similar statistical rules apply to each of these types of testing, the amount of prior information available to be used in designing the testing program is different, and the effect of the testing on the equipment or system is different. Because testing may place unusual stress on equipment, and often removes a system from service, the purpose of testing should be thoroughly defined and rigorous statistical methods should be used to minimize the amount of testing.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

7.6.1 Acceptance Sampling. In order to provide assurance that an item meets or continues to meet reliability goals, it may be desirable to establish a test program. Such a test program might be preoperational (in fact it might be used to help choose among manufacturers of the item) or it might be operational. For example, diesel generators are tested periodically to see whether an acceptable probability of starting is being maintained. In this section, results from 6.2.3 are applied to provide guidance on an acceptance test program.

The situation considered is binomial. There will be n independent tests with two possible outcomes, success and failure, and the failure probability at each test can be assumed to remain constant throughout the tests. Furthermore, for the test to be of use, it must be reasonable to assume that the failure probability under test conditions is equal to that under operational conditions. The objective is to "demonstrate" that the item has a failure probability that does not exceed its goal, say p_0. However, with a finite number of tests, any demonstration cannot be conclusive. There will be some probability of incorrectly concluding the goal has been met. Controlling this probability provides a way to determine the number of tests, n.

Consider an acceptance test in which the item is deemed acceptable if there are no failures in n tests. Under the binomial distribution, the probability of this outcome is $P(A) = (1 - p)^n$, where p is the probability of an item failing the tests and A denotes "acceptance." The number of tests n can be specified such that if p exceeds the goal p_0, then $P(A)$ will be less than a specified probability α. In particular, the number of tests is given by

$$n = (1n\ \alpha)/1n\ (1 - p_0)$$

The following gives some values of n determined from this relationship.

Values of n such that $P(A) < \alpha$ at $p > p_0$:

p_0	0.10	0.05	0.01
0.10	22	29	44
0.05	45	59	90
0.01	230	299	459
0.005	460	598	919

Thus, for a given value of n, if the failure probability exceeds p_0, the chance of passing the test is less than α.

From the results of the acceptance tests just discussed, zero failures in n tests, statistical confidence statements can be made. In fact, the statement is that the upper 100 $(1 - \alpha)$% confidence limit on p, the underlying failure probability, is less than or equal to p_0. Or, equivalently, the lower 100 $(1 - \alpha)$% confidence limit on reliability is greater than or equal to $1 - p_0$. Plans are often referred to in this way. For example, the acceptance plan that requires no failures in 59 tests corresponds to $\alpha = 0.05$ and $p_0 = 0.05$ and is sometimes called a 95/95 plan. If the acceptance criterion is met, then with 95% confidence the underlying reliability is at least 0.95. The first number denotes the confidence level, the second and lower limit on reliability; so for example, a requirement of zero failures in 45 tests, which corresponds to $\alpha = 0.10$, $p_0 = 0.05$, would be called a 90/95 plan.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

For any given set of data, one can make a whole battery of confidence statements. From the above table, it is apparent that for zero failures in 45 tests it can be stated that with 90% confidence the reliability exceeds 0.95, and because $\alpha = 0.01$, $p_0 = 0.10$ leads to virtually the same plan (44 tests instead of 45) it can also be stated that with 99% confidence the reliability exceeds 0.90. That is, a 90/95 plan is essentially the same as a 99/90 plan, and of course, a whole continuum of equivalent confidence statements and corresponding plans can be obtained. All of these are different, legitimate ways of summarizing the same basic data: zero failures in 45 tests. In choosing a plan, the user should consider more than just a single confidence level and failure probability.

For a given value of n and any value of p, the probability of passing the test, $P(A) = (1-p)^n$ can be calculated. A plot of $P(A)$ versus p is called the operating characteristic (OC) curve of an acceptance test plan. The OC curve summarizes the performance properties of the test. It indicates what quality of product will be accepted with high probability and what quality will have a low probability of acceptance, and thus shows the discriminating power of the test. Any test plan, whether chosen by probabilistic arguments such as convenience or economics, has an associated OC curve and this curve should be examined before the plan is put into practice.

A single sampling plan is determined by two parameters, the sample size n and the acceptance number, usually denoted by c. An item will pass the demonstration test if c or fewer failures occur in n binomial tests. Thus, the acceptance probability is given by

$$P(A) = \sum_{r=0}^{c} f(r),$$

where $f(r)$ is the binomial distribution

$$f(r) = \binom{n}{r} p^r (1-p)^{n-r}$$

From this relationship, p_0, α, and c are specified; then the required sample size n can be derived. For $c = 0$, the derivation is particularly simple, as shown above.

For a specified p_0 and α, many values of (n, c) will provide the desired demonstration. To choose among the possibilities, the OC curve needs to be considered. The user has to decide how much discrimination is required. In quality control applications, it is conventional to summarize the OC curve by two points, one the value of p at which $P(A) = 0.95$ and the other the value of p at which $P(A) = 0.10$. Thus, one point is at the high end of the curve, the other at the low end. The ratio of the two values of p, call them $p'_{0.10}$ and $p'_{0.95}$, is a measure of the discriminatory power of the test. The larger c is, the smaller the ratio $p'_{0.10}/p'_{0.95}$, becomes, which means that the OC curve becomes steeper and hence, there is better discrimination between large and small p. Table 4, reproduced from [14], gives values of this ratio as a function of c and also gives values of np corresponding to $P(A) = 0.95$ and $P(A) = 0.10$. (These values are obtained from a Poisson approximation to the binomial distribution.)

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Table 4
Two-Point Design of a Single-Sampling Plan with α Approximately 0.05 and β Approximately 0.10

c	$p'n_{0.95}$	$p'n_{0.10}$	$p'n_{0.10}/p'n_{0.95} = p'_{0.10}/p'_{0.95}$
0	0.051	2.30	45.10
1	0.355	3.89	10.96
2	0.818	5.32	6.50
3	1.366	6.68	4.89
4	1.970	7.99	4.06
5	2.613	9.28	3.55
6	3.285	10.53	3.21
7	3.981	11.77	2.96
8	4.695	12.99	2.77
9	5.425	14.21	2.62
10	6.169	15.41	2.50
11	6.924	16.60	2.40
12	7.690	17.78	2.31
13	8.464	18.96	2.24
14	9.246	20.13	2.18
15	10.040	21.29	2.12

Not for Resale

Suppose, for example, that one wishes a plan such that at $p = p_0 = 0.01$ the probability of acceptance will be $P(A) = 0.10$, while at $p = 0.002$, $P(A)$ will equal 0.95. The ratio of these two failure probabilities is $p'_{0.10}/p'_{0.95} = 0.01/0.002 = 5.0$. From Table 4, the smallest value of c that gives a ratio less than or equal to this value is $c = 3$. The corresponding value of np at $P(A) = 0.10$ is $np = 6.68$. Thus $n = 6.68/p'_{0.10} = 6.68/0.01 = 668$ and the demonstration plan that meets the requirements is $(n, c) = (668.3)$.

The quality control literature, for example, [16], contains a wide variety of acceptance test plans. One extension beyond single sampling plans is to double sampling plans wherein an initial sample is taken and then, based on the results, a second sample may be taken. These plans, in turn, have been extended to multiple sampling plans. In general, the double and multiple sampling plans require, on the average, less testing than do single sampling plans.

Demonstration test plans have also been developed for other than the binomial distribution. In particular, tests for failure rates, based on the exponential distribution, are available (for example, [26]). Some of these tests, usually referred to as "life tests" are quite similar to the binomial tests just discussed. For example, the plan might be to test an item, or collection of items, until T time units have been accumulated. Then if c or few failures (deaths) have occurred during this time, the item is accepted. The number of observed failures will be Poisson distributed, so by substituting λ (the failure rate) for p and T for n, Table 4 can be used to specify the test parameters, T and c.

7.6.2 Initial Test Intervals. Having established numerical reliability goals, the next task is to determine at what intervals the various portions of the system must be tested to ensure that the system can be maintained in a state that meets the necessary reliability goals.

It is presumed that at this stage models have been prepared and that the credibility of the results of the trial analyses has been established. If the trial calculations were made on the basis of realistic test intervals, the comparison of the results with the goals can be used to determine if the goals have been met and by what margin. If the goals have not been met, it might be necessary to alter test schedules or perhaps even change system components or configuration. In any case, one should at this time (if it is possible at all within other constraints) be able to establish a test interval that is practical and that provides significant reliability margins over the goals.

The next step should be to review the whole process and to recall that the test interval and schedule are constrained by factors not related to the specific analyses outlined here. Since tests can detect not only random component failures but also certain classes of common mode failures, the full benefits of the tests are not necessarily apparent. Also one should remember that a reliability calculation usually represents an upper bound on system success probability, being primarily a measure of the likelihood of proper operation despite random component failures. Other nonrandom failures, such as common cause, are not always accounted for.

After having established a mathematical model for the system, the test interval can be calculated as a function of the assigned availability design goal. This is accomplished by equating the expression for unavailability to the design goal, and solving for the test interval.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

For a single component, the unavailability is given by

$$\bar{A} = \frac{\lambda\theta}{2}$$

Let the unavailability goal be $\bar{G}$; then

$$\bar{G} = \frac{\lambda\theta}{2} \qquad \text{(Eq 56)}$$

and

$$\theta = \frac{2\bar{G}}{\lambda} \qquad \text{(Eq 57)}$$

The popular logic configurations normally encountered can be treated similarly provided that the criteria of 5.3 are met. Table 2 can be rearranged to tabulate test intervals as a function of the design goal for various logic configurations as shown in Table 5. The test intervals from Table 5 do not include margin.

Table 5
Test Interval as a Function of Logic Configuration and Unavailability Design Goal *G*

Logic Configuration	Test Interval	
	Simultaneous Testing	Perfectly Staggered Testing
1/2	$\frac{1}{\lambda} \cdot (3\bar{G})^{1/2}$	$\frac{1}{\lambda} \cdot \left(\frac{24\bar{G}}{5}\right)^{1/2}$
2/2	$\frac{1}{\lambda} \cdot \bar{G}$	$\frac{1}{\lambda} \cdot \bar{G}$
1/3	$\frac{1}{\lambda} \cdot (4\bar{G})^{1/3}$	$\frac{1}{\lambda} \cdot (12\bar{G})^{1/3}$
2/3	$\frac{1}{\lambda} \cdot (\bar{G})^{1/2}$	$\frac{1}{\lambda} \cdot \left(\frac{3\bar{G}}{2}\right)^{1/2}$
3/3	$\frac{1}{\lambda} \cdot \frac{2\bar{G}}{3}$	$\frac{1}{\lambda} \cdot \frac{2\bar{G}}{3}$
1/4	$\frac{1}{\lambda} \cdot (5\bar{G})^{1/4}$	$\frac{1}{\lambda} \cdot \left(\frac{7680\bar{G}}{251}\right)^{1/4}$
2/4	$\frac{1}{\lambda} \cdot (\bar{G})^{1/3}$	$\frac{1}{\lambda} \cdot \left(\frac{8\bar{G}}{3}\right)^{1/3}$
3/4	$\frac{1}{\lambda} \cdot \left(\frac{\bar{G}}{2}\right)^{1/2}$	$\frac{1}{\lambda} \cdot \left(\frac{8\bar{G}}{11}\right)^{1/2}$
(1/2) · 2	$\frac{1}{\lambda} \cdot \left(\frac{3\bar{G}}{2}\right)^{1/2}$	$\frac{1}{\lambda} \cdot \left(\frac{12\bar{G}}{5}\right)^{1/2}$

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

7.6.3 In-Service Adjustment of Test Intervals. Because of uncertainty in data, high estimates of failure rates are usually used, resulting in conservative initial test intervals. Since too frequent testing is an economic burden and may contribute to unnecessary down time or may shorten component lifetimes, it is often desirable to extend the test interval if failure rates are proven to be significantly lower than postulated. In the event that failure rates are appreciably greater than estimated, it is important to shorten test intervals (or enhance reliability by other means). A significant increase in failure rate of a specific component should be investigated to find whether or not application or environmental problems exist; these problems may make the component behave differently from its counterparts on which the original failure data were obtained.

It is important to recognize that testing more frequently may actually be a detriment to reliability because of wearout, time out of service for testing, and improper restoration after testing. Methods for estimating this effect are given in [6] and [27].

As a part of the reliability analysis package for determining test intervals, the analyst should provide a set of specific guides for justifying alteration of testing intervals. He should also provide instructions for interpreting and documenting test results to ensure that the best data possible for future failure rate determination are obtained.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

Appendix

(This Appendix 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.)

A1. Introduction. This appendix is provided to assist those unfamiliar with reliability analysis in understanding the concepts involved and the methods employed in assessment of system reliability or availability. Both qualitative and quantitative analyses are covered, although the techniques of qualitative analyses are already familiar to those dealing with reactor protection systems through the use of single-failure analysis. A general procedure is described whereby, in stepwise fashion, the principles of reliability analysis can be implemented. The order in which the steps are done is not particularly significant, except that some steps are useful as preparatory or preliminary work for others; for example, qualitative block diagram analysis can be useful in providing the basis for quantitative reliability computation. It is not necessary to perform each step illustrated because some are equivalent methods where the choice of procedure will depend on the preference of the analyst and the purpose of the study. Similarly, the examples are not intended to be all-inclusive, and other methods may well be used to accomplish the same objective. The examples do illustrate methods that have been successfully employed to ensure that system reliability or availability is predicted to be consistent with the goal appropriate for the function performed by the system.

A2. Procedure. A procedure such as that outlined in the following is illustrated by examples in this appendix. More details of each of the steps are contained in the appropriate sections in the body of this document.

A2.1 System Definition. Before any analysis, it is necessary to define the system being evaluated. For small systems such as an alarm on an equipment enclosure door, such definitions are easily perceived and simply stated. However, for complex systems such as a reactor plant protective system, the problem is more difficult and more significant. Several decisions must be made in the definition of a complex system. The system boundaries must be clearly and unambiguously described. For example, one must consider how the system depends on other systems for power, environment control, etc, and decide where the interface should be drawn for the analysis. Next, one must decide the level of detail at which the system will be analyzed. Generally, it is most efficient to consider the system as a collection of replaceable modules or units. On occasion, however, it is necessary to go to subassembly or part level to adequately assess system performance. It is also necessary to determine the operating conditions under which the system is to carry out its function and the operational profile expected for the system. The most critical part of system definition as far as analysis is concerned is the definition of failure. This

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

will include consideration of minimum performance requirements and allowable limits in both the functional and physical sense and should include the effects of the operational environment. Reliability analysis deals basically in two states, operable and inoperable, and it is frequently necessary to convert a continuous spectrum of performance degradation into success/failure terms.

Having adequately defined the system, one can proceed with failure mode identification.

A2.2 Failure Mode and Effects Analysis (FMEA) (Qualitative Analysis). The qualitative analysis of system failure modes is the familiar single-failure analysis. This study, one example of which is a failure mode and effects analysis (FMEA) (see 4.1), is conducted to determine the effects of each component failure mode on the overall system performance. In this process, the component failure modes that could contribute to unsafe system failure are identified, and necessary action can be taken at this point in the procedure.

A2.3 Common-Mode-Failure Analysis. Having identified the unsafe component failure modes, another step in qualitative analysis that can give assurance of system adequacy is common-mode-failure analysis. As an extension of single-failure analysis, the total system is examined in a systematic manner to identify the combinations of failures that can lead to unsafe system failure. The combinations are then assessed for their relative likelihood in a qualitative engineering sense, and any necessary action can be taken prior to quantitative prediction of system performance.

A2.4 Reliability/Availability Prediction (Quantitative). System probabilities (reliability/availability) can be represented in terms of mathematical models for success or failure. The models are typically represented in logic diagrams, that is, fault trees or reliability block diagrams. After the model has been selected, the system identified, and appropriate failure modes identified, predictions can be made of system reliability or availability using the logic diagrams.

A2.4.1 Determination of Test Interval. From the model and the identification of significant components, the maintenance level (if necessary) can be established and the surveillance frequency determined. In a continuously operating system, the mission time can be taken as the time between tests, and thus determination of test interval often will involve an iterative process with goal allocation.

A2.4.2 Reconciliation of System Goals. The component failure modes and rates, and the logic diagram, are used to reconcile the system goals. From the model, the system reliability can be calculated. A sensitivity analysis could be performed to identify the component(s) significantly affecting the result. Any design or operational strategy changes necessary to predict achievement of the goals can be made at this point.

A3. Illustrative Examples. To illustrate the application of the principles of this document, the *typical reactor trip function* described in Section 4 will be used as an example. This is a subsystem of a total plant protection system and thus must be considered in the context of the overall system operation and requirements.

A3.1 System Definition. The typical reactor trip function to be evaluated is defined by the diagram in Fig A1 and operates as described in 4.4.1. The system

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

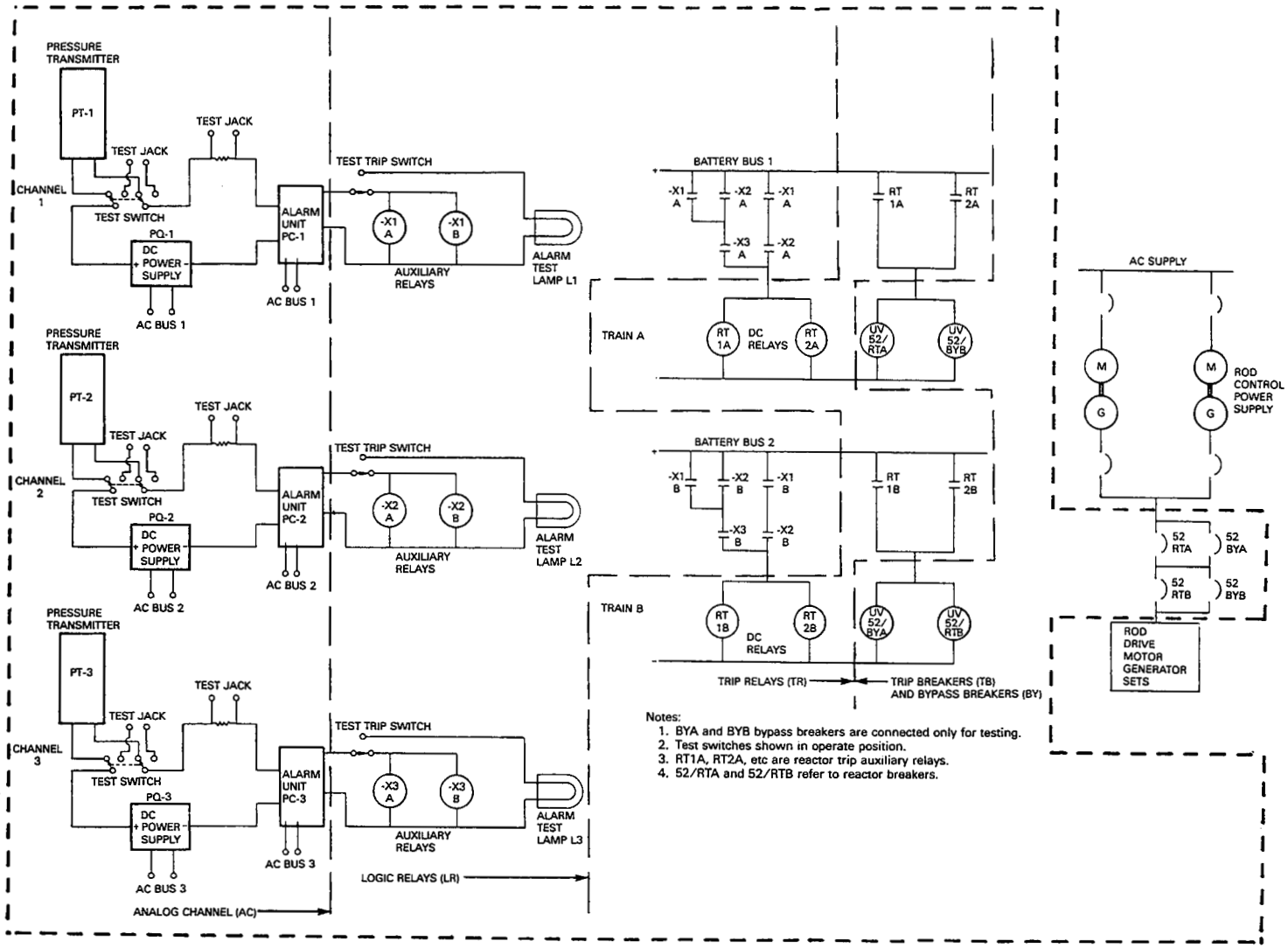


Fig A1
One Function Diagram for a Typical Reactor Trip Function

352-87 4805702 0008232 6

boundary is defined such that motor-generators, rod-control-power supply, ac and battery buses, and test circuitry are external interfacing items rather than components of the system itself. The level of analysis is that of a replaceable component, for example, pressure transmitter, dc power supply, etc. These units may be analyzed as functional "black boxes" with failure rates as listed in Table A1. Their failure modes need not be further defined unless it is desirable to assess in detail the relative probabilities of different failure modes, to assess the vulnerability of the unit to a particular combination of circumstances, or to modify the predicted reliability by consideration of changes to the internal makeup of a unit.

A3.2 Qualitative Analysis—FMEA. The qualitative single-failure analysis used in this part of the appendix is failure modes and effects analysis (FMEA). This section will deal with the uses of the FMEA, the mechanics of doing the work, and the results obtained for the example problem. The steps for doing the FMEA will not be covered here because they are adequately described in Section 4.

A3.2.1 Uses of the FMEA. The FMEA can have many uses, depending upon who is using it. This section will focus on two users who can benefit from the study, the analyst and the designer. The analyst benefits because he uses the FMEA to evaluate the system and to assess the extent of conformance to criteria. The designer benefits because he can test his system analytically and determine the various ways that it could fail in use, and take necessary remedial action.

A3.2.1.1 Conformance to Criteria. The FMEA is used here to evaluate the example system for conformance to criteria. By it, one analytically tests the model for conformance to design requirements as specified in ANSI/IEEE Std 603-1980 [5] and other appropriate documents. Some of these criteria that will be covered in the analysis are identified principally as

(1) single-failure
(2) channel independence
(3) automatic action
(4) testability

In doing the work, then, one simply examines each component in the model and tests it by the above criteria. If the system still works for each test, the criteria are met; if not, then something should be done to correct it.

A3.2.1.2 Design Tool. The FMEA process causes the designer to think of what can happen to his system if a single failure should occur. It motivates him to go through the mechanical motions of tracing single failures from initial cause to ultimate effect. He determines the effects the failure will have on the logical operation of the design, such as changing a normal 2/3 coincidence to a 1/3 or 2/2 coincidence (depending upon which failure mode is being investigated). Through this process, he learns how the failure could be detected and how the design compensates or could be made to compensate for the failure.

During his design process a designer might consider only one failure mode of the component since most components are usually selected for a single purpose. By doing an FMEA, he is forced to look at other failure modes (fails open, short, high ripple, low voltage level, high voltage level, etc) of the component that could cause entirely different effects on the system.

A3.2.2 Mechanics of the FMEA. The system under analysis is described. It is then represented in a functional block diagram and analyzed. The boundaries of

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Table A1
Generic Part Failure Rate and Failure Mode Classification

Component Identification	Failure Rate* (failures per 10^6 h)	Failure Mode: Open (percent)	Short (percent)	High (percent)	Low (percent)	Off (percent)	On (percent)	Other
AC or dc relay	5.0	90 (trip)	10 (no trip)					
Alarm unit (bistable trip unit)	5.3					83	17	
DC power supply	21.0			20	20	60		
Pressure transmitter	0.02			35	65			
Circuit breaker	1.8	42	35		(unable to reset 23 percent)			
Test point, resistor	1.0	90	10					
Switch DPDT	0.1	67	33					

*Estimated failure rates for use in illustrative examples only.

Not for Resale

the system are defined and the level established at which the analysis is done. Accordingly, the work is recorded on worksheets for documentation and tabulation of results.

A3.2.2.1 System Description for the FMEA. The typical reactor trip function to be evaluated is a system that monitors pressure P_M, and when a set-point P_S is exceeded ($P_M > P_S$), it initiates protective action (trip). This system is defined by the diagram in Fig 1 and operates as described in 4.4.1. It is again shown in Fig A1. The system has redundant features in its design to allow for single failure. These features are characterized by three channels for sensing pressure and two trip paths, which develop the proper coincidence logic (2/3), for initiating trip. The three channels are redundant, identical, and independent. They continuously measure pressure and automatically start channel trip when $P_M > P_S$. The two trip paths are redundant, identical, and independent. They automatically open circuit breakers (trip) when a 2/3 coincidence logic exists for channel trip. The system is testable at the channels, trip paths, and trip circuit breaker levels of design with appropriate built-in test interfaces. These test circuits are shown in diagram form. The channels are tested individually by inserting a test signal in the measurement loop, and the trip breakers are tested by actuating them with a test signal. Each trip breaker (52RTA) is bypassed (52BYA) during the test, while the other (52RTB) is maintained for protective action.

A3.2.2.2 Functional Block Diagram for the FMEA. As a starting point, the functional block diagram is a useful illustration for doing the work. It shows the logical arrangement of components in the design for the protective system to operate as required. The function of the system could be described in terms of the function of each block in its makeup. The description of the principal components and their primary functions are given in Table A2. Each component used in the system is selected with a specific function in mind. This function is chosen for proper circuit operation at the particular level of design. In the course of doing the analysis, one determines the effects of failure on the function of the components at the various system levels of design, that is, component, pressure transducer; subsystem, channel; system, protective system. He can then factor this information into the models of his system and treat them accordingly.

A3.2.2.3 System Boundary and Level of Analysis for the FMEA. As in any analysis, it is necessary that the boundaries of the system be clearly defined and that the level of detail of the analysis be established. The boundaries and definitions may vary depending upon the timing of the analysis. These conditions should be stated in order to understand the extent of the analysis and to properly interpret the results of the work.

The boundary of the system for analysis is shown by the dotted line in Fig A1. All components contained within the dotted line were included in the study and those outside were excluded. By "those outside" is meant external interfacing items rather than components of the system itself; they are shown to illustrate the interrelationship between components, or systems, in the plant, that is, motor-generator sets and rod-control-power supply.

The level of detail of the analysis is according to the replaceable component level in the system. Some of these components can be represented by a piece-part, while

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Table A2
Principal Design Components and Their Primary Function

Item	Name	Function
Channel 1		
1	Pressure transmitter, PT-1	Convert pressure to analog current
2	DC power supply, PQ-1	Provide power for analog current loop
3	Alarm unit, PC-1	Remove ac power to relays for $P_M > P_S$
4	AC control relay, X1A	Breaks circuit to dc relay in trip path *A* on trip for channel 1
5	AC control relay, XLB	Breaks circuit to dc relay in trip path *B* on trip for channel 1
6	Alarm test lamp, L-1	Indicates trip in channel
7	Test jack/test switch	Inserts test signal in measurement loop
8	Test jack signal buffer	Converts analog current to test voltage
9	Test trip switch	Bypass channel for test
Channel 2	Same as channel 1	
Channel 3	Same as channel 1	
Trip path *A*		
28	DC control relay RT1A	Breaks half-circuit to circuit breakers 52/RTA, 52/BYB
29	DC control relay RT2B	Breaks other half-circuit to circuit breakers 52/RTA, 52/BYB
30	Circuit breaker 52/RTA	Interrupts portion of power path from motor—generator to rod control power supply
31	Bypass breaker 52/BYB	Bypass circuit breaker 52/RTB when 52/RTB is tested
Trip path *B* (same as trip path *A*)		

Not for Resale

others are represented by functional black boxes. An example of these parts are a pressure transducer (*PT*-1), power supply (*DC*-1), alarm unit (*PC*-1), relay (*X*1*A*), etc. The power supply (*DC*-1) and alarm unit (*PC*-1) are analyzed as a functional black box. The development of their failure modes to the next lower level of component detail is not necessary to adequately assess system performance.

A3.2.2.4 FMEA Worksheet. The analysis is recorded on the worksheets (Table A3). The FMEA worksheets provide a systematic layout for tabulating information, keeping track of the analysis, and documenting the results. The format is specifically designed to serve this purpose.

The analysis is conducted by identifying components in the subsystem, listing their failure modes, and studying their effects on system performance. Each component selected for analysis is identified in Table A1 and shown in Fig A1.

The following is a description of each entry in the worksheet. .

(1) *Diagram.* The diagram shows the functional relationship between each item under investigation in the analysis.

(2) *Name.* Each item in Fig A1 is identified by a name. The analysis is conducted at this equipment level.

(3) *Failure Mode.* All significant failure modes, including both random and degradation failures, of the item are evaluated.

(4) *Cause.* The most predictable cause associated with each failure mode is listed. These causes are generally related to the next lower echelon of equipment breakdown and to the circuit and principal environmental parameter sources.

(5) *Symptom and Local Effects Including Dependent Failures.* The immediate consequence of each failure mode, along with a dependent failure or secondary side effects resulting from the possible cause, is determined. These symptoms are generally examined to one level higher than the item that has failed.

(6) *Method of Detection.* This entry lists the mechanism within the system that detected or indicated the occurrence of the failure mode. The failure effect could be annunciating or nonannunciating to the operator. If it is nonannunciating, the means by which the operator can detect the failure, such as use of external test equipment, periodic performance check, etc, are listed.

(7) *Inherent Compensating Provisions.* This entry lists the existing circuitry within the block (diagram) that will compensate for the failure mode and the level being analyzed. It excludes redundant circuitry in other parts of the system, unless so identified.

(8) *Effects Upon:* _____. This entry lists the ultimate effect of the failure mode on the next higher level of equipment breakdown than in the "system and local effects" entry.

(9) *Remarks and Other Effects.* This entry lists the effects of this particular system on the overall system performance. Effects that may not be recognized locally, but can be observed on a system level, including interfacing systems are entered in this column.

In doing this type of work, one questions the extent the design meets the criteria. One example of this question and answer exercise is found in line 1 of the worksheet and could go as follows:

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Table A3
Failure Mode and Effects Analysis

Functional Level
System Typical Reactor Trip Function
Subsystem Sensor Circuit 1
Equipment _____

Diagram
See Fig A1

Program Typical Plant
Report No IEEE Std 352-1975, Appendix
Prepared By _____
Date _____ Rev _____

No	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon: RPS	Remarks and Other Effects
1	Pressure transmitter PT-1	Fail low	Corrosion wear, mechanical damage, heat effects	Low output to alarm unit; ac relays will remain energized for channel 1	Periodic test	Redundant channels, 2 and 3	Both trip paths 2/2 logic	Possible immediate detection
		Fail high	Misadjustment	High signal level to alarm unit; ac relays will deenergize for channel 1, with no trip	Periodic test	Redundant channels, 2 and 3	Both trip paths 1/2 logic	Partial trip alarm
2	DC power	Fail low or OFF	Transformer failure, diode failure	Removes operating power for transducer; alarm unit will sense low pressure; ac relay will open will open with no trip on channel 1	Periodic test, spurious trip alarm	Redundant channels, 2 and 3	Both trip paths 1/2 logic	Spurious trip if other channel failed 1/2
		Fail high	Heat effects, misadjustment	Transducer setpoint exceeds trip level; relays will remain energized for channel 1	Periodic test	Redundant channels, 2 and 3	Both trip paths 2/2 logic	
3	Alarm unit PC1	Fail OFF	Transformer failure open circuit in output section, setpoint drift	AC power to ac relays removed for channel 1; ac relay open when no trip on channel 1	Periodic test, spurious trip alarm light	Redundant channels, 2 and 3	Both trip paths 1/2 logic	Spurious trip if other channel failed 1/2
		Fail ON	Short in output, section, setpoint drift	Does not remove ac power to ac relay for channel 1 trip; ac relay remains energized. Both paths become 2/2 logic	Periodic test	Redundant channels, 2 and 3	Both trip paths 2/2 logic	
4	AC control relay, X1A	Fail closed	Contacts shorted or fused armature jammed wiring	Does not break circuit to dc relays on trip; dc relay remains energized for channel 1; trip path *A* becomes 2/2 instead of 2/3 logic	Periodic test	Redundant channels, 2 and 3	Degraded trip, trip path *A*, 2/2 logic	
		Fail open	Loss of ac power (instrument bus), coil failure broken wire or loose connection	DC relay opens when no trip on channel 1	Spurious trip on test	Redundant channels, 2 and 3	Both trip paths 1/2 trip logic	Spurious trip if other channel fails 1/2

Not for Resale

352-87
4805702 0008237 5
ANSI/IEEE
Std 352-1987

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Table A3 *(continued)*

Functional Level
System Typical Reactor Trip Function
Subsystem Sensor Circuit 1 (continued)
Equipment

Diagram
See Fig A1

Program Typical Plant
Report No IEEE Std 352-1975, Appendix
Prepared By
Date Rev

No	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon: RPS	Remarks and Other Effects
5	AC control relay X1B	Fail closed	Contacts shorted or fused armature jammed wiring	Does not break circuit to dc relays on trip; dc relay remains energized for channel 1; trip path 3 becomes 2/2 instead of 2/3 logic	Periodic test	Redundant channels, 2 and 3	Degraded trip, trip Path *B*, 2/2 logic	
		Fail open	Loss of ac power (instrument bus), coil failure, broken wire or loose connection	DC relay opens when no trip on channel 1	Spurious trip on test	Redundant channels, 2 and 3	Both trip paths 1/2 trip logic	Spurious trip if other channel fails 1/2
6	Alarm test lamp L1	Open	Age	No visual indication of circuit operation during test	No light during test	N/A	Nuisance	
7	Test jack test switch	Fail open	Contact resistance, mechanical failure	Unable to insert test signal in channel 1 measurement loop	No test status	N/A	Nuisance	
		Fail short contacts remain in test position	Mechanical failure, contact pitted	Unable to connect pressure transducer PT-1 back into circuit after periodic test; alarm unit senses low pressure and ac relays open with no trip on channel 1	Trip alarm	Redundant channels, 2 and 3	Both trip paths, 1/2 logic	
8	Test jack signal input buffer	Drift	Aging	Erroneous input signal level to alarm unit during test	Test signal level comparison to channels 2 and 3	N/A	Both trip paths, 1/2 logic	
9	Test trip switch	Open	High contact resistance, mechanical failure	Lamp position — unable to get light verification of trip during test	Visual	N/A	Nuisance	
				Channel position — ac power to ac relays removed for channel 1; ac relay open when no trip on channel 1	Trip alarm light	Redundant channels, 2 and 3	Both trip paths, 1/2 logic	

Not for Resale

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Table A3 *(continued)*

Functional Level
System Typical Reactor Trip Function
Subsystem Sensor Circuit 2
Equipment _____

Diagram
See Fig A1

Program Typical Plant
Report No IEEE Std 352-1975, Appendix
Prepared By _____
Date _____ Rev _____

No	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon: RPS	Remarks and Other Effects
10	Pressure transmitter PT-2	Fail low	Corrosion wear, mechanical damage, heat effects	Low output to alarm unit; ac relays will remain energized for channel 2	Periodic test	Redundant channels, 1 and 3	Both trip paths 2/2 logic	Possible immediate detection
11	DC power supply PT-2	Fail high	Misadjustment	High signal level to alarm unit, ac relays will deenergize for channel 2 with no trip	Periodic test	Redundant channels, 2 and 3	Both trip paths 1/2 logic	Partial trip alarm
		Fail low or OFF	Transformer failure, diode failure	Removes operating power for transducer; alarm unit will sense low pressure; relay will open with no trip on channel 2	Periodic test, spurious trip alarm	Redundant channels, 1 and 3	Both trip paths 1/2 logic	Spurious trip if other channel failed 1/2
		Fail high	Heat effects, misadjustment	Transducer setpoint exceeds trip level; relays will remain energized for channel 2	Periodic test	Redundant channels, 1 and 3	Both trip paths 2/2 logic	
12	Alarm unit PC-2	Fail OFF	Transformer failure open circuit in output section, setpoint drift	AC power to ac relays removed for channel 2; ac relay open when no trip on channel 2	Periodic test, spurious trip alarm light	Redundant channels, 1 and 3	Both trip paths 1/2 logic	Spurious trip if other channel failed 1/2
		Fail ON	Short in output section	Does not remove ac power to ac relay for channel 2 trip; ac relay remains energized; both paths become 2/2 logic	Periodic test	Redundant channels, 1 and 3	Both trip paths 2/2 logic	
13	AC control relay X2A	Failed closed	Contacts shorted or fused, armature jammed wiring fault	Does not break circuit to dc relays on trip; dc relay remains energized for channel 2; trip path *A* becomes 2/2 instead of 2/3 logic	Periodic test	Redundant channels, 1 and 3	Degraded trip, trip path *A* 2/2 logic	
		Fail open	Loss of ac power (instrument bus), coil failure, broken wire or loose connection	DC relay opens when no trip on channel 2	Spurious trip on test	Redundant channels, 1 and 3	Both trip paths 1/2 trip logic	Spurious trip if other channel fails 1/2

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Table A3 *(continued)*

Functional Level

System Typical Reactor Trip Function

Subsystem Sensor Circuit 2 (continued)

Equipment _____

Diagram

See Fig A1

Program Typical Plant

Report No IEEE Std 352-1975, Appendix

Prepared By _____

Date _____ Rev _____

No	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon: RPS	Remarks and Other Effects
14	AC control relay X2	Fail closed	Contacts shorted or fused, armature jammed wiring fault	Does not break circuit to dc relays on trip; dc relay remains energized for channel 2; trip path *B* becomes 2/2 instead of 2/3 logic	Periodic test	Redundant channels, 1 and 3	Degraded trip, trip path *B* logic	
		Fail open	Loss of ac power (instrument bus), coil failure, broken wire or loose connection	DC relay opens when no trip on channel 2	Spurious trip on test	Redundant channels, 1 and 2	Both trip paths 1/2 trip logic	Spurious trip if other channel fails 1/2
15	Alarm test lamp L1	Open	Age	No visual indication of circuit operation during test	No light during test	N/A	Nuisance	
16	Test jack test switch	Fail open	Contact resistance, mechanical failure	Unable to insert test signal in channel 2 measurement loop	No test status	N/A	Nuisance	
		Fail short	Mechanical failure, contact pitted	Unable to connect pressure transducer PT-2 back into circuit after periodic test alarm unit senses low pressure and ac relays open with no trip on channel 1	Trip alarm	Redundant channels, 1 and 3	Both trip paths 1/2 logic	
17	Test jack signal input buffer	Drift	Aging	Erroneous input signal level to alarm unit during test	Test signal level comparison to channels 1 and 3	N/A	Both trip paths 1/2 logic	
18	Test trip switch	Open	High contact resistance, mechanical failure	Lamp position — unable to get light verification of trip during test	Visual	N/A	Nuisance	
				Channel position — ac power to ac relays removed for channel 2 ac relay open when no trip on channel 2	Trip alarm light	Redundant channels, 1 and 3	Both trip path 1/2 1 and 3	

Not for Resale

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Table A3 *(continued)*

Functional Level
System Typical Reactor Trip Function
Subsystem Sensor Circuit 3
Equipment _____

Diagram
See Fig A1

Program Typical Plant
Report No IEEE Std 352-1975 Appendix A
Prepared By _____
Date _____ Rev _____

No	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon: RPS	Remarks and Other Effects
19	Pressure transmitter PT-3	Fail low	Corrosion wear, mechanical damage, heat effects	Low output to alarm unit; ac relays will remain energized for channel 3	Periodic test	Redundant channels, 1 and 2	Both trip paths 2/2 logic	Possible immediate detection
		Fail high	Misadjustment	High signal level to alarm unit; ac relays will deenergize for channel 3 with no trip	Periodic test	Redundant channels, 1 and 2	Both trip paths 1/2 logic	Partial trip alarm
20	DC power supply PT-3	Fail low or OFF	Transformer failure, diode failure	Removes operating power for transducer; alarm unit will sense low pressure; ac relay will open with no trip on channel 3	Periodic test, spurious trip alarm	Redundant channels, 1 and 2	Both trip paths 1/2 logic	Spurious trip if other channel failed 1/2
		Fail high	Heat effects, misadjustment	Transducer setpoint exceeds trip level; relays will remain energized for channel 3	Periodic test	Redundant channels, 1 and 2	Both trip paths 2/2 logic	
21	Alarm unit PC 3	Fail OFF	Transformer failure, open circuit in output section, setpoint drift	AC power to ac relays removed for channel 3; ac relay open when no trip on channel 3	Periodic test, spurious trip alarm light	Redundant channels, 1 and 2	Both trip paths 1/2 logic	Spurious trip if other channel failed 1/2
		Fail ON	Short in output section, setpoint drift	Does not remove ac power to ac relay for channel 3 trip, ac relay remains energized; both paths become 2/2 logic	Periodic test	Redundant channels, 1 and 2	Both trip paths 2/2 logic	
22	AC control relay X3A	Fail closed	Contacts shorted or fused amature jammed wiring fault	Does not break circuit to dc relays on trip; dc relay remains energized for channel 3; trip path *A* becomes 2/2 instead of 2/3 logic	Periodic test	Redundant channels, 1 and 2	Degraded trip, trip path *A* 2/2 logic	
		Fail open	Loss of ac power (instrument bus), coil failure, broken wire or loose connection	DC relay opens when no trip on channel 3	Spurious trip on test	Redundant channels, 1 and 2	Both trip paths 1/2 trip logic	Spurious trip if other channel fails 1/2

Not for Resale

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Table A3 *(continued)*

Functional Level

System Typical Reactor Trip Function

Subsystem Sensor Circuit 3 (continued)

Equipment _____

Diagram

See Fig A1

Program Typical Plant

Report No IEEE Std 352-1975, Appendix

Prepared By _____

Date _____ Rev _____

No	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon: RPS	Remarks and Other Effects
23	AC control relay X3B	Fail closed	Contacts shorted or fused armature jammed wiring fault	Does not break circuit to dc relays on trip; dc relay remains energized for channel 3, trip path *B* becomes 2/2 instead of 2/3 logic	Periodic test	Redundant channels, 1 and 2	Degraded trip, trip path *B* 2/2 logic	
		Fail open	Loss of ac power (instrument bus), coil failure, broken wire or loose connection	DC relay opens when no trip on channel 3	Spurious trip on test	Redundant channels, 1 and 2	Both trip paths 1/2 trip logic	Spurious trip if other channel fails 1/2
24	Alarm test lamp L1	Open	Age	No visual indication of circuit operation during test	No light during test	N/A	Nuisance	
25	Test jack test switch	Fail open	Contact resistance, mechanical failure	Unable to insert test signal in channel 3 measurement loop	No test status	N/A	Nuisance	
		Fail short contacts remain in test position	Mechanical failure, contact pitted	Unable to connect pressure transducer PT-3 back into circuit after periodic test; alarm unit senses low pressure and ac relays open with no trip on channel 3	Trip alarm	Redundant channels, 1 and 2	Both trip paths 1/2 logic	
26	Test jack signal input buffer	Drift	Aging	Erroneous input signal level to alarm unit during test	Test signal level comparison to channels 1 and 2	N/A	Both trip paths 1/2 logic	
27	Test trip switch	Open	High control resistance, mechanical failure	Lamp position — unable to get light verification of trip during test	Visual	N/A	Nuisance	
				Channel position — ac power to ac relays removed for channel 3 ac relay open when no trip on	Trip alarm light	Redundant channels, 1 and 2	Both trip path 1/2 logic	

Not for Resale

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

352-87 4805702 0008243 0

Table A3 *(continued)*

Functional Level
System Typical Reactor Trip Function
Subsystem Trip Path *A*
Equipment ____

Diagram
See Fig A1

Program Typical Plant
Report No IEEE Std 352-1975, Appendix
Prepared By ____
Date ____ Rev ____

No	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon: RPS	Remarks and Other Effects
28	DC control relay RT1A	Fail closed	Contacts shorted or fused armature jammed wiring fault	Circuit breaker 52RTA, BY; remains closed for trip path *A*; trip is 1/1	Periodic test	Trip path *B*	Loss of 1/2 trip path	
		Fail open	Loss of dc control power coil failure	Circuit breakers 52RTA, BY; opens for no trip, spurious trip in path *A*	Spurious trip control room alarm	N/A	Nuisance	Alarm in control room
			Broken contacts broken wire or loose connection	Same	Same	Same	Same	Same
29	DC control relay RT2A	Fail closed	Contacts shorted or fused armature jammed wiring fault	Circuit breaker 52RTA, BY; remains closed for trip path *A*; trip logic is 1/1	Periodic test	Trip path *B*	Loss of 1/2 trip path	
		Fail open	Loss of dc control power coil failure	Circuit breakers 52RTA, BY; opens for no trip, spurious trip in path *A*	Spurious trip control room alarm	N/A	Nuisance	Alarm in control room
			Broken contacts broken wire or loose connection	Same	Same	Same	Same	Same
30	Circuit breaker 52RTA	Fail closed	Jam mechanism UV trip attachment mechanism stuck fuse main contacts	Trip path *A* inoperative trip 1/1 logic for *B* path	Periodic test	N/A	Loss of 1/2 trip logic	
		Fail open	Loss of dc control power UV coil failure worn trip latch	Path *A* in trip state could result in spurious trip	Spurious trip	N/A	Nuisance	Immediate detection
31	Circuit breaker 52BYB	Fail closed	Jam mechanism UV trip attachment mechanism stuck fuse main contacts	Trip path *A* inoperative trip 1/1 logic for *B* path	Periodic test	N/A	Loss of 1/2 trip logic	
		Fail open		Loss of dc control power UV coil failure worn trip latch	Path *A* in trip state, could result in spurious trip	N/A	Nuisance	Immediate detection

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Table A3 *(continued)*

Page ____ of ____

Functional Level
System Typical Reactor Trip Function
Subsystem Trip Path *B*
Equipment

Diagram
See Fig A1

Program Typical Plant
Report No IEEE Std 352-1975, Appendix
Prepared By
Date Rev

No	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon: RPS	Remarks and Other Effects
32	DC control relay RT1B	Fail closed	Contacts shorted or fused armature jammed wiring fault	Circuit breaker 52RTB, BYA remains closed for trip; path *B* trip logic is 1/1	Periodic test	Trip path A	Loss of 1/2 trip path	
		Fail open	Loss of dc control, power coil failure	Circuit breakers 52TRB, BYA opens for no trip; spurious trip in path *B*	Spurious trip control room alarm	N/A	Nuisance	Alarm in control room
			Broken contacts broken wire or loose connection	Same	Same	Same	Same	Same
33	DC control relay RT2	Fail closed	Contacts shorted or fused armature jammed wiring fault	Circuit breaker 52RT, BYA; remains closed for trip path *B*, trip logic is 1/1	Periodic test	Trip path A	Loss of 1/2 trip path	
		Fail open	Loss of dc control power coil failure	Circuit breakers 52RTB, BYA opens for no trip, spurious trip in path *B*	Spurious trip control room alarm	N/A	Nuisance	Alarm in control room
			Broken contacts broken wire or loose connection	Same	Same	Same	Same	Same
34	Circuit breaker 52/BYA	Fail closed	Jam mechanism UV trip attachment mechanism stuck fuse main contacts	Trip path *B* inoperative trip 1/1 logic for path *A*	Periodic test	N/A	Loss of 1/2 trip logic	
		Fail open	Loss of dc control power UV coil failure worn trip latch	Path *B* in trip state, could result in spurious trip	Spurious trip	N/A	Nuisance	Immediate detection
35	Circuit breaker 52/RTB	Fail closed	Jam mechanism UV trip attachment mechanism stuck fuse main contacts	Trip path *B* inoperative trip 1/1 logic for path *A*	Periodic test	N/A	Loss of 1/2 trip patch	
		Fail open	Loss of dc control power UV coil failure worn trip latch	Path *B* in trip state, could result in spurious trip	Spurious trip	N/A	Nuisance	Immediate detection

Not for Resale

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Table A3 *(continued)*

Functional Level

System _____

Subsystem _____

Equipment _____

_____

_____

Diagram

Program _____

Report No _____

Prepared By _____

Date _____ Rev _____

No	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon:	Remarks and Other Effects
10—18	Sensor	Channel 2		Same as channel 1				
19—27	Sensor	Channel 3		Same as channel 1				
32—35	Trip path *B*			Same as trip path *A*				

Not for Resale

352-87
4805702 0008245 4
ANSI/IEEE
Std 352-1987

(1) How can the pressure transducer fail? Fail low.
(2) What could cause it? Corrosion, mechanical damage.
(3) What will be its effects? Causes low output to alarm unit and ac relay will remain energized for channel.
(4) If it occurs will it be annunciating? No.
(5) If it is not annunciating, can it be detected? Yes.
(6) How? Periodic test.
(7) Can the system compensate for this single failure? Yes, redundant channels 2, 3.
(8) Will this single failure fail the system? No.
(9) Then how will it degrade it? Makes both trip paths 2/2 logic, etc.

A3.2.3 Results of FMEA. The results of the analysis are used to assess the extent to which the system complies with the criteria. From the worksheets, listings can be made with information about failure modes that cause various sytem effects, the existence of components or portions of the system for operation if a single failure occurs, and the means by which failures can be detected or annunciated.

A3.2.3.1 Failure Modes, Effects Identification. The various ways in which the system could fail are found in the worksheets (Table A3). The major ones are listed in Table A4.

By observation of this table, one can determine the different effects a component failure has on the system for its different failure modes, for example, if alarm unit *PC*-1 fails OFF, both trip paths become 1/2 logic (vice 2/3); if it fails ON, both trip paths become 2/2 logic (vice 2/3). Furthermore, one can also observe similar failure effects due to different components, that is, *spurious trip*: ac control relay *open*, dc control relay *open*.

Table A4 lists failure effects caused by the component failure mode according to the severity level of the failure modes. The severity notation shown in the table is only one example and can be adapted to fit the purpose of the analysis and the criteria appropriate to the system for which the failure mode is being considered. This information combined with rough estimates of the relative likelihood of various failures can guide a designer to concentrate his efforts in the most significant areas.

A3.2.3.2 Availability of System Components. The results of the FMEA can be given in terms of the operating states of the subsystem for single-failure conditions. A summary of these results is shown in Table A5. This table presents subsystems within the system that are operating during normal conditions. The subsystems are arranged in the columns of the table, and the single components in the rows. The subsystem operating status is shown for each single-failure condition listed.

Two symbols are used in the table to indicate operating status. These symbols are "+" for operating or available, or "0" for nonoperating or not available. The effects of a single failure are shown in terms of a "+" or a "0" for subsystems in the system. When represented by a "-" the subsystem is operative or available and is unaffected by the failure, and when represented by a "0" the subsystem is inoperative or unavailable as a direct result of the failure. For example, if power supply *PQ*-1

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Table A4
Summary of Failure Modes and Effects

Component	Failure Mode	Failure Effect				
		Spurious Trip	One Path 2/2	Both Path 1/2	Trip 1/1	Both Path 2/2
Trip function circuit breaker	Closed	—	—	—	At	—
	Open	A	—	—	—	—
Trip path dc control relay	Closed	—	—	—	At	—
	Open	A	—	—	—	—
Coincident logic ac control relay	Closed	—	—	A	—	—
	Open	A	—	—	—	—
Sensing circuit alarm unit	Off	—	—	A	—	—
	On	—	—	—	—	At
DC power supply	Low or off	—	—	—	—	At
	High	—	—	A	—	—
Pressure transmitter	Low	—	—	—	—	At
	High	—	—	A	—	—

—: Not applicable result of component fault.

A: Acceptable system state regardless of detectability.

At: Acceptable because detectable by planned periodic testing.

Not for Resale

4805702 0008248 0

Table A5
Summary of Results

Single-Failure Item	Sensor Channel			Coincidence Logic *A*			Path	Coincidence Logic *B*			Path	Trip RT	
	A	*B*	*C*	1—2	1—3	2—3	*A*	1—2	1—3	2—3	*B*	*A*	*B*
Circuit breaker													
52RTA	+*	+	+	+	+	+	+	+	+	+	+	0	+
52RTB	+	+	+	+	+	+	+	+	+	+	+	+	0
Relay													
RT1A	+	+	+	+	+	+	0	+	+	+	+	0	+
RT2A	+	+	+	+	+	+	0	+	+	+	+	0	+
RT1B	+	+	+	+	+	+	+	+	+	+	0	+	0
RT2B	+	+	+	+	+	+	+	+	+	+	0	+	0
X1A	+	+	+	0	0	+	+	+	+	+	+	+	+
X1B	+	+	+	+	+	+	+	0	0	+	+	+	+
X2A	+	+	+	0	+	0	+	+	+	+	+	+	+
X2B	+	+	+	+	+	+	+	0	+	0	+	+	+
X3A	+	+	+	+	0	0	+	+	+	+	+	+	+
X3B	+	+	+	+	+	+	+	+	0	0	+	+	+
Alarm													
PC1	0†	+	+	0	0	+	+	0	0	+	+	+	+
PC2	+	0	+	0	+	0	+	0	+	0	+	+	+
PC3	+	+	0	+	0	0	+	+	0	0	+	+	+
Power supply													
PQ1	0	+	+	0	0	+	+	0	0	+	+	+	+
PQ2	+	0	+	0	+	0	+	0	+	0	+	+	+
PQ3	+	+	0	+	0	0	+	+	0	0	+	+	+
XMTR													
PT1	0	+	+	0	0	+	+	0	0	+	+	+	+
PT2	+	0	+	0	+	0	+	0	+	0	+	+	+
PT3	+	+	0	+	0	0	+	+	0	0	+	+	+

*+: Available when required.
†0: Not available when required.

Not for Resale

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

failed, sensor channel *A* will be unavailable; coincidence logic 1-2, 1-3, in logic *A* and 1-2, 1-3 in logic *B* will be unavailable. The table is set up such that for a given single failure (listed in the left column) one can read across the table and determine which items remain operating in the system. From this data one can identify the number of components operating in the systems for $P_M > P_S$ using the single-failure criteria.

A3.2.3.3 Failure Detectability. The information in the FMEA will indicate to the designer the failure modes of components that must be detected by test or annunciation. This information is useful in determining compliance with applicable criteria. Table A6 is a listing of failure modes that are not annunciated and can only be detected by test. With this information, the designer can develop his test plan to detect failed components as well as to verify performance of operation.

A3.3 Common-Mode-Failure Analysis. In a reliability analysis, it is not sufficient to consider only random component failures. Also of concern is the possibility of system malfunctions termed systematic or *common-mode* failures. These cause system failure through simultaneous deficiency in several system components. Where the simultaneous deficiencies arise from a single source such as faulty design, inadequate maintenance, etc, the resulting loss of system function is called common-mode failure.

Common-mode failures are subject to qualitative analytical techniques using either fault tree or FMEA techniques. These techniques are useful to identify the combinations of component malfunctions or the conditions leading to system failure. It then remains necessary to assess the susceptibility of the system to failure from each combination considering the acting causative factors and the preventative measures taken. The following example typifies one method using fault trees to obtain failure combinations and matrices to tabulate the evaluation.

A3.3.1 Failure Combinations. As with any system failure, common-mode failures arise only when certain associated functions are not performed. If, for this

Table A6
Nonannunciating Failures Detectable by Test

Name	Failure Mode
Channel 1	
Pressure transmitter PT-1	Fail high
DC Power	Fail high
Alarm unit PC-1	Fail on
AC control relay X1A	Fail closed
AC control relay X1B	Fail closed
Channel 2, 3 (same as channel 1)	
Trip path *A*	
DC control relay RT1A	Fail closed
DC control relay RT2A	Fail closed
Circuit breaker 52RTA	Fail closed
Circuit breaker 52BYB	Fail closed
Trip path *B* (same as trip path *A*)	

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

example, one assumes that the typical trip function shown in Fig 1 is the entire system, and that no others act, a table can be made to summarize the situation (Table A7).

A3.3.2 Causative Factors. Identification of the important causative factors to be considered is the next step in the analysis. Five general categories of causes are identified in connection with common-mode failure.

(1) *External Normal Environment*
- (a) dust, dirt
- (b) temperature
- (c) humidity, moisture
- (d) vibration
- (e) electrical interference

(2) *Design Deficiency*
- (a) unrecognized interdependence between "independent" subsystems, components
- (b) unrecognized electrical or mechanical dependence on common elements
- (c) dependence on equipment or parameters whose failure or abnormality causes need for protection

(3) *Operation and Maintenance Errors*
- (a) miscalibration
- (b) inadequate or improper testing
- (c) outdated instructions or prints
- (d) carelessness in maintenance
- (e) other human factors

(4) *External Catastrophe*
- (a) tornado
- (b) fire
- (c) flood
- (d) earthquake

(5) *Functional Deficiency*
- (a) misunderstanding of process variable behavior
- (b) inadequacy of designed protective action
- (c) inappropriate instrumentation

A3.3.3 Preventative Measures. Redundancy forms the principal insurance against random failures in that the probability of several redundant components all failing together from random causes can be made very small.

However, redundancy alone does not solve the common-mode-failure problem. A combination of many measures is useful in dealing with these failures. Functional diversity, physical separation, inspection, testing, safe failure mode, and administrative controls all must be taken into account in the system evaluation. Table A8 summarizes some of the useful preventative measures. Such a listing focuses the analyst's attention on this aspect of the system and is a logical basis for the step-by-step comparison to follow.

A3.3.4 Evaluation of System Susceptibility to Common-Mode Failure. Having identified potential causes of common-mode failure and available preventative measures, it remains necessary to evaluate the resulting balance sheet line by line

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

Table A7
Minimum Number of Like Functional Blocks Required to Suffer Common-Mode Failure to Prevent Automatic Reactor Trip

Transient	Component	Train	Number Affected	Number Active	Mode
Overpressure	Trip breakers	*A* and *B*	2	2	Do not open circuit
	DC relays	*A* and *B*	2	4	Do not open circuit
	AC relays	*A* and *B*	4	6	Do not open circuit
	Analog channels	*A* and *B*	2	3	Do not remove power to relay coil

NOTE: A similar tabulation can be made for combinations of unlike components.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

and assess the likelihood of common-mode failure. One means to do so is a tabular development, as illustrated in Table A9. This is simply a thorough systematic objective application of engineering judgment. For each of the combinations of functional units, the analyst must evaluate the adequacy of the preventative measures against each of the causative factors considered. In this manner, thorough assessment of the system is gained and maximum assurance can be obtained that the likelihood of common-mode failure is sufficiently low. Table A9 is a matrix for the example system showing areas of concern that must be assessed.

As an example of the type of evaluation intended consider the trip breakers, since they represent the numerically smallest of the groupings of like components.

The example case reactor trip circuit breakers are metal-enclosed three-phase air circuit breakers of the 600 V class. Two trip breakers are connected in series between the motor-generator and rod-drive power supply. One breaker is tripped by undervoltage when the *A* trip relays open the circuit in the *A* logic train and the other by the *B* train. Bypass breakers are provided for on-line testing. These breakers are interlocked to trip all breakers on simultaneous closing of both bypass breakers. As an added precaution the *A* trip signal is also wired to the *B* bypass breaker and the *B* trip signal is wired to the *A* bypass. Thus, only two

Table A8
Common-Mode-Failure Preventative Measures

Failure Category	Possible Preventative Measure
External normal environment	Functional diversity Design administrative controls Operational administrative controls Safe failure modes Proven Design Standardization Equipment diversity
Design deficiency	Functional diversity Physical separation Design administrative controls Operational administrative controls Safe failure modes
Maintenance errors	Functional diversity Operational administrative controls Equipment diversity
External catastrophe	Functional diversity Physical separation Design administrative controls Safe failure modes Equipment diversity
Functional deficiency	Functional diversity Design administrative controls Operational administrative controls Equipment diversity

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Table A9
Common-Mode-Failure Matrix Relating Causative Factors to Equipment Required Failure Modes in Reactor Protection System

	External Normal Environment				Design Deficiency				Operation and Maintenance Errors						External Catastrophy				Functional Deficiency		
Required Failure (Equipment and Mode of Failure)	Dirt	Temperature	Moisture	Vibration	Electrical Interference	Unrecognized Interdependence	Common Element	Fault Dependence	Miscalibration	Improper Testing	Outdated Prints	Careless Maintenance	Operator Error	Inadequate Training	Tornado	Fire	Flood	Earthquake	Phenomenological Misconception	Inadequate Protective Action	Inappropriate Instrumentation
Trip breakers (low-voltage metal-enclosed circuit breaker) fail to open circuit on signal	X*	X	X	X		X	X		X	X		X			X	X	X	X	X	X	X
Trip relays (dc industrial control relay) fail to open circuit on signal	X	X	X	X		X	X			X		X				X	X				X
Logic relays (ac industrial control relays) fail to open circuit on signal	X	X	X	X		X	X			X		X					X	X			X
Analog channels (pressure transducer, dc power supply, solid-state comparator/switch) fail to remove power to relay coils		X	X	X	X	X	X	X	X	X	X	X	X	X		X	X		X		X
Interconnecting wiring (shorts equivalent to above faults)											X	X		X	X	X	X				
Test circuitry (block signals to logic or test relays)										X	X	X				X	X				

*Indicates potential for common-mode failure.

Not for Resale

breakers are anticipated to be active at any time, both of which must fail to open on receipt of the trip signal.

To evaluate whether or not the common-mode causative factors could make two trip breakers fail closed, each type of cause should be considered individually. First, consider those environmental factors that lie within the extremes of the normal operating environment, that is, dust or dirt, temperature, moisture, vibration, and electrical interference.

Taking these factors in order, consider the accumulation of dust and dirt. It is not possible to build up a sufficient amount to stop the action of the main mechanism. The kick-out springs that open the main contacts are (by design) strong enough to overcome any dirt accumulation. However, a slow build-up of sticky dirt on the plunger of the undervoltage trip device could be imagined. Such deposits would have to get inside the solenoid coil during normal operation. The deposits must then harden onto the shaft in such thickness and strength that the spring force is insufficient to drive out the plunger on loss of coil voltage.

Measures taken to prevent such occurrences are physical separation and operational administrative controls. Each circuit breaker is housed in its own metal enclosure, which shelters it from airborne dirt contamination. Administrative controls include requirements for cleaning filters on ventilation units, keeping switchgear areas generally clean, and, most importantly, periodic inspection and testing of the trip breakers themselves. Furthermore, some wiping action could be expected to loosen dirt on the trip plunger during the periodic exercise or testing. Thus, common-mode failure of two trip breakers due to dirt buildup is unlikely.

A similar assessment can be made of each of the other areas of concern noted in Table A9, and any problems or recommended design, operation, or maintenance changes can be noted on a separate listing. When this study is carefully completed, one can have reasonable assurance that from an engineering point of view common-mode failure has been adequately considered.

A3.4 Quantitative Analysis. Quantitative analysis using the methods described in Section 5 can be done either with reliability block diagrams or fault trees to yield predictions of system performance. In this example, the fault tree method is used.

A3.4.1 Fault Tree Analysis. The fault tree, being a logic diagram that relates component faults to system failure, is readily adaptable to quantitative analysis. Fault tree analysis employs the principles of Boolean algebra and can be used for either reliability or availability prediction. The important thing to remember is that the probabilities associated with each event are probabilities of failure (unreliability or unavailability) and must be on a consistent basis throughout the fault tree.

Having constructed the example fault tree (Fig A2) and identified the failure probabilities for the components (Table A1), it is only necessary to associate probabilities with each fundamental event and perform the logic substitutions. For example, where there are several independent input events to AND logic, the probability of the output events is the product of the probabilities of the input events. For the case of OR logic, the probability of the output event is the logical sum of the input probabilities.

The first step in evaluating the fault tree in Fig A2 is to label each basic event. In the example the basic events are labeled with letters. By numbering each event, the

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

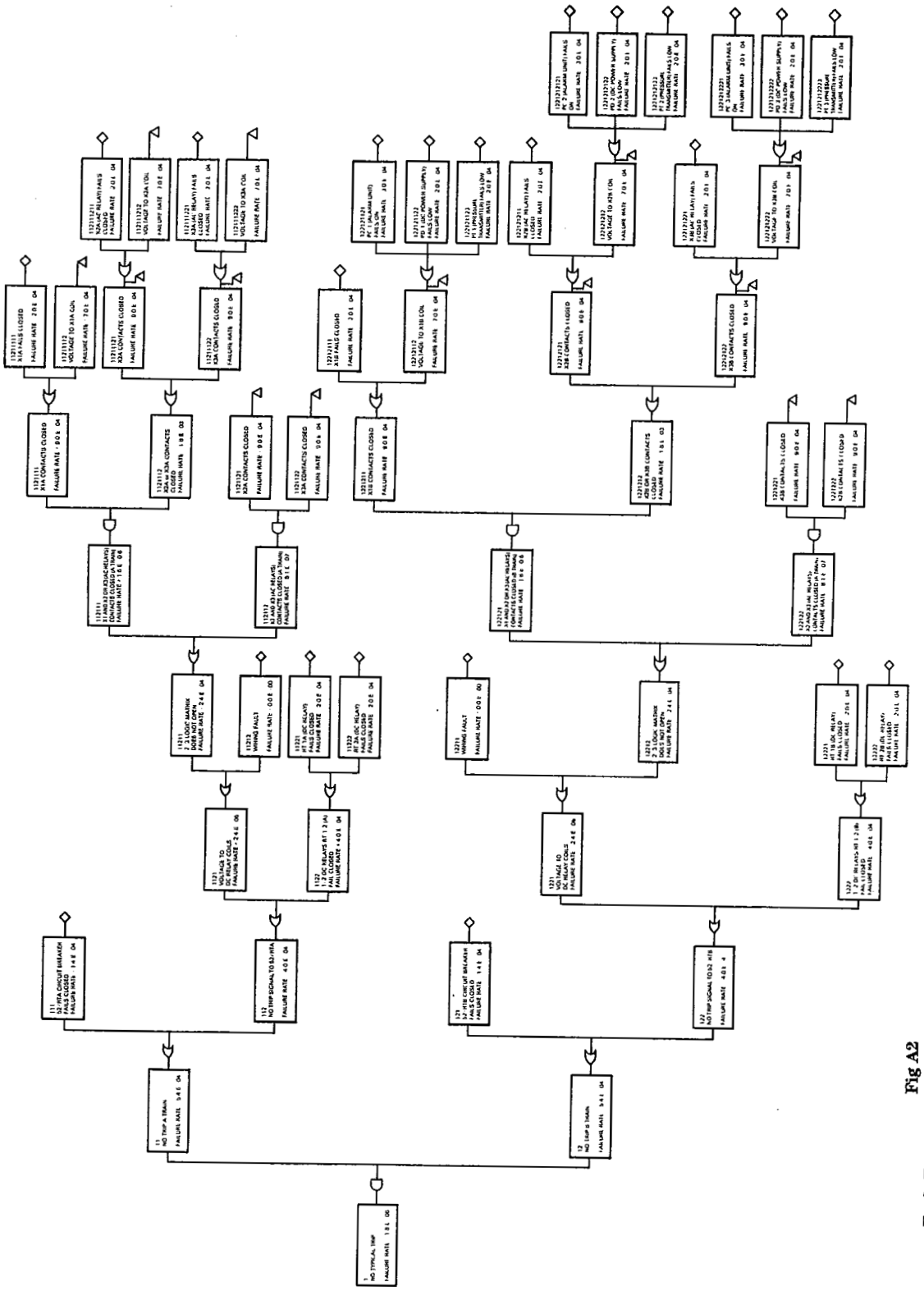


Fig A2
Fault Tree for No Typical Trip Function

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Boolean expression for every event in the fault tree can be determined. One must be cautious in making the compilations to ensure that inputs are independent from one another or at least that no two are identical. The evaluation of the tree begins at the extreme right and proceeds to the left, to the top of the tree.

Events 4, 6, 14, 15, 18, 19, 22, 23, 24, 25, 36, 40, 44, 46, 48, 49, 50, 51, 53, and 55 through 60 are basic events for which the Boolean expression is obvious.

Event 54 is the logical sum (union) of events 58, 59, and 60. The Boolean expression for event 54 is $(W + X + Y)$. It is worthy to note that event 54 is a transfer out and that it transfers in as event 47; therefore, event 47 has the same Boolean expression as event 54.

The logic and Boolean expression for each event in the fault tree is given in Table A10. AND logic is denoted by concatenation, OR logic by the symbol "+."

The failure probabilities are calculated using the failure rates in Table A1 to assess the probability of event 1 occurring in a 30-day interval. The input probabilities are as follows:

$$\begin{aligned} A, B &= 4.5 \cdot 10^{-4} \\ C, D, E, F, K, L, M, R, N, S &= 3.6 \cdot 10^{-4} \\ G, I, H, J &= 0.0 \quad [17] \\ O, T, W &= 6.5 \cdot 10^{-4} \\ P, U, X &= 3.0 \cdot 10^{-3} \\ Q, V, Y &= 1.0 \cdot 10^{-5} \end{aligned}$$

Substituting these values into the expression for event 1 yields a probability of occurrence over a 30-day interval equal to $1.48 \cdot 10^{-6}$ for the example fault tree.

A3.4.2 System Goals and Test Intervals. One, but not the only, means to handle the problem of reconciling goals, testing strategy, and system design is outlined in this example. This method utilizes the "limit consequence" approach [A1],[18] which concentrates upon a severe loss of plant protection, the consequences of which are acceptable only with an extremely small probability of occurrence. All other minor events or system failures are assessed on the basis of their contribution to the probability of the limit consequence status of the plant. The steps are as follows:

(1) Fault tree techniques are used to arrive at the combinations of system malfunctions and natural phenomena that result in limit consequence status.

(2) An acceptably small probability of achieving limit consequence is selected.

(3) System goals are apportioned such that the total plant goal can be achieved in a balanced fashion.

(4) Operating strategy and system design are adjusted as necessary to meet individual system or subsystem goals.

As an example, consider a plant wherein protective system failure can lead to limit consequences as shown in Fig A3. Once the allowable probability of a system failure, or unreliability, is allocated to the lowest levels of the fault tree, the tree can

[17] Wiring faults are assumed to be eliminated by surveillance, initial testing, and good operating practice.

[18] The numbers in brackets preceded by the letter A correspond to those of the bibliography in A4.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

be developed to include all components that are to be assigned unreliability goals and testing intervals. The 2/3 pressure sensor logic and a 3/4 level sensor logic protect against Transient No 1 (β_1).

The annual probability of a hazard chain P_h is defined as

$$P_h = \beta\bar{R} \qquad \text{(Eq A1)}$$

where β is the frequency of a single hazard occurring in one year, and

$$\beta\bar{R} \ll 1 \qquad \text{(Eq A2)}$$

where $\bar{R}$ is the probability of failure of the protection equipment provided for the hazard considered.

In a plant with n hazard chains leading to limit consequences,

$$P_h = \sum_{i=1}^{n} \beta_i \bar{R}_i$$

$$= (\beta_1 \bar{R}_1 + \beta_2 \bar{R}_2 + \cdots + \beta_n \bar{R}_n)$$

If there are no other constraints, the individual contributions to the total probability can be set equal to each other and the equation reduced. However, there may be valid reasons for other apportionments at the level of the hazard chains. Then it is necessary to develop testable subsystems or groupings in more detail.

Figure A3 will be used down to the subsystem level to allocate the goals. It contains several testable groups of devices. Goal allocation is solvable by using either a fault tree or a reliability block diagram (RBD) approach. The two approaches are logically equivalent, and the choice depends on convenience and the analyst's personal preference. Similarly, goals may be established in terms of either unreliability or unavailability.

Once the goal is chosen the values for the failure rates and assumed testing intervals are used to calculate the system or subsystem unreliability. If this is less than the goal, the system testing intervals are suitable. The test intervals may be varied as long as the goal is met.

The allowable hazard chain probability for the limit consequences of this example is set at 10^{-6} per year [A2].

For this example, the limit consequence is defined as a "failure to scram when required" coincident with a "loss of safeguards." The goal for the plant experiencing this overall limit consequence is numerically equal to $P_{h\,(\text{goal})} = G\bar{R}_0 = 10^{-6}$ per year, where G is the allowable annual probability of the "failure to scram when required" and $\bar{R}_0$ is the unreliability of the safeguard system.

It is emphasized that this is strictly an example for illustrative purposes and should not be taken as necessarily representative of any nuclear power generating station design. Actual plants may have several potential combinations, such as LOCA plus safeguards or scram failure, loss of all cooling water systems, etc, leading to limit consequences. The analysis of specific plant designs may even result in single events that by themselves constitute a limit consequence. For such cases, the results will be much more restrictive than the example presented here.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

let $\bar{R}_0 = 10^{-2}$, thus the goal for the example plant experiencing a failure to scram when required" is taken to be 10^{-4} per year.

Table A10
Logic and Boolean Expressions for Events in a Fault Tree

Event	Logic Expression	Boolean Expression
54	(58 + 59 + 60)	$(W + X + Y)$
52	(55 + 56 + 57)	$(T + U + V)$
47	54	$(W + X + Y)$
45	52	$(T + U + V)$
43	(53 + 54)	$(S + W + X + Y)$
42	(51 + 52)	$(R + T + U + V)$
41	(48 + 49 + 50)	$(O + P + Q)$
39	(46 + 47)	$(N + W + X + Y)$
38	(44 + 45)	$(M + T + U + V)$
37	41	$(O + P + Q)$
35	42	$(R + T + U + V)$
34	43	$(S + W + X + Y)$
33	(42 + 43)	$(R + T + U + V + S + W + X + Y)$
32	(40 + 41)	$(L + O + P + Q)$
31	39	$(N + W + X + Y)$
30	38	$(M + T + U + V)$
29	(38 + 39)	$(N + W + X + Y + M + T + U + V)$
28	(36 + 37)	$(K + O + P + Q)$
27	(34)(35)	$(S + W + X + Y)(R + T + U + V) = (RS + ST + SU + SV + RW + WT + UW + WV + RX + XT + XU + XV + RY + YT + YU + YV)$
26	(32)(33)	$(L + O + P + Q)(R + T + U + V + S + W + X + Y) = (LR + LT + LU + LV + LS + LW + LX + LY + OR + OT + OU + OV + OS + OW + OX + OY + PR + PT + PU + PV + PS + PW + PX + PY + QR + QT + QU + QV + QS + QW + QX + QY)$
21	(30)(31)	$(M + T + U + V)(N + W + X + Y) = (MN + MW + MX + MY + TN + TW + TX + TY + UN + UW + UX + UY + VN + VW + VX + VY)$
20	(28)(29)	$(K + O + P + Q)(N + W + X + Y + M + T + U + V) = (KN + KW + KX + KY + KM + KT + KU + KV + ON + OW + OX + OY + OM + OT + OU + OV + PN + PW + PX + PY + PM + PT + PU + PV + QN + QW + QX + QY + QM + QT + QU + QV)$
17	(26 + 27)	$(LR + LT + LU + LV + LS + LW + LX + LY + OR + OT + OU + OV + OS + OW + OX + OY + PR + PT + PU + PV + PS + PW + PX + PY + QR + QT + QU + QV + QS + QW + QX + QY + SR + ST + SU + SV + WR + WT + WU + WV + XR + XT + XU + XV + YR + YT + YU + YV)$
16	(24 + 25)	$(I + J)$
13	(22 + 23)	$(G + H)$
12	(20 + 21)	$(KN + KW + KX + KY + KM + KT + KU + KV + ON + OW + OX + OY + OM + OT + OU + OV + PN + PW + PX + PY + PM + PT + PU + PV + QN + QW + QX + QY + QM + QT + QU + QV + MN + MW + MX + MY + TN + TW + TX + TY + UN + UW + UX + UY + VN + VW + VX + VY)$

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

Table A10 *(continued)*

Event	Logic Expression	Boolean Expression
11	(18 + 19)	$(E + F)$
10	(16 + 17)	$(I + J + 17)$
9	(14 + 15)	$(C + D)$
8	(12 + 13)	$(G + H + 12)$
7	(10 + 11)	$(E + F + I + J + 17)$
5	(8 + 9)	$(C + D + G + H + 12)$
3	(6 + 7)	$(B + E + F + I + J + 17)$
2	(4 + 5)	$(A + C + D + G + H + 12)$
1	(2)(3)	$(B + E + F + I + J + 17)(A + C + D + G + H + 12) =$ $(BA + BC + BD + BG + BH + B12 +$ $EA + EC + ED + EG + EH + E12 +$ $FA + FC + FD + FG + FH + F12 +$ $IA + IC + ID + IG + IH + I12 +$ $JA + JC + JD + JG + JH + J12 +$ $17A + 17C + 17D + 17G + 17H + 17\ 12)$

Since two paths to this event are considered, the goal for each path is arbitrarily set at one-half the overall goal

$$G_1 + G_2 = 10^{-4}$$

$$G_1 = G_2 = 5 \cdot 10^{-5} \qquad \text{(Eq A3)}$$

The goals are allocated as follows. Considering the elements of the tree that make up G_1, each breaker and associated actuator will have the same characteristics as its redundant counterpart. Therefore,

$$\bar{R}_{3A} = \bar{R}_{3B} = \bar{R}_3$$

and

$$G_1 = (\bar{R}_3)^2 \sum_{i=1}^{n} \beta_1$$

solving for R_3, assuming $\sum_{i=1}^{n} \beta_1 = 0.1$,

$$\bar{R}_3 = (5 \cdot 10^{-4})^{1/2} = 2.24 \cdot 10^{-2}$$

thus,

$$\bar{R}_5 + \bar{R}_7 = 2.24 \cdot 10^{-2} \qquad \text{(Eq A4a)}$$

and with $\bar{R}_5 = \bar{R}_7$

$$\bar{R}_5 = \bar{R}_7 = 1.1 \cdot 10^{-2} \qquad \text{(Eq A4b)}$$

The elements that make up G_2 are composed of individual transient hazard rates and the unreliability of the protection subsystems protecting against each transient.

The equation for G_2 is

$$G_2 = G_{41} + G_{42} + G_{43} + G_{44} \qquad \text{(Eq A5)}$$

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

where

$G_{4i} = \beta_i \bar{R}_{6i}$

is the annual hazard probability for transient i and

$$\bar{R}_{6i} = \bar{R}_{8i} \bar{R}_{10i} \qquad \text{(Eq A6)}$$

is the failure of sensor groups used to protect against transient i.

Since the particular logic scheme (sensor group arrangement) associated with each $\bar{R}_{6i}$ will govern the test intervals to be selected, and since the sensors and sensor relays can be assumed to have the same failure rates, we can select the most limiting G_{4i} and solve for a test interval that meets all required goals.

Since

$$G_2 = 5 \cdot 10^{-5} \sum_{i=1}^{n} G_{4i}$$

letting

$$G_{41} = G_{42} = G_{43} = G_{44} = G_4 = \frac{5 \cdot 10^{-5}}{4}$$

$$G = 1.25 \cdot 10^{-5} \qquad \text{(Eq A7)}$$

since

$$G_4 = \beta_1 \bar{R}_6$$
$$= \beta_1 (\bar{R}_8 \bar{R}_{10}) = 1.25 \cdot 10^{-5}$$

In our example,

$\beta_1 = 2 \cdot 10^{-2}$ per year

then,

$$\bar{R}_6 = \frac{1.25 \cdot 10^{-5}}{2 \cdot 10^{-2}} = 6.25 \cdot 10^{-4} \qquad \text{(Eq A8)}$$

Thus, from Eq A6

$$\bar{R}_8 \bar{R}_{10} = 6.25 \cdot 10^{-4} \qquad \text{(Eq A9)}$$

We now examine the elements composing $\bar{R}_8$ and $\bar{R}_{10}$.

$\bar{R}_8 = 3(\bar{R}_9)^2$ $\qquad$ $\bar{R}_{10} = 6(\bar{R}_9)^2$

$\bar{R}_9 = \bar{R}_{11} + \bar{R}_{12}$ $\qquad$ $\bar{R}_{12} = (\bar{R}_{13})^2$

Substituting in Eq A9 we get

$$3[\bar{R}_{11} + (\bar{R}_{13})^2]^2 \, 6[\bar{R}_{11} + (\bar{R}_{13})^2]^2 = 6.25 \cdot 10^{-4}$$
$$18[\bar{R}_{11} + (\bar{R}_{13})^2]^4 = 6.25 \cdot 10^{-4}$$
$$[\bar{R}_{11} + (\bar{R}_{13})^2]^4 = 34.60 \cdot 10^{-6} \qquad \text{(Eq A10)}$$

Letting $A = \bar{R}_{11} + (\bar{R}_{13})^2$, we have

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

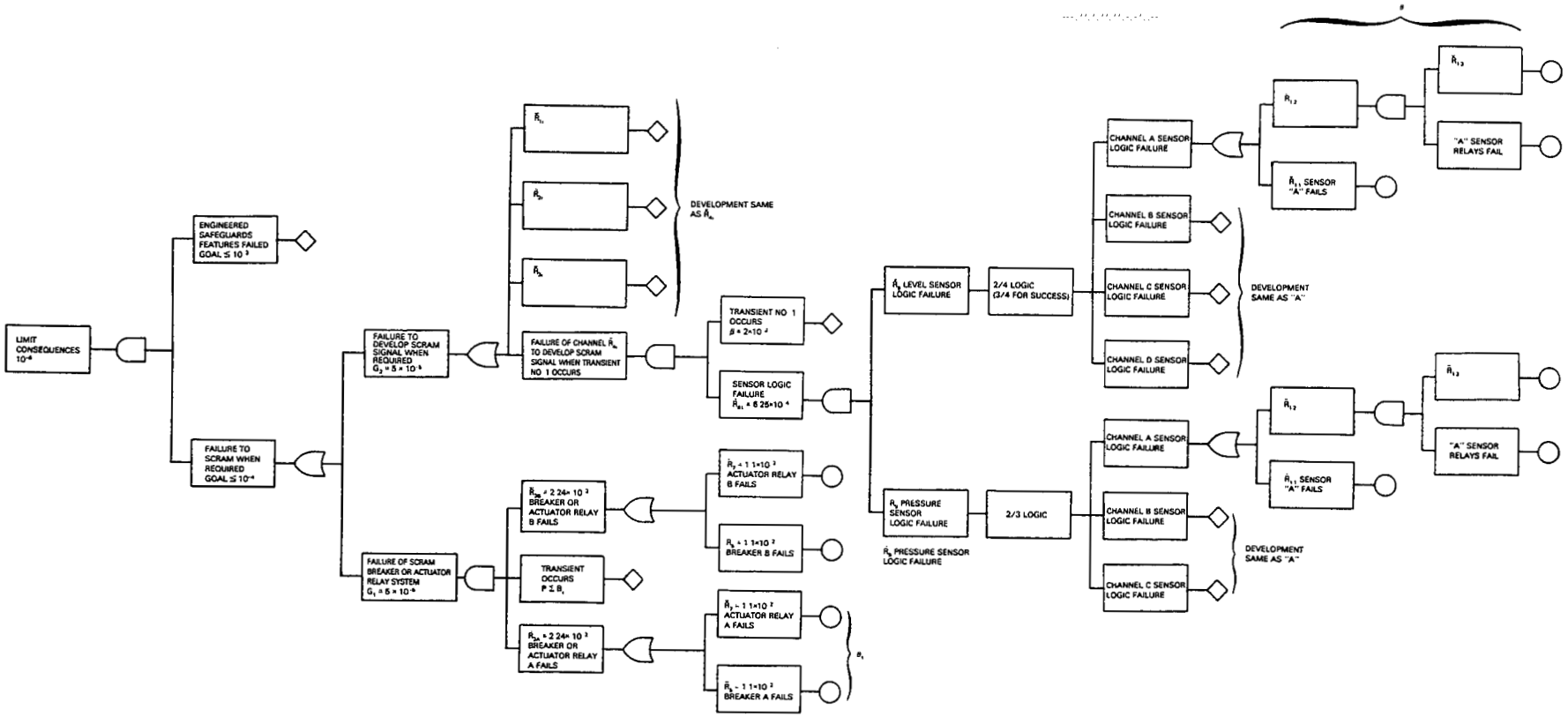


Fig A3
Fault Tree for Limit Consequences

352-87
4805702 0008261 2

$[A]^4 = 34.6 \cdot 10^{-6}$

$[A]^2 = 58.8 \cdot 10^{-4}$

$[A] = 7.65 \cdot 10^{-2}$

or

$$R_{11} + (\bar{R}_{13})^2 = 7.65 \cdot 10^{-2} \qquad \text{(Eq A11)}$$

Equations A4 and A11 can be used to find the appropriate test intervals that will satisfy goals just developed. Using Eq A4,

$\bar{R}_5 = \lambda_5 \theta_1$ and $\bar{R}_7 = \lambda^7 \theta_2$

with failure rates given in Table A1,

$\lambda_5 = 1.8 \cdot 10^{-6}$ (breaker failure rate)

$\lambda_7 = 5 \cdot 10^{-6}$ (actuator relay failure rate)

Equation A4a is solved for the test intervals θ_1 and θ_2:

$$\theta_1 = \frac{1.1 \cdot 10^{-2}}{1.8 \cdot 10^{-6}} = 6111 \text{ hours}$$

$$\theta_2 = \frac{1.1 \cdot 10^{-2}}{5 \cdot 10^{-6}} = 2200 \text{ hours}$$

Since it is convenient to test the actuator relay at the same time as the breaker, we will use the same test interval for both calculated as follows. From Eq A4,

$\lambda_5 \theta_1 + \lambda_7 \theta_1 = 2.24 \cdot 10^{-2}$

where

$$\theta_1 = \frac{2.24 \cdot 10^{-2}}{\lambda_5 + \lambda_7} = \frac{2.24 \cdot 10^{-2}}{6.8 \cdot 10^{-6}} = 3290 \text{ hours}$$

Thus θ_1 should be about 3000 hours.

Equation A11 is now used to determine the test intervals for the sensors and sensor relays. Again referring to Table A1,

$\lambda_{11} = 2.63 \cdot 10^{-5}$ (sensor channel failure rate)

$\lambda_{13} = 5 \cdot 10^{-6}$ (relay channel failure rate)

with

$\bar{R}_{11} = \lambda_{11} \theta_3$

$\bar{R}_{13} = \lambda_{13} \theta_4$

Equation A11 becomes

$2.63 \cdot 10^{-5} \theta_3 + (5 \cdot 10^{-6} \theta_4)^2 = 7.65 \cdot 10^{-2}$

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

letting $\theta_3 = \theta_4 = \theta$

$$2.63 \cdot 10^{-5}\,\theta + 25 \cdot 10^{-12}\,\theta^2 = 7.65 \cdot 10^{-2}$$

The second term is negligible, and

$$\theta = \frac{7.65 \cdot 10^{-2}}{2.63 \cdot 10^{-5}} = 2900 \text{ hours}$$

Therefore θ should be 2900 hours.

At this point, the overall system should be checked to ascertain that the goals are met. The overall equation was

$$G \leq 10^{-4} = G_1 + G_2$$

where

$$G_1 = (\bar{R}_3)^2 \sum_{i=1}^{n} \beta_i$$

$$= (\bar{R}_5 + \bar{R}_7)^2 \sum_{i=1}^{n} \beta_i$$

and

$$G_2 = 4\,G_4 = 4\,\beta \bar{R}_6 = 4\,\beta \bar{R}_8 \bar{R}_{10}$$

$$= 4\,\beta\,[3(\bar{R}_9)^2]\,[6(\bar{R}_9)^2]$$

$$= 4\,\beta\,[18(\bar{R}_{11} + \bar{R}_{12})^4]$$

$$= 4\,\beta\,[18(\bar{R}_{11} + (\bar{R}_{13})^2)^4]$$

$$G_2 = 72\,\beta\,[\bar{R}_{11} + (\bar{R}_{13})^2]^4$$

Thus,

$$G = (\bar{R}_5 + \bar{R}_7)^2 \sum_{i=1}^{n} \beta_i + 72\,\beta\,[\bar{R}_{11} + (\bar{R}_{13})^2]^4 \qquad \text{(Eq A12)}$$

Solution of Eq A14 is as follows:

$$G = (\lambda_5 \theta_1 + \lambda_7 \theta_1)^2\,(0.1) + 72 \cdot 2 \cdot 10^{-2}\,[\lambda_{11}\theta + (\lambda_{13}\theta)^2]^4$$

$$G = 9.09 \cdot 10^{-5}$$

which meets the goal requirement $G \leq 10^{-4}$. Equation A12 can be reevaluated after failure data has been collected for a period of time long enough to justify the use of failure rates that differ from the original data used. As an example, consider that 100 dc power supplies are observed for a time duration of 16 000 hours each, where each is replaced or repaired when it fails. Thus the total time is $T^* = (100)\,(16\,000)$. There were 33 failures, so, assuming that the times to failure are exponentially distributed, the estimate of $\lambda^* = n/T^* = 33/(100)\,(16\,000) = 20.63 \cdot 10^{-6} \approx 21 \cdot 10^{-6}$.

The 0.5 and 0.95 fractiles of a chi-square distribution with 66 and 68 degrees of freedom are, respectively, 48.31 and 88.25. Using Eq 47, the 90% confidence interval is

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

$$\frac{\chi^2 0.05;66}{2T^*} \leq \lambda^* \leq \frac{\chi^2 0.95;68}{2T^*}$$

$$\frac{48.31}{2(100)(16\,000)} \leq \lambda^* \leq \frac{88.25}{2(100)(16\,000)}$$

$$15.1 \cdot 10^{-6} \leq \lambda^* \leq 27.6 \cdot 10^{-6}$$

Care should be taken prior to a decision to change test intervals so that the goal is not jeopardized.

A4. Bibliography

[A1] Salvatori, R. *Systematic Approach to Safety Design and Evaluation.* Presented at the Nuclear Power Systems Symposium, 1970.

[A2] Farmer, F. R. Reactor Safety and Siting: A Proposed Risk Criterion. *Nuclear Safety*, vol B, no 6, Nov-Dec 1967.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

Index

A

Acceptance sampling, 23, 96-99. *See also* Reliability testing
Analysis, qualitative. *See* Qualitative analysis
Analysis, quantitative. *See* Quantitative analysis
Analysis, reliability. *See* Reliability analysis
AND function, 50
AND gate, 33
Announced failure, 17. *See also* Failures
Availability, 17, 47-48, 57-58, 61, 87, 89, 103-104, 120

B

Bayesian techniques, 75-76
Binomial distribution, 73-75
Block diagram. *See* Reliability block diagram (RBD)
Boolean techniques, 49-56, 128, 130
  limitations, 90
Break-in period, 17

C

Cascade failures, 42, 59. *See also* Failures
CCFA (common-cause failure analysis). *See* Common-cause failures
Common-cause failure analysis (CCFA). *See* Common-cause failures
Common-cause failures (common-mode failures)
  definition, 17
  qualitative analysis, 38-44, 104, 123-128
  quantitative analysis, 58-59
  see also Failures
Computers
  qualitative analysis, use in, 35, 91
  quantitative analysis, use in, 48, 55, 59-62, 64, 89-90, 94
  software, possibly inaccurate decisions contained in, 19
Confidence interval, 70, 72
Confidence limit, 70, 72
Confirmation testing, 23, 96-99. *See also* Reliability testing
Containment closure systems, 89
Critical failures, 22. *See also* Failures
Cumulative distribution function, 69
Cut set, 35, 43-44, 55
  limitations, 90

D

Data acquisition and use, 20, 45, 67-85
  binomial distribution, 73-75
  combining and updating data, 75-76
  developing field data programs, 80-85
  established data programs. *See* Established data programs
  exponential distribution, 70-73
  failure analysis, 81-83

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Data acquisition and use *(cont.)*
failure data analysis, 83-85
failure rates. *See* Failure rate
input parameters, 67-69
mean time to repair (MTTR), 17, 67-68
mission time, 18, 45, 67-68
Poisson distribution, 73
probability distribution. *See* Probability distribution
test interval, 18, 45, 57-58, 67-68, 99-101, 104
test schedule, 18, 63, 68-69
Weibull distribution, 75
Definitions, 17-18
Demand, 88
De Morgan's theorem, 51, 53
Design of nuclear power generating station safety systems, 13, 20-21, 25, 28, 124
Designers of nuclear power generating station safety systems, 13, 20-21, 64, 87, 106
Documentation requirements, 20-22, 25-29, 43, 110-120

E

Early-failure period, 17
Earthquakes, 42, 124
Emergency cooling systems, 89
Emergency shutdown systems, 88-89
Energy Technology Engineering Center (ETEC), 77
Environmental conditions, 42, 45, 58, 68, 83, 103, 124
Equipment and system testing, 95-101. *See also* Reliability testing
Established data programs, 76-80
Energy Technology Engineering Center (ETEC), 77
Failure Incident Report Review (FIRR), 79
Failure Rate Data Program (FARADA), 76
Generating Availability Data System (GADS), 78-79
Government-Industry Data Exchange Program (GIDEP), 76-77
IEEE Nuclear Reliability Data Manual, 80
IEEE Survey of Industrial and Commercial Power Systems, 79-80
Licensee Event Report, 79
Nonelectric Parts Reliability Data (NPRD-1), 77
Nuclear Plant Reliability Data System (NPRDS), 77-78
Nuclear Power Experience Reports, 80
Operating Units Status Report (Gray Book), 79
Reactor Safety Study, 79
United Kingdom Atomic Energy Authority Data Program (UKAEA), 77
ETEC (Energy Technology Engineering Center), 77
Event trees, 90
Exponential distribution, 70-73

F

Failure data reporting and analysis, 81-85
Failure Incident Report Review (FIRR), 79
Failure mode and effects analysis (FEMA), 20-22, 34-36, 38, 90, 104
applications, 22, 106
documentation, 26-27, 110-120
example, 106-123
preparatory steps, 28-29
procedure, 26-27, 29, 42-43
purposes, 25, 28
timing, 28

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

Failure rate, 17, 45, 67, 85, 89, 93-94, 101
Failure Rate Data Program (FARADA), 76
Failures, 22
  announced, 17
  cascade, 42, 59
  causes, 83, 124, 127
  common-cause. *See* Common-cause failures
  definition, 17, 103-104
  modes, 43, 82, 120. *See also* Failure mode and effects analysis
  prevention, 124, 126
  rate. *See* Failure rate
  safe, 22, 63
  unsafe, 22, 63
Failure state model, 37
FARADA (Failure Rate Data Program), 76
Fault trees, 21, 28, 59, 104
  examples, 38, 39, 128-138
  functions and benefits, 32, 90-91
  limitations, 90-91
  "limit consequence" approach, 130-131, 135
  procedure, 34-35
  representation of events, 32-34
Field data programs, 80-85
Fires, 124
FIRR (Failure Incident Report Review), 79
Floods, 124
FMEA. *See* Failure mode and effects analysis

G

Generating Availability Data System (GADS), 78-79
GIDEP (Government-Industry Data Exchange Program), 76-77
Go methodology, 62
Government-Industry Data Exchange Program (GIDEP), 76-77
Gray Book (Operating Units Status Report), 79

H

Hazard function, 75
House symbol in fault tree, 34
Human factor considerations, 19-20, 23, 67-68, 83, 124
  concerning computer software, 19
  shortage of data, 19, 76

I

IEEE Nuclear Reliability Manual, 80
IEEE Survey of Industrial and Commercial Power Systems, 79-80
"Infant mortality," 17
INHIBIT gate, 34
Instantaneous availability, 17
Item failure, 17. *See also* Failures

L

Licensee Event Report, 79
"Limit consequence" approach, 130-131, 135
Logic configurations, 63-64
Logic trees, 21-22

M

Maintenance of nuclear power generating station safety systems, 13, 21, 87, 124
Manual calculation in quantitative analysis, 48-59, 64, 89-90
Markov models, 22, 60-61, 91-95

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Markov models *(cont.)*
constant failure and repair rate components, 94
constant repair or switching time components, 94-95
constant success/failure on demand, 95
example, 61
limitations, 90
Mathematical modeling. *See* Quantitative analysis analysis
Mean time between failures (MTBF), 17, 67, 85
Mean time to failure (MTTF), 17, 62, 85
Mean time to repair (MTTR), 17, 57-58, 67-68. *See also* Repair time
Minimal cut set, 35, 43-44, 55
Mission, 17
Mission failure, 17
Mission time, 18, 45, 67-68
Modeling techniques. *See* Quantitative analysis
Monte Carlo methods, 61-62
limitations, 90
MTBF (mean time between failures), 17, 67, 85
MTTF (mean time to failure), 17, 62, 85
MTTR (mean time to repair), 17, 57-58, 67-68. *See also* Repair time
Mutually exclusive events, 18

N

Nonelectric Parts Reliability Data (NPRD-1), 77
Nuclear Plant Reliability Data System (NPRDS), 77-78
Nuclear Power Experience Reports, 80
Nuclear power generating station safety systems
analysis. *See* Reliability analysis
definitions, 17-18
demand, 88
design, 13, 20-21, 25, 28, 124
designers, 13, 20-21, 64, 87, 106
introduction, 13-16
operation and maintenance, 13, 21, 87, 124
references, 13-16
reliability analysis. *See* Reliability analysis
testing. *See* Reliability testing
Numerical goals for reliability and availability, 87-89

O

Operating Units Status Report (Gray Book), 79
Operation of nuclear power generating station safety systems, 13, 21, 87, 124
Operational testing, 22-24. *See also* Reliability testing
OR function, 50
OR gate, 33

P

Perfectly staggered testing, 18, 69. *See also* Reliability testing
Poisson distribution, 73
Probability density function, 69
Probability distribution, 18, 69-76, 83-85, 89-91
binomial, 73-75
combining and updating data, 75-76
exponential, 70-73
Poisson, 73
Weibull, 75

Q

Qualitative analysis
common-cause failures, 38-44, 104, 123-128
documentation, 20-21, 26-27, 43, 110-120

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

Qualitative analysis *(cont.)*
example, 37-41, 103-128
failure mode and effects analysis. *See* Failure mode and effects analysis (FMEA)
fault trees. *See* Fault trees
as preliminary step to quantitative analysis, 20, 87
principles and procedure, 19-21, 25-44, 87
reliability block diagrams. *See* Reliability block diagram (RBD)
Quantitative analysis
availability, 17, 47-48, 57-58, 87, 89, 103-104, 120
common-cause failures, 58-59
computer calculation, 48, 55, 59-62, 64, 89-90, 94
credibility check of results, 64-66
example, 103-106, 128-138
GO methodology, 62
manual calculation, 48-59, 64, 89-90
Markov models. *See* Markov models
mathematical modeling, by computer, 48, 55, 59-62, 64, 89-90
mathematical modeling, manual, 48-59, 64, 89-90
mission definition, 45-48
modeling technique selection, 89-90
Monte Carlo methods, 61-62, 90
numerical goals, 87-89
principles and procedure, 19, 21-23, 29, 45-66
reliability, 18, 45-46, 55, 57, 87, 89, 104
success failure state modeling, 22, 95
tabular reference to popular logic configurations, 63-64
trial calcultions, 64

R

RBD. *See* Reliability block diagram (RBD)
Reactor emergency shutdown, 88-89
Reactor Safety Study, 79
Redundant components and systems, 18, 22, 38-45, 68
References, 13-16
Reliability, 18, 45-46, 55, 57, 87, 89, 101, 103-104
Reliability analysis
applications, 19-24, 87-101, 103-138
data for. *See* Data acquisition and use
definitions, 17-18
demand, 88
documentation requirements, 20-22, 25-29, 43, 110-120
examples, 37-41, 103-138
and human factor. *See* Human factor considerations
introduction to, 13-16
numerical goals, 87-89
objectives and methods, 19-24, 87-101, 103-138
qualitative analysis. *See* Qualitative analysis
quantitative analysis. *See* Quantitative analysis
references, 13-16
reliability testing. *See* Reliability testing
Reliability block diagram (RBD), 35-37, 104, 128, 131
examples, 38, 40-41, 55
Reliability testing, 13, 21-25, 87
acceptance testing, 23, 96-99
confirmation testing, 23, 96-99
documenting, 10
equipment and system testing, 95-101
frequency, 18
interval, 18, 24, 45, 57-58, 67-68, 99-101, 104
operational testing, 22-24
perfectly staggered testing, 18, 69
schedule, 18, 45, 63, 67-69
simultaneous testing, 18, 68-69
surveillance testing, 45, 67
testing as a detriment to reliability, 101
Repair rate, 18, 45, 57, 67, 89, 92, 94
Repair time, 89, 94-95. *See also* Mean time to repair (MTTR)

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Replacement time, 89
Restricted repair, 92-93
Risk, 18, 88-89

S

Safe failures, 22, 63
Safety systems, nuclear power generating station. *See* Nuclear power generating station safety systems
Sensitivity analysis, 18, 21, 23, 64-66, 89, 104
Simultaneous testing, 18, 68-69. *See also* Reliability testing
Single-failure analysis, 103-104, 106
Software, computer, 19
Steady-state availability, 17, 47-48
Success/failure state modeling, 22, 95
Surveillance testing, 45, 67. *See also* Reliability testing
Switching time, 94-95
System boundaries, 28, 34, 36, 42, 103, 108
System functional diagram, 21, 37
System interfaces, 28, 42
System modeling. *See* Quantitative analysis
System state, 92

T

Tabular reference to popular logic configurations, 63-64
Tests. *See* Reliability testing
Top event, 34, 44, 90
Tornadoes, 124
Transfer gate, 33
Transient availability, 17, 61
Transition rate, 93-94
Truth table, 48-50

U

UKAEA (United Kingdom Atomic Energy Authority Data Program), 77
Unavailability, 18, 63
United Kingdom Atomic Energy Authority Data Program (UKAEA), 77
Unrestricted repair, 92-93
Unsafe failures, 22, 63. *See also* Failures

V

Variable-parameter — narrow-range method (sensitivity analysis), 66
Variable-parameter — wide-range method (sensitivity analysis), 64-66
Venn diagram, 49-50, 52

W

Wearout period, 18
Weibull distribution, 75

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

ANSI/IEEE Std 352-1987 provides the user with basic principles needed to conduct a reliability analysis of safety systems for nuclear power generating stations. These principles, together with further information provided in the references, are sufficient to develop a reliability/availability analysis not only for nuclear power plant safety systems, but for other protection systems as well. A user may select a specific section of the standard that applies to the particular needs of his organization. Some areas discussed are:

- Quantitative analysis and mathematical modeling
- Problems of failure data
- Probability distribution, estimation, and confidence intervals used in evaluating failure and repair rate data
- Information on established data programs

Application of the principles and procedures of reliability engineering that are presented will allow designers and operators to analyze the system, compare the results with reliability objectives, and suitably document the basis for decisions made at various phases of the system's lifetime.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS