

IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Systems and Other Nuclear Facilities

IEEE Power and Energy Society

Sponsored by the
Nuclear Power Engineering Committee



IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 352™-2016
(Revision of IEEE Std 352-1987)

IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Systems and Other Nuclear Facilities

Sponsor

Nuclear Power Engineering Committee
of the
IEEE Power and Energy Society

Approved 7 December 2016

IEEE-SA Standards Board

This is a Redline Document produced by Techstreet, a business of Thomson Reuters.

This document is intended to provide users with an indication of changes from one edition to the next. It includes a full-text version of the new document, plus an indication of changes from the previous version.

Redlines are designed to save time and improve efficiencies by using the latest software technology to find and highlight document changes. More professionals are using valuable new technologies like redlines, to help improve outcomes in a fastpaced global business world.

Because it may not be technically possible to capture all changes accurately, it is recommended that users consult previous editions as appropriate. In all cases, only the current base version of this publication is to be considered the official document.

Redline Processing Notes:

1. ~~Red Text~~ - Red strikethrough text denotes deletions.
2. Blue Text - Blue underlined text denotes modifications and additions.

Abstract: General reliability and availability analysis methods that can be applied to structures, systems, and components (SSCs) in nuclear power generating stations and other nuclear facilities are contained in this guide.

Keywords: availability, Class 1E, failure rate, IEEE 352™, MTBF, MTTF, MTTR, nuclear power generating station, reliability

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2017 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 7 April 2017. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-1-5044-3643-1 STD22368
Print: ISBN 978-1-5044-3644-1 STDPD22368

IEEE prohibits discrimination, harassment, and bullying. For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.
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.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (“IEEE-SA”) Standards Board. IEEE (“the Institute”) develops its standards through a consensus development process, approved by the American National Standards Institute (“ANSI”), which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

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.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

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

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Xplore at <http://ieeexplore.ieee.org/> or contact IEEE at the address listed previously. For more information about the IEEE-SA or IEEE's standards development process, visit the IEEE-SA Website at <http://standards.ieee.org>.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE-SA Website at the following URL: <http://standards.ieee.org/findstds/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website at <http://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association

Participants

At the time this IEEE guide was completed, the Reliability (PE/NPE/WG_3.3) Working Group had the following membership:

John A. Stevens, *Chair*

George Ballassi
John Beatty
Tom Crawford
Marie Cuvelier
John Erinc

Sharon Honecker
Jacob Kulangara
James K. Liming
Joseph Napper

Vish Patel
Sheila Ray
Ted Riccio
Yvonne Williams
Kiang Zee

At the time this IEEE guide was completed, the Operations, Surveillance, Aging, Reliability, and Testing Subcommittee (SC-3) had the following membership:

Yvonne Williams, *Chair*
Tom Crawford, *Vice-Chair*

Gopal Aravapalli
George Ballassi
John Beatty
Thomas Carrier
Suresh Channarasappa
Marie Cuvelier
John Erinc
Edward Eustace

Hamid Heidarisafo
Sharon Honecker
Steven Hutchins
Jacob Kulangara
James K. Liming
Kirklyn Melson
Edward Mohtashemi
Joseph Napper
James Parello

Vish Patel
Sheila Ray
Ted Riccio
Rebecca Steinman
Craig Sellers
John Stevens
John Taylor
Kiang Zee

At the time this IEEE guide was completed, the Nuclear Power Engineering Committee (NPEC) had the following membership:

Stephen Fleger, *Chair*
Thomas Koshy, *Vice-Chair*
Daryl Harmon, *Secretary*

Satish Aggarwal
Ijaz Ahmad
George Attarian
George Ballassi
Royce Beacom
Mark Bowman
Keith Bush
Robert Carruth
John Carter
Suresh Channarasappa
Paul Colaanni
Tom Crawford
Dennis Dellinger
David Desaulniers
John Disosway
Kenneth Fleischer
Robert Fletcher

Robert Francis
Cristopher Georgeson
James Gleason
Dale Goodney
Robert Hall
David Herrell
Dirk Hopp
Greg Hostetter
Steven Hutchins
Gary Johnson
Chris Kerr
Wolfgang Koenig
Robert Konnik
James K. Liming
Bruce Lord
John MacDonald
Scott Malcolm

Kenneth Miller
Michael Miller
Edward Mohtashemi
Yasushi Nakagawa
Warren Odess-Gillett
Ted Riccio
Mitchell Staskiewicz
Rebecca Steinman
John Stevens
Marek Tengler
Sudhir Thakur
James Thomas
Masafumi Utsumi
Tammy Womack
John White
Yvonne Williams
Paul Yanosy

The following members of the individual balloting committee voted on this guide. Balloters may have voted for approval, disapproval, or abstention.

Satish Aggarwal
George Ballassi
John Beatty
Jason Bellamy
Daniel Brosnan
Gustavo Brunello
Nissen Burstein
Robert Carruth
Tom Crawford
John Disosway
Neal Dowling
John Erinc
Stephen Flegler
Dale Goodney
Eric W. Gray

Randall Groves
Ajit Gwal
Daryl Harmon
Hamidreza Heidarisa
Lee Herron
Werner Hoelzl
Greg Hostetter
Steven Hutchins
Yuri Khersonsky
Yoonik Kim
Robert Konnik
Thomas Koshy
Jacob Kulangara
Benjamin Lanz
Michael Lauxman
James K. Liming

Bruce Lord
Omar Mazzoni
Kirklyn Melson
Andrew Nack
Warren Odess-Gillett
Mirko Palazzo
Howard Penrose
Ted Riccio
Jeremy Smith
Deirdre Spaulding
Rebecca Steinman
John A. Stevens
John Vergis
Yvonne Williams
Shuhui Zhang

When the IEEE-SA Standards Board approved this guide on 7 December 2016, it had the following membership:

Jean-Philippe Faure, *Chair*
Ted Burse, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Chuck Adams
Masayuki Ariyoshi
Stephen Dukes
Jianbin Fan
J. Travis Griffith
Gary Hoffman

Ronald W. Hotchkiss
Michael Janezic
Joseph L. Koepfinger*
Hung Ling
Kevin Lu
Annette D. Reilly
Gary Robinson

Mehmet Ulema
Yingli Wen
Howard Wolfman
Don Wright
Yu Yuan
Daidi Zhong

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 352-2016, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Systems and Other Nuclear Facilities.

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 [Clause 6](#). The very important problem of failure data is discussed in [Clause 7](#); 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, IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations. In the intervening years, IEEE Std 279 has been superseded by IEEE Std 603™, and in March, 1984, IEEE Std 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 IEEE Std 603, 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 to the analyses of other facilities and systems by selecting those parts of the principles relevant to those other facilities/systems.

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

Contents

1. Overview	12
1.1 General	12
1.2 Scope	12
1.3 Purpose	13
2. Normative references.....	13
3. Definitions, acronyms, and abbreviations	13
3.1 Definitions	13
3.2 Acronyms and abbreviations	15
4. Objectives and methods.....	15
4.1 Overview	15
4.2 Consideration of the human factor.....	15
4.3 Qualitative analysis.....	16
4.3.1 Objectives of a qualitative analysis.....	16
4.3.2 Steps in a qualitative analysis	16
4.4 Quantitative analysis.....	17
4.5 Applications of reliability methodology	17
4.5.1 Overview.....	17
4.5.2 Failure modes and effects analysis (FMEA)	17
4.5.3 Logic trees.....	18
4.5.4 System modeling.....	18
4.5.5 Reliability testing	19
5. Qualitative analysis principles.....	20
5.1 Overview	20
5.2 Failure modes and effects analysis (FMEA).....	20
5.2.1 Purposes of failure modes and effects analysis (FMEA)	20
5.2.2 Timing of a failure mode and effects analysis (FMEA).....	23
5.2.3 Issues addressed in a failure mode and effects analysis (FMEA)	23
5.2.4 Preparatory steps for a failure mode and effects analysis (FMEA).....	24
5.2.5 Procedure for a failure mode and effects analysis (FMEA).....	24
5.3 Fault tree analysis	25
5.3.1 Functions and benefits of fault tree analysis	27
5.3.2 Representation of events and operations in a fault tree	28
5.3.3 Procedure for constructing a fault tree	30
5.4 Reliability block diagram (RBD).....	31
5.4.1 Reliability block diagram (RBD) construction	32
5.4.2 Reliability block diagram (RBD) reduction	32
5.4.3 Comparison of fault tree and reliability block diagrams (RBDs).....	32
5.5 Example.....	33
5.5.1 Description of a typical reactor trip function	33
5.5.2 Failure mode and effects analysis (FMEA).....	33
5.5.3 Fault tree analysis	33
5.5.4 Reliability block diagram (RBD)	33
5.6 Extended qualitative analysis for common-cause failures.....	34
5.6.1 Extended failure mode and effect analysis (FMEA)	38
5.6.2 Extended fault tree analysis	39
5.6.3 Termination of the analyses	39
6. Quantitative analysis principles.....	40

6.1 Overview	40
6.2 Mission definition	40
6.2.1 Reliability	40
6.2.2 Availability (steady-state)	42
6.3 Mathematical modeling	43
6.3.1 Manual calculation	44
6.3.2 For computer calculation	57
6.4 Tabular reference to popular logic configurations	60
6.5 Trial calculations	61
6.5.1 Manual calculations	61
6.5.2 Computer calculations	61
6.6 Credibility check of results	61
6.6.1 Comparison with prior analysis	61
6.6.2 Sensitivity analysis	61
7. Guides for data acquisition and use	63
7.1 Overview	63
7.2 Input parameters	64
7.2.1 Failure rates	64
7.2.2 Mean time to repair (MTTR)	64
7.2.3 Mission time	65
7.2.4 Test interval	65
7.2.5 Test schedule	65
7.3 Probability distributions, parameters, and estimation	65
7.3.1 Exponential distribution	67
7.3.2 Poisson distribution	70
7.3.3 Binomial distribution	71
7.3.4 Weibull distribution	72
7.3.5 Combining and updating data	73
7.4 Established data programs	73
7.4.1 Failure Rate Data Program (FARADA)	74
7.4.2 Government-Industry Data Exchange Program (GIDEP)	74
7.4.3 Nonelectric parts reliability data (NPRD-1)	74
7.4.4 Energy Technology Engineering Center (ETEC)	75
7.4.5 United Kingdom Atomic Energy Authority Data Program (UKAEA), National Center of Systems Reliability (SYREL)	75
7.4.6 Nuclear Plant Reliability Data System (NPRDS)	75
7.4.7 Generating Availability Data System (GADS)	76
7.4.8 Licensee event reports	76
7.4.9 Operating Units Status Report (NUREG-0020)	77
7.4.10 Reactor Safety Study, WASH-1400 (NUREG-75/01 4)	77
7.4.11 Failure Incident Report Review (FIRR)	77
7.4.12 IEEE Survey of Industrial and Commercial Power Systems	77
7.4.13 Nuclear power experience reports	77
7.4.14 IEEE Nuclear Reliability Data Manual—IEEE Std 500™ [B22]	78
7.5 Developing field data programs	78
7.5.1 Failure analysis	79
7.5.2 Failure data analysis	81
8. Application of reliability methods	84
8.1 Introduction	84
8.2 Numerical goals	84
8.2.1 Basis for establishing numerical goals	84
8.2.2 Specific goals	85
8.2.3 Procedures	86
8.3 Selection of the modeling technique	86

8.3.1 Model requirements	86
8.3.2 Model limitations	86
8.4 Fault tree techniques	87
8.4.1 Characteristics	87
8.4.2 Recommended uses	88
8.5 The Markov process as a reliability model	88
8.5.1 Constant failure and repair rate components	91
8.5.2 Constant repair or switching time components	91
8.5.3 Constant success/failure on demand	92
8.6 Monte Carlo techniques	92
8.6.1 Characteristics	92
8.6.2 Recommended uses	93
8.7 Equipment and system testing	93
8.7.1 Acceptance sampling	93
8.7.2 Initial test intervals	98
8.7.3 In-service adjustment of test intervals	100
Annex A (informative) Bibliography	101
Annex B (informative) Illustration of concepts and methods of reliability and availability analyses	104
B.1 Introduction	104
B.2 Procedure	104
B.2.1 System definition	104
B.2.2 Failure mode and effects analysis (FMEA) (qualitative analysis)	105
B.2.3 Common-cause-failure analysis	105
B.2.4 Reliability/Availability prediction (quantitative)	105
B.3 Illustrative examples	105
B.3.1 System definition	105
B.3.2 Qualitative analysis—failure modes and effects analysis (FMEA)	107
B.3.3 Common-cause-failure analysis	127
B.3.4 Quantitative analysis	131
Annex C (informative) Mean time to repair (MTTR) process	148
C.1 Introduction	148
C.1.1 Call-out	148
C.1.2 Briefing	148
C.1.3 Access control	148
C.1.4 Establishing prerequisite conditions	148
C.1.5 Troubleshooting	149
C.1.6 Spare parts acquisition	149
C.1.7 Pre-configuration	149
C.1.8 Disassembly	149
C.1.9 Re-assembly	149
C.1.10 Inspections	149
C.1.11 Post-configuration	150
C.1.12 Test	150
C.2 Systematic mean time to repair (MTTR) estimation method	150
C.3 A sample mean time to repair (MTTR) estimation	152

~~An American National Standard~~

IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station ~~Safety Systems~~ and Other Nuclear Facilities

1. Overview ~~Introduction and References~~

1.1 General ~~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]~~ TM [B24].¹

1.2 Scope

This guide contains general reliability and availability analysis methods that can be applied to structures, systems, and components (SSCs) in nuclear power generating stations and other nuclear facilities.

¹The numbers in brackets correspond to those of the references listed in ~~1-2~~ the bibliography in Annex A.

1.3 Purpose

This guide provides the designers, operators, and regulators with a common and consistent framework for performance of reliability and availability analyses of nuclear power generating stations and other nuclear facilities.

2. Normative references

None.

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

~~[8] BAIN, L. J. *Statistical Analysis of Reliability and Life Testing Models*. New York: Dekker, 1978.~~

~~[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~~

3. Definitions, acronyms, and abbreviations

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary: Glossary of Terms and Definitions* should be consulted for terms not defined in this clause.²

3.1 Definitions

availability: The probability that an item or system will be operational on demand. *See also: steady-state availability and transient availability.*

~~**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.”~~

²*IEEE Standards Dictionary: Glossary of Terms and Definitions* is available at <http://dictionary.ieee.org>.

common-cause failures: ~~Multiple failures attributable to a common cause. (Sometimes called “common mode failure,” but this term is becoming obsolete.)~~ Loss of function to multiple structures, systems, and components due to a shared initiating event or reason. Common-cause failures are dependent failures.

common-mode failures: Loss of function to multiple structures, systems, and components in the same manner. Common-mode failures can be dependent failures (if they are the result of single initiating event or reason) or independent failures (if they are the result of distinct initiating events or reasons).

failure: The termination of the ability to perform a required function. ~~(See also: **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 the number of operations, environmental conditions, etc., may also occur.

human error probability: The quantitative estimation of the likelihood of a human error.

infant mortality: 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 “break-in period.”

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

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

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

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

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

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

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

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

mutually exclusive events: Events that cannot exist simultaneously.

probability distribution function: The mathematical function that gives $\text{Pr}(X \leq x)$, 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.

steady-state availability is the expected fraction of the time in the long run that an item (or system) operates satisfactorily.

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

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.

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)~~, maintained, or tested or it may occur as a result of malfunctions. Unavailability is the complement of availability.

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

3.2 Acronyms and abbreviations

<u>CCFA</u>	<u>common-cause failure analysis</u>
<u>FMEA</u>	<u>failure mode and effects analysis</u>
<u>GADS</u>	<u>Generating Availability Data System</u>
<u>GIDEP</u>	<u>Government-Industry Data Exchange Program</u>
<u>I&C</u>	<u>instrumentation and control</u>
<u>Iid</u>	<u>identically distributed</u>
<u>MTBF</u>	<u>mean time between failures</u>

MTTF	mean time to failure
MTTR	mean time to repair
NPRD	nonelectric parts reliability data
NPRDS	Nuclear Plant Reliability Data System
RBD	reliability block diagram
SSC	structures, systems, and components

4. Objectives and methods

[4.1 Overview](#)

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.

4.2 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.

See IEEE Std 1082™ [B25], Conference Record Bibliography [B10], NUREG/CR-1278 [B39], NUREG/CR-2254 [B40], NUREG/CR-2300 [B41], and NUREG/CR-3010 [B42] for information on incorporating the human factor into system reliability analysis.

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

- ~~1) Bibliography contained in the Conference Record for 1979 IEEE Standards Workshop on Human Factors and Nuclear Safety, sponsored by the Institute of Electrical and Electronics Engineers, the United States Nuclear Regulatory Commission, and Brookhaven National Laboratory [12].~~
- ~~2) NUREG/CR 1278. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Final Report, August 1983 [31].~~ 3)

- 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].~~

4.3 Qualitative analysis

4.3.1 Objectives of a qualitative analysis

Qualitative reliability analyses are used to identify possible ways in which a system can fail and to identify proper precautions (e.g. design changes, administrative procedures, ~~ete~~) 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:

- a) To identify weak spots or imbalances in the design.
- b) To aid in the systematic assessment of overall plant safety.
- c) To document and assess the relative importance of all identified failures.
- d) To develop discipline and objectivity on the part of a designer of safety-related systems and interfaces between systems.
- e) 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 or she considered unimportant during the original design process. Therefore, ~~his~~ the designer's systematic analysis should be reviewed and checked by qualified people (including a reliability analyst) 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.~~

4.3.2 Steps in a qualitative analysis

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

- a) Identify the functional required performance of the system.
- b) Identify the system boundaries and components.
- c) Identify significant failures and their consequences (generally called failure mode and effects analysis—FMEA).
- d) Display the above information in a table, chart, fault tree, or other format.
- e) Evaluate overall system reliability relative to the information above and identify potential problems.
- f) Identify improvements that can be made from items identified in item e).

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~~ reliability engineer to ~~document~~ assemble these modes. An experienced reliability analyst should be consulted to define the level of detail to be pursued in identifying failures.

In the ~~fourth~~ fifth general step [item e)], 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~~ prioritize areas where improvements can be made.

4.4 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 faded conditions to determine appropriate system or operator actions, or both.~~

The mathematical model generated can be used in a sensitivity analysis. Thus, ~~one~~ [the analyst](#) 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.

4.5 Applications of reliability methodology

4.5.1 Overview

In ~~Sections 4.~~ [Clause 5](#) and ~~5.~~ [Clause 6](#) of this guide various reliability methods will be introduced. The intent of this ~~subsection~~ [subclause](#) is to provide an outline of ways in which these methods can be applied to enhance system reliability. ~~Each method~~ [Select methods](#) will be discussed in greater detail in ~~Section 7~~ [Clause 8](#). 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 [the](#) four categories [listed next](#):

- a) Failure modes and effects analysis (FMEA)
- b) Logic tree analysis
- c) System modelling
- d) 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.

4.5.2 Failure modes and effects analysis (FMEA)

The FMEA is usually the first reliability activity performed to provide a better understanding of a design's failure potential. It can be limited to a qualitative assessment, but may include numerical estimates of a failure probability [such as a criticality analysis](#).

Important applications of the FMEA include the following:

- a) The specification of future tests—such as a qualification test—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.
- b) Identification of “safe” versus “unsafe” failures for use in the quantitative evaluation of safety-related reliability.
- c) 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.
- d) The establishment of the level of parts quality—(=particularly true in electrical systems) = needed to meet allocated reliability goals.
- e) The identification of the need for design modifications to eliminate unacceptable failure mechanisms. These failures could produce unacceptable safety or operational conditions.
- f) Identification of the need for failure detection.

4.5.3 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:

- a) They identify single point failures. These are single (or multiple dependent) failures that can prevent the system from performing its intended function.
- b) 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.

- c) They aid in establishing the frequency of operational tests by identifying those system components that may be required to have high “demand availability.”
- d) They identify the need for system configuration changes because of inadequate redundancy or diversity to meet allocated reliability goals.
- e) 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.

4.5.4 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:

- a) 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.
- b) Sensitivity studies to identify the component failures, [maintenance actions](#), and/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.
- c) 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.

- d) Apportionment of reliability goals by establishing reasonable contributions to the overall system goal of lower level subsystems or components.
- e) Evaluation of the degree to which predicted system reliability satisfies apportioned goals.
- f) Establishment of the amount of [reliability demonstration](#) testing required for various system elements (or the system itself) to confirm meeting established goals.

4.5.5 Reliability testing

Reliability testing can be divided into [the following](#) two broad categories:

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

4.5.5.1 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~~, [However](#), 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. For example, when practical 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.

4.5.5.2 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. [Analog and digital devices have different considerations when determining test intervals because modern digital devices often contain self-diagnostics that can allow longer operational test intervals.](#)

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 uptime and downtime 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~~ [helps ensure](#) 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~~ [helps ensure](#) 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.

5. Qualitative analysis principles

[5.1 Overview](#)

As mentioned in 4.3, 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 (RBD) 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.~~

5.2 Failure ~~Mode~~ [modes](#) 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~~ [SSC](#), how it may fail (the mode of failure), and what the effect of the failure on the ~~system~~ [SSC](#) would be (the failure effect). Usually, the analysis is organized by creating a format like that shown in Table 1.

5.2.1 Purposes of failure ~~Mode~~ modes and effects analysis [23] (FMEA)

The purposes of an FMEA are as follows:

- a) To assist in selecting design alternatives with high reliability and high safety potential during early design phases.
- b) To ensure that all conceivable failure modes, such as transient failures, off-normal failures, and parameter drifts, and their effects on the operational success of the system have been considered.
- c) To list potential failures and identify the magnitude of their effects.
- d) To develop early criteria for test planning and the design of test and checkout systems.
- e) To provide a basis for quantitative reliability and availability analyses.
- f) To provide historical documentation for future references to aid in the analysis of field failures and consideration of design changes.
- g) To provide input data for tradeoff studies.
- h) To provide a basis for establishing corrective action priorities.
- i) 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~~ component or system. A complete analysis requires comprehensive input data that ~~include~~ includes material properties, design details, and component failure rates; however, it is not necessary to wait until all of these are known before much can be determined about the reliability of the design.

By confining the scope of an analysis to ~~determining~~ determine how the ~~article~~ component or system can fail and what the consequences would be ~~if~~, should it 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.

Table 1—Typical failure mode and effects analysis (FMEA)
documentation

Component identification (1)	Function (2)	Failure mode (3)	Failure mechanism(s) (4)	Effect on system (5)	Method of detection (6)	Remarks (7)	Ranking S O D (8)
1. Circuit breaker 52/RTA, B, BYA, B	Trip	Fail closed	Jam mechanism UV trip attachment mechanism stuck Fuse main contacts	Makes trip 1/1	Monthly test		2 5 8
		Fail open	Loss of dc control power UV coil failure Worn trip latch	Spurious trip	Spurious trip	Immediate detection	1 5 2
2. DC Control relay RT1A, B, RT2A, B	Break circuit to trip breaker undervoltage coil on trip (deenergize to trip)	Fail closed	Contacts shorted or fused Armature jammed Wiring fault	Makes trip 1/1	Monthly test		2 5 8
		Fail open	Loss of dc control power Coil failure	Spurious trip	Spurious trip	Immediate detection	1 6 2
3. AC Control relay (relay logic) X1A, B, X2A, B, X3A, B	Break circuit to dc relays on trip (deenergize to trip)	Fail closed	Broken contacts Broken wire or loose connection Contacts shorted or fused Armature jammed Wiring fault	Spurious trip if 2/2 fail Makes 1 train 2/2 vice 2/3	Spurious trip	Immediate detection	1 6 2
		Fail open	Loss of ac power (instrument bus) Coil failure Broken contacts Broken wire or loose connection	Spurious trip if 2/3	Spurious trip	Monthly test	1 5 8
4. Alarm unit PC-1, 2, 3	Remove ac power to relays for $P_{st} > P_{set}$	Fail off	Transformer failure Open circuit in output section Setpoint drift	Makes both trains 1/2	Spurious trip if 2/3 fail	Partial trip alarm	2 6 7
		Fail on	Short in output section Setpoint drift	Makes both trains 2/2	Monthly test		1 5 8
5. DC Power Supply PQ-1, 2, 3	Provide power for analog current loop	Fail low or off	Transformer failure Diode failure	Makes both trains 1/2	Spurious trip if 2 fail	Partial trip alarm	2 7 7
		Fail high	Heat effects Misadjustment	Makes both trains 2/2	Monthly test		1 6 8
6. Pressure transmitter PT-1, 2, 3	Convert pressure to analog current	Fail low	Corrosion Wear Mechanical damage Heat effects Electronic failure	Makes both trains 2/2	Monthly test and comparison with redundant channel indicators	Possible immediate detection	1 4 8
		Fail high	Misadjustment Electronic failure	Makes both trains 1/2	Spurious trip if 2 fail	Partial trip alarm	2 3 8

(New)

FAILURE MODE AND EFFECTS ANALYSIS – TYPICAL TRIP FUNCTION						
Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
1. Circuit Breaker 52/RTA, RTB BYA, BYB	Trip	Fail Closed	Jam Mechanism UV Trip Attachment Mechanism Stuck Fuse Main Contacts	Makes Trip 1/1 " "	Monthly Test " "	Immediate Detection
		Fail Open	Loss of DC Control Power UV Coil Failure Worn Trip Latch	Spurious Trip " "	Spurious Trip " "	
2. DC Control Relay	Break Ckt. To Trip Breaker UV Coil on Trip (DE-EN To Trip)	Fail Closed	Contacts Shorted or Fused Armature Jammed Wiring Fault	Makes Trip 1/1 " "	Monthly Test " "	Immediate Detection
		Fail Open	Loss of DC Control Power Coil Failure Broken Contacts Broken Wire or Loose Connec.	Spurious Trip " Spurious Trip if 2/2 Fail " "	Spurious Trip " " "	
3. AC Control Relay X1A, B, X2A, B, X3A, B	Break Ckt. To DC Relays on Trip (DE-EN To Trip)	Fail Closed	Contacts Shorted or Fused Armature Jammed Wiring Fault	Makes 1 Train 2/2 vice 2/3 " "	Monthly Test " "	
		Fail Open	Loss of AC Power (Instr. Bus) Coil Failure Broken Contacts Broken Wire or Loose Connec.	Spurious Trip if 2/3 " " "	Spurious Trip " " "	
4. Alarm Unit PC-1, 2, 3	Remove AC Power To Relays For $P_M > P$ set	Fail Off	Transformer Failure Open Circuit in Output Sect. Setpoint Drift	Makes Both Trains 1/2 " "	Spurious Trip if 2/3 Fail " "	Partial Trip Alarm
		Fail On	Short in Output Section Setpoint Drift	Makes Both Trains 2/2 "	Monthly Test "	

(Deleted)

FAILURE MODE AND EFFECTS ANALYSIS – TYPICAL TRIP FUNCTION						
Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
5. DC Power Supply PQ-1, 2, 3	Provide Power For Analog Current Loop	Fail Low or Off	Transformer Failure Diode Failure	Makes Both Trains 1/2 "	Spurious Trip if 2 Fail "	Partial Trip Alarm
		Fail High	Heat Effects Misadjustment	Makes Both Trains 2/2 "	Monthly Test "	
6. Pressure Transmitter PT- 1, 2, 3	Convert Pressure To Analog Current	Fail Low	Corrosion Wear Mechanical Damage Heat Effects	Makes Both Trains 2/2 " " "	Monthly Test and Comparison with Redundant Channel Indicators	Possible Immediate Detection
		Fail High	Misadjustment	Makes Both Trains 1/2	Spurious Trip if 2 Fail	Partial Trip Alarm

(Deleted)

5.2.2 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:

- Concept formulation or selection
- Preliminary design or layout
- Completion of detail ~~part~~ design
- Design improvement programs

5.2.3 Issues addressed in a failure mode and effects analysis (FMEA)

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 may include the following:

- a) How can each part conceivably fail?
- b) What mechanisms might produce these modes of failure?
- c) What could the effects be if the failures did occur?
- d) Is the failure in the safe or unsafe direction?
- e) How is the failure detected?
- f) What inherent provisions are provided in the design to compensate for the failure?

However, as the design matures it is best practice to revisit the FMEA to add ranking information for each failure mode for severity of the effect of the failure mode, probability of occurrence of the failure mode, and detectability of the failure mode. These rankings can help the analyst prioritize which failure modes will be the most important ones for increasing safety and availability of the system. There are a variety of methods for performing this part of the analysis, ranging from a formal criticality analysis described in MIL-STD-1629A [B32] to less formal methods such as the one presented in Annex B. The severity S , occurrence O , and detectability D , are commonly ranked using 5-or 10-point scales that are set up before the FMEA is performed.

Severity rankings should be consistent with the information in the “Effect on system” column of the FMEA. As a starting point, generic analysis of severity can offer guidance as to the potential impact of each failure mode, but final analysis requires project-specific input. For example, in the severity ranking scale of Table B.3, appropriate and full use of the severity ranking values from 3 to 10 requires project-specific input.

Probability of occurrence rankings can be either subjective or objective. Subjective rankings are used before failure rate data for each failure mode are available. An advantage of subjective rankings is that they allow better ranking than objective rankings, based on operating experience. Objective rankings are based solely on component and system failure rate information. For example, in the occurrence ranking scale of Table B.4, ranking values of 1 to 3 represent unlikely failure modes, values of 4 to 6 represent occasional failure modes, and 7 to 10 represent failure modes that are possible repeatable or inevitable.

Detectability rankings should be consistent with the information in the “Method of detection” column of the FMEA. For example, in the detectability ranking scale of Table B.5, appropriate and full use of the severity ranking values—especially from 5 to 10—requires project-specific input.

5.2.4 Preparatory steps for a failure mode and effects analysis (FMEA)

The depth to which ~~one performs~~ the preparatory steps are performed is a function of the complexity of the equipment being studied and the experience that ~~one~~ an analyst has with similar equipment. Each of the following preparatory steps is essential, but may vary greatly in scope:

- a) Definition of the system to be analyzed and its mission objective.
- b) Description of the operation of the system for the given missions, considering surveillance and maintenance policies.
- c) Identification of failure categories.
- d) 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~~ contract requirement may be used. The analyst must know just what he or she is to analyze; he or she will then be able to define the interface functions. ~~The~~ More complex ~~the system, the greater the need to carefully define~~ systems require that more care be taken when defining 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,~~ as discussed ~~later~~ in 5.3.

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.

5.2.5 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~~ Figure 1 and Figure 2 and described in ~~4.4~~ 5.5. The form shown in Table 1 is typical of that which can be used to document an FMEA; however, other forms may also be used. A form similar to that shown in Table 1 is not only very helpful, but ~~also may actually be~~ 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] 577TM [B23].

The system component or part being analyzed is shown in ~~Table 1,~~ column 1 of Table 1. The normal 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~~ that use integral modular units as system building blocks, the modules, rather than their parts, may be ~~listed~~ 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~~ [of Table 1](#)).

Each failure mode that the analyst can conceive for each feature or location of the part is noted in column 3. ~~Again,~~ [of Table 1](#). The question is “Could it?” not “Will it?” When the item designated in column 1 is a piece-part, the failure modes ~~will~~ [might](#) 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~~ [causes](#) of failure that could result in the mode described in column 3 are noted in column 4 [of Table 1](#).

Column 5 [of Table 1](#) 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.

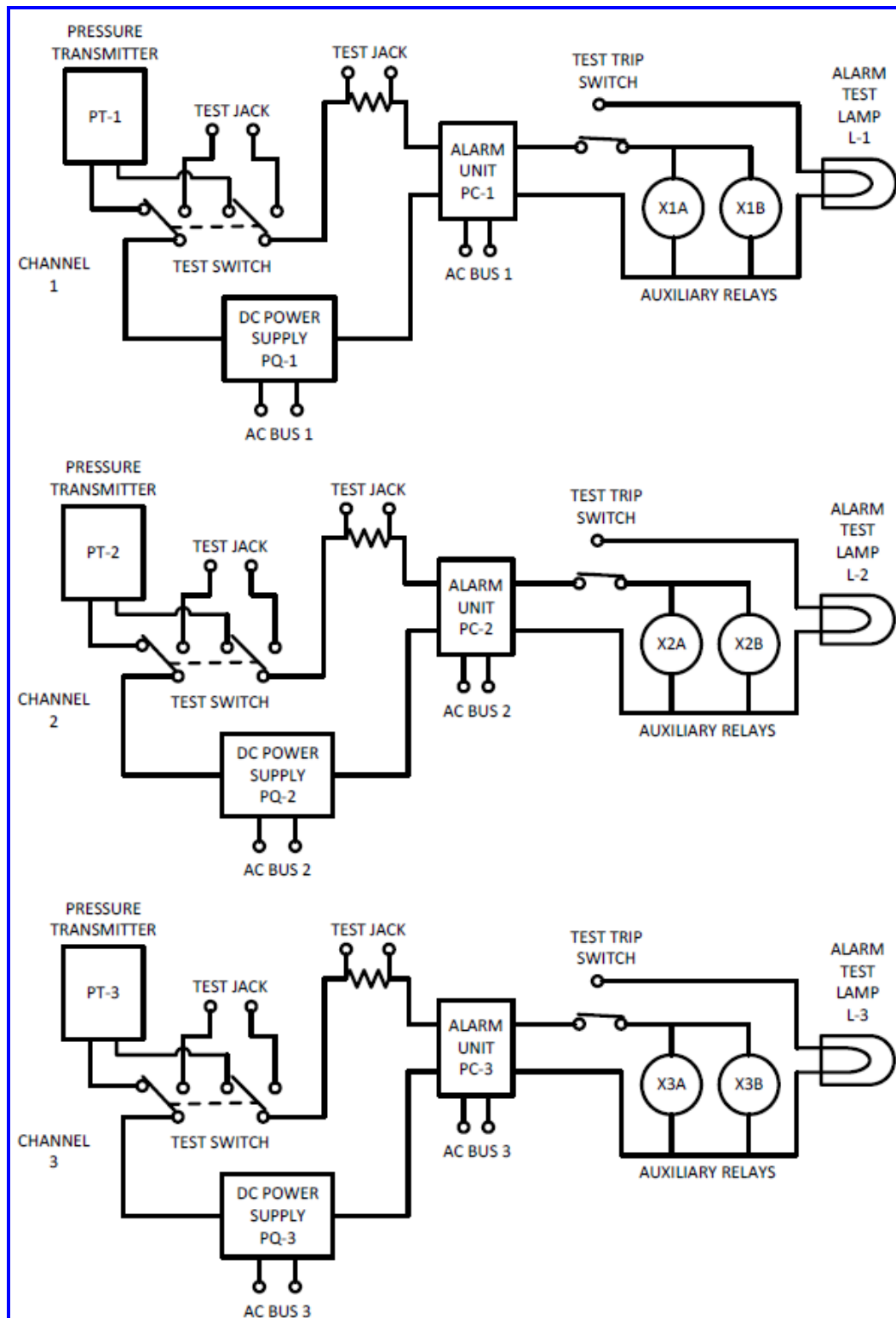
Column 6 [of Table 1](#) describes the ways that failure can be detected. In the absence of some means of detection, it is possible that loss of redundancy will not be noticed until the whole system fails.

Column 7 [of Table 1](#) contains information that the analyst may feel is pertinent to ~~his~~ [the](#) analysis, particularly whether the failure is acceptable or unacceptable.

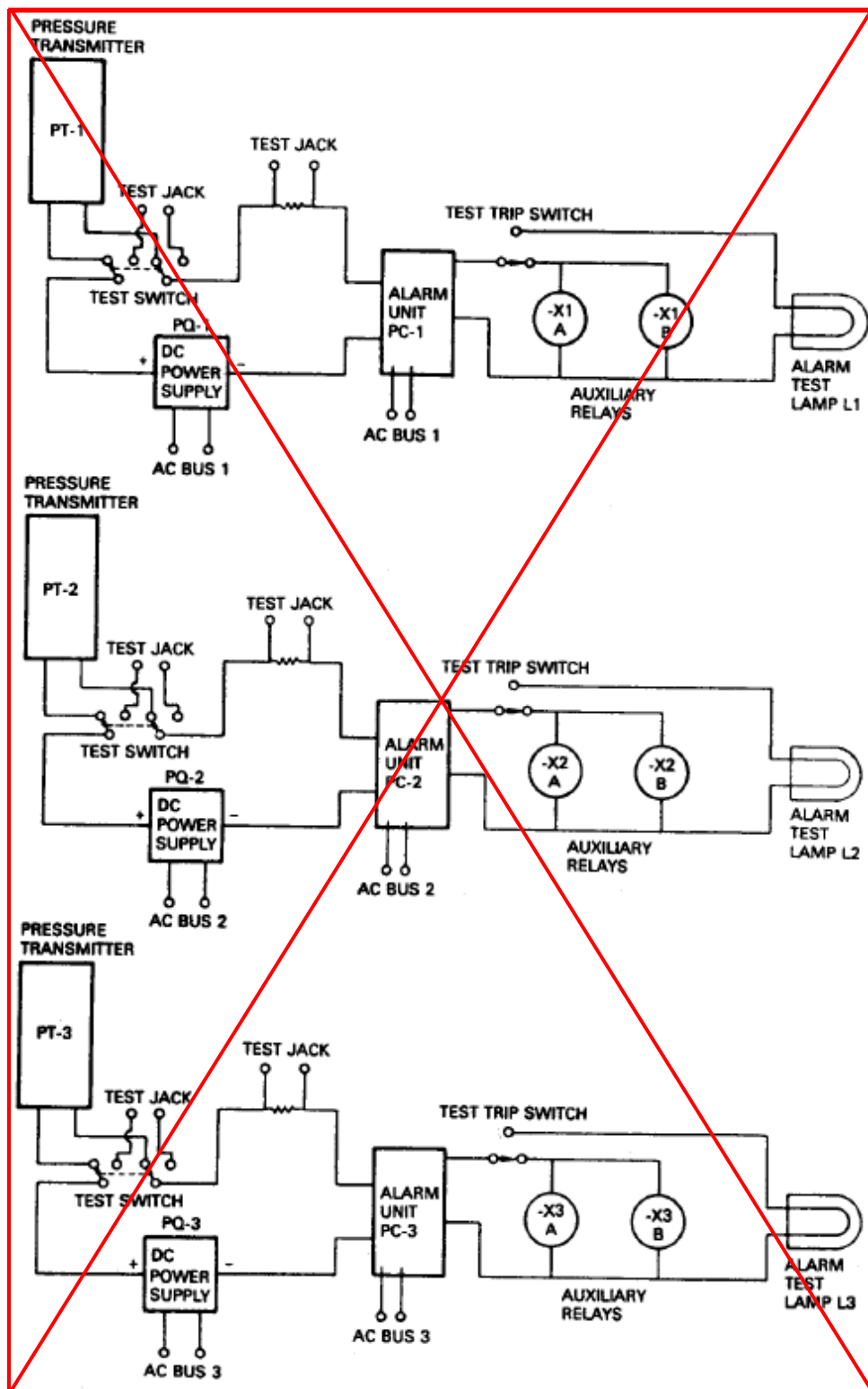
[Column 8 of Table 1 contains rankings for severity of the effect of the failure—S, probability of occurrence of the failure—O, and the detectability of the failure—D.](#)

5.3 Fault tree analysis

Fault tree analysis is a technique, (either qualitative or quantitative,) by which failures that can contribute to an undesired event are organized deductively in a logical process and represented pictorially. It is one way to diagram and communicate the information developed in ~~a failure mode and effects analysis~~ (an FMEA). The resulting arrangement is a treelike 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~~ [Figure 3](#). The symbols used are defined in [4.2.2](#) [5.3.2](#).

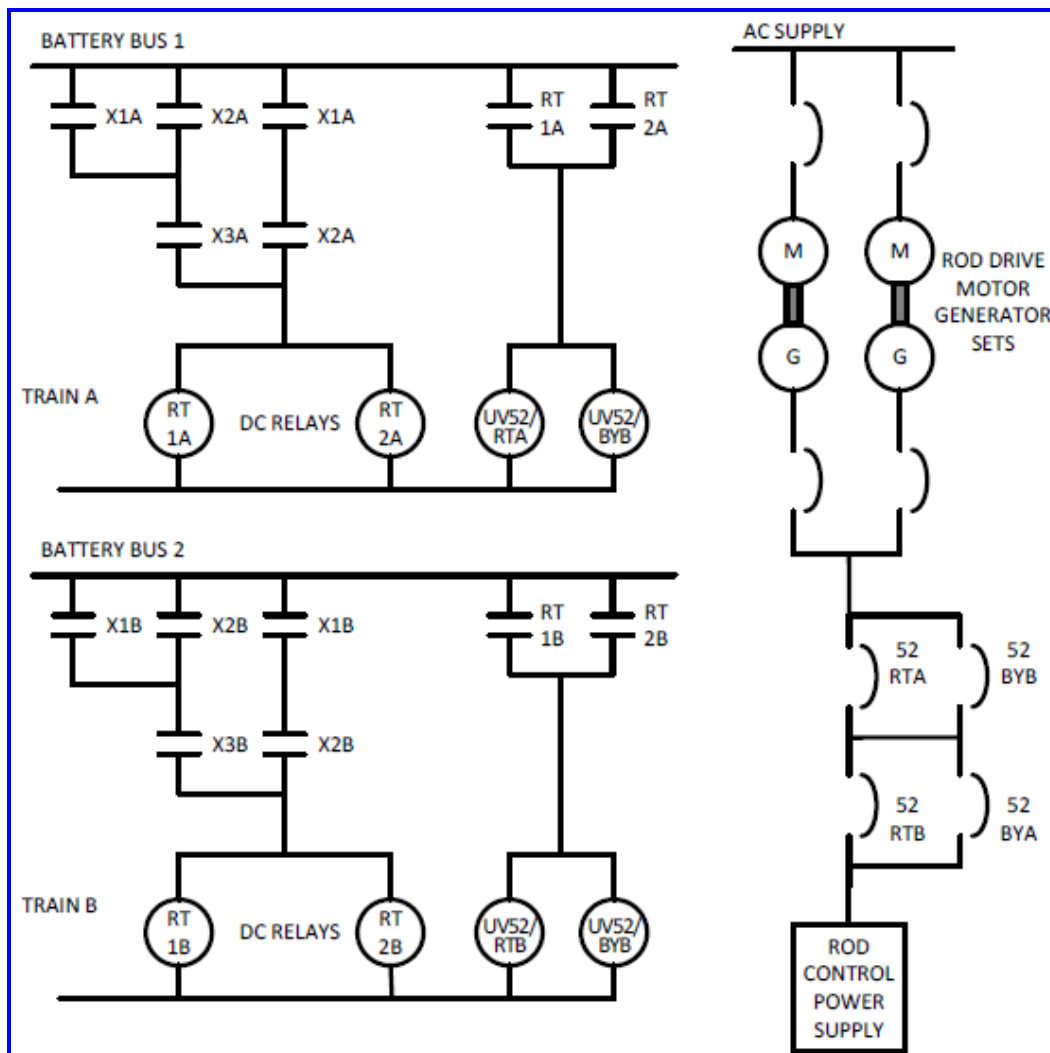


(New)



(Deleted)

Figure 1—Schematic of a typical reactor trip function—Channels 1-3



(New)

NOTE 1—BYA and BYB bypass breakers are connected only for testing.³

NOTE 2—Test switches shown in operate position.

NOTE 3—RT1A, RT2A, etc. are reactor trip auxiliary relays.

NOTE 4—52/RTA and 52/RTB refer to reactor breakers.

³Notes in text, tables, and figures are given for information only and do not contain requirements needed to implement the standard.

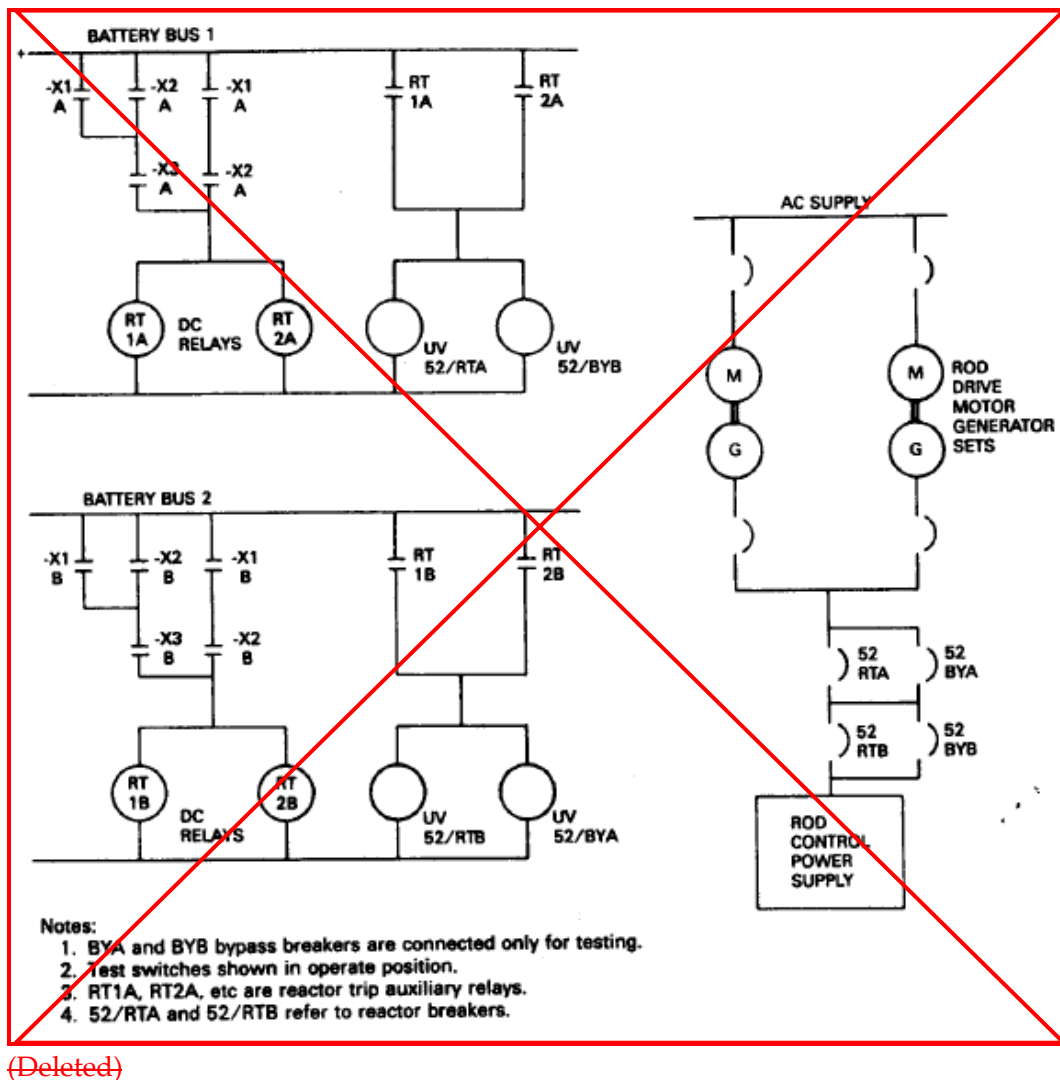


Figure 2—Schematic of a typical reactor trip function—[Trains A and B](#)

5.3.1 Functions and benefits of fault tree analysis

The primary features of ~~the~~ [this](#) technique are as follows:

- a) It forces the analyst to actively seek out failure events in a deductive manner.
- b) It provides a visual display of how the system can malfunction, allowing for an understanding of the system by persons other than the designer.
- c) It points out the critical aspects of system behavior.

- d) It provides a reference for the evaluation of modifications.
- e) It provides a systematic basis for progressing to a quantitative analysis.
- f) It provides consistent and clear documentation of the consideration of failure characteristics in the design process.
- g) It provides a basis for identifying multiple failures and common-cause failure mechanisms for the system.

5.3.2 Representation of events and operations in a fault tree

~~Because~~ Since 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~~ Figure 15. The symbols and their explanations are as follows:

- a) **Circle:** As shown in Figure 3, 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.

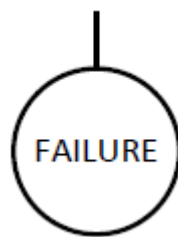


Figure 3—Circle

- b) **Diamond:** As shown in Figure 4, 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.

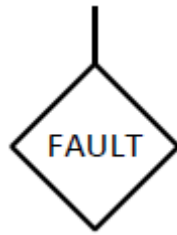


Figure 4—Diamond

- c) **Rectangle:** As shown in Figure 5, 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.

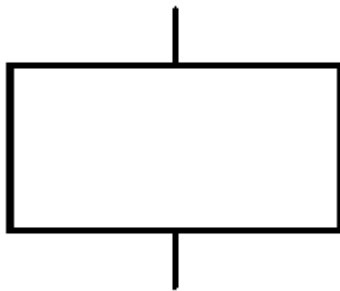
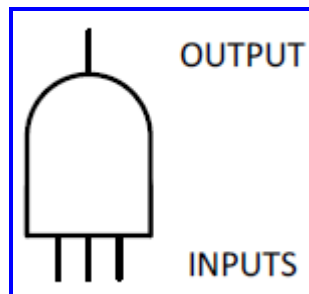


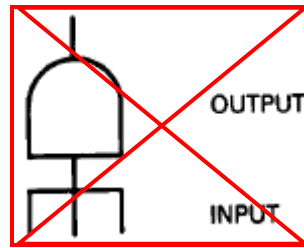
Figure 5—Rectangle

- d) **AND Gate:** As shown in Figure 6, the AND gate is the intersection operation of sets; that is, an output event occurs if and only if all the input events occur.



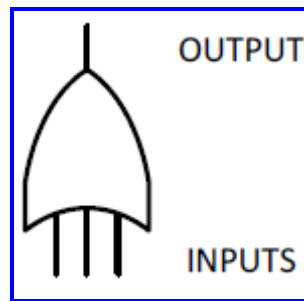
(New)

Figure 6—AND Gate



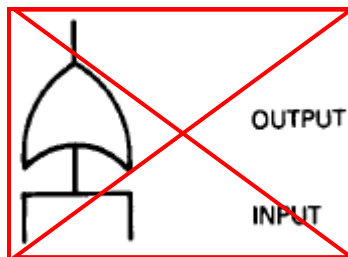
(Deleted)

- e) **OR Gate:** As shown in Figure 7, the OR gate is the union operation of sets; that is, an output event occurs if one or more of the input events occur.



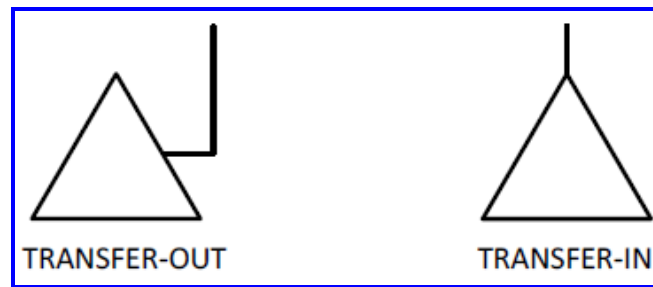
(New)

Figure 7—OR Gate



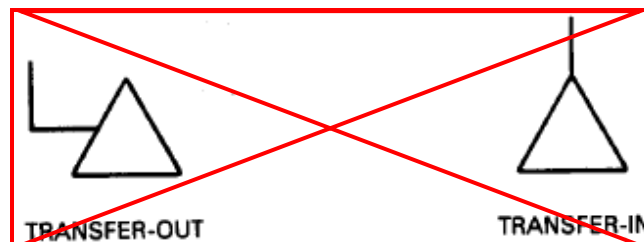
(Deleted)

- f) **Transfer Gates:** As shown in Figure 8, 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~~ (e.g., *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~~ rather than drawing it again it is simply inserted at this point.



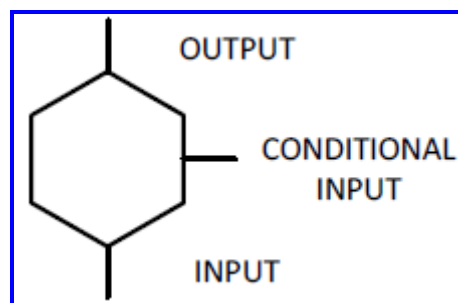
(New)

Figure 8—Transfer Gates



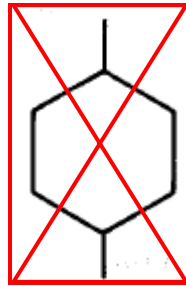
(Deleted)

- g) **INHIBIT Gate:** As shown in Figure 9, 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.



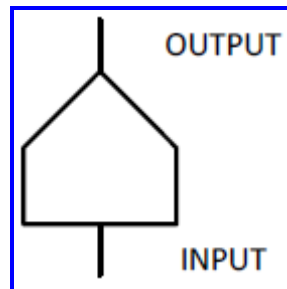
(New)

Figure 9—INHIBIT Gate



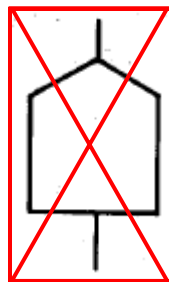
(Deleted)

- h) **The External Event, or House:** As shown in Figure 10, 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.



(New)

Figure 10 – External Event or House



(Deleted)

5.3.3 Procedure for constructing a fault tree

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

- a) Define system boundaries, success criteria, and initial conditions.
- b) 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.
- c) 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, [guided by the FMEA](#). They should be kept sufficiently general so that details of the system can be developed by subsequent branches.
- d) 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 (basic fault) or when a transfer gate can be used for another subtree ~~already~~ [previously](#) 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~~ [6.3.2](#).