ORNL
MASTER COPY

DATE ISSUED JUN 19 1972

[redacted]

ORNL
Central Files Number
72-3-39

RELIABILITY ENGINEERING METHODS IN REACTOR SAFETY TECHNOLOGY

P. Rubel

NOTICE This document contains information of a preliminary nature and was prepared primarily for internal use at the Oak Ridge National Laboratory. It is subject to revision or correction and therefore does not represent a final report. The information is only for official use and no release to the public shall be made without the approval of the Law Department of Union Carbide Corporation, Nuclear Division.

OAK RIDGE NATIONAL LABORATORY

operated by

UNION CARBIDE CORPORATION

for the

U.S. ATOMIC ENERGY COMMISSION

ORNL CF 72-3-39

Contract No. W-7405-eng-26

Nuclear Safety Information Center

RELIABILITY ENGINEERING METHODS IN REACTOR SAFETY TECHNOLOGY

P. Rubel
Instrumentation and Controls Division

JUNE 1972

OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37830
operated by
UNION CARBIDE CORPORATION
for the
U.S. ATOMIC ENERGY COMMISSION

CONTENTS

Page

FOREWORD ix

ABSTRACT xi

1. INTRODUCTION 1

1.1 Evolution of Reactor Plant Protection Systems 1

1.2 Practical Safety Considerations in Modern Protection Systems 3

1.3 Reliability Engineering Scope 4

1.4 Reliability Methods Applied to Reactor Systems 7

1.5 Safety and Reliability Guidance from Analysis 9

2. RELIABILITY OBJECTIVES 12

2.1 Reliability in Practical System Design 13

2.2 Goals for Use in System Analyses 14

2.3 System Serviceability 15

2.4 Reliability Optimization: A System Analysis Problem . . . 15

2.5 Implementation Goals 16

2.6 Formal Definition of Goals 16

3. RELIABILITY ANALYSIS 17

3.1 Rationale of Analysis 18

3.1.1 Logic Modeling 18

3.1.2 Probability Modeling 19

3.1.3 Qualitative Analysis 21

3.1.4 Evolution of Analysis Practice 21

3.2 Reliability Models 23

3.2.1 Reliability Analysis Model 23

3.2.2 Reliability Analysis Model: Addition of Events . . 23

3.2.3 Event Tree 24

3.2.4 Decision Tree 25

3.3 Qualitative Assessment of System Reliability 25

3.3.1 "Failure Mode and Effect" Analysis (FMEA) 25

3.3.2 "Common Mode Failure" (CMF) Analysis 26

3.3.3 "Single Failure" Analysis 26

3.3.4 System Performance Analysis 27

3.3.5 Network Simplification 27

3.4 Numerical Analysis 28

3.4.1 Probability at a Fixed Point in Time 28

3.4.2 Probability as a Function of Time 28

3.4.3 Systems with Repairable Elements: General Method 29

3.4.4 Systems with Repairable Elements: Steady-State Reliability 30

3.4.5 Reliability Measures: Calculation Objectives . . . 33

3.4.6 Evaluating Effects of Component Testing 38

3.4.7 Level of Analysis Detail 39

3.4.8 Simplification of Analysis: Depth Control and Cut Sets 40

3.4.9 Effects of Problem Variations: Sensitivity Analysis 41

3.4.10 Some Practical Aspects of Modeling 42

3.5 Computerized Analysis of System Reliability 44

3.5.1 "Automatic Reliability Mathematical Model" (ARMM) . 45

3.5.2 Analog Computation 47

3.5.3 "Monte Carlo" Method 47

3.5.4 "The Generalized Effectiveness Methodology Program" (GEM) 50

3.5.5 Later Programs Developed by Holmes and Narver, Inc. 51

3.5.6 "Kinetic Tree Theory" 52

3.6 Advanced Analysis Methods 52

3.7 Reliability of Operating Systems 53

3.8 Analysis Precision: Boundary Solutions and Confidence 54

3.8.1 Confidence in Operating Statistics 54

3.8.2 Confidence in Calculations to Establish Test Frequencies 55

3.8.3 Confidence in System Probabilistic Analysis Results 57

3.8.4 Analysis Evaluation by Boundary Solutions 58

3.9 Analysis of Reactor Systems 58

3.9.1 Salient Aspects of Protection Systems 58

3.9.2 Emerging Application Roles 60

3.9.3 Current Status and Trends: An Evaluation 62

4. RELIABILITY OF COMPONENTS 65
4.1 Failure Fundamentals 65
4.2 Failure Statistics 68
4.2.1 Frequency Distribution of a Random Variable 68
4.2.2 Reliability Function 74
4.2.3 Use of Statistics for Reliability Prediction . . . 74
4.2.4 Binomial Distribution 75
4.2.5 Confidence 76
4.3 Practical Measures to Assure Component Reliability 76
4.3.1 Component Qualification 76
4.3.2 Component Quality Control 78
4.3.3 Testing and Monitoring in Service 79
4.3.4 Long-Term Effects 80
4.4 Reliability Data Programs 81
4.4.1 Nonnuclear Component Data Programs 82
4.4.2 Reactor Component Data Programs 91
4.4.3 Status of Reliability Data Effort 96

5. RELIABILITY IMPLEMENTATION FOR REACTOR SYSTEMS 100
5.1 System Design for Reliability 100
5.1.1 System Design Criteria 100
5.1.2 Literature on Design of Protection Systems 102
5.1.3 Design and Review Practice 102
5.2 Components Qualification and Quality Control 103
5.2.1 Quality Assurance in Private Plant Construction . . 103
5.2.2 AEC "Quality Assurance" Program 104
5.2.3 Standards and Criteria for Components 104
5.3 Safety Research 105
5.4 Organization and Training 105
5.5 Reliability in Operation, Maintenance, and System Modifications 106

6. TOWARD A UNIFIED RELIABILITY EFFORT 108
6.1 Defining the Safety Reliability Requirement 108
6.2 Efforts to Establish Uniform Reliability Monitoring Program 110

7. CONCLUDING REMARKS 112
7.1 Emerging Analysis Roles 112
7.2 Aims in Analysis Development 115
7.2.1 Problem Formulation 115
7.2.2 Support Information 116
7.2.3 Model Evaluation 117
7.2.4 Analysis Uncertainties 117
7.3 Reliability Implementation 117
7.4 The Safety-Reliability Record 118
7.5 Viewpoints Abroad 118

REFERENCES 120

APPENDIX 131
Part 1: Analysis Basic Examples 131
1.1 Notations 131
1.2 Basic Examples 132
1.2.1 Direct ("Immediate") Probability Combinations . . 132
1.2.2 Combinations of Probability vs Time Functions . . 138
1.2.3 Probability vs Time Functions for Repairable Systems: "Markov Chain" Problems 143
1.2.4 Other Aspects of System Problems 146
1.3 Examples of Analysis by Computer Programs 150
1.3.1 "Analytical" Approach: by "Automatic Reliability Mathematical Model" (ARMM) 150
1.3.2 Monte-Carlo Simulation: SAFTE Program Concept . . 154
1.3.3 Monte Carlo Simulation to Identify System Failure Modes, Combined with Analytical Evaluation of Failure Mode Probabilities 159
1.4 Confidence 160
1.4.1 Basis of Confidence Calculations 161
1.4.2 Examples of Confidence Calculations 168

Part 2: Practical System Analysis Exercise 174
2.1 Basis System and Reliability Problem Statements 174
2.1.1 Function Diagram of System Conceptual Design: Core Spray System 174
2.1.2 System Performance Objective 174
2.1.3 System Reliability Problem Statement 174

2.2 "Simple" Reliability Analysis Formulation for System Conceptual Design 174

2.2.1 Basic Assumptions and Method 174

2.2.2 Analysis Block Diagram or Model 175

2.2.3 Data Input and Adaptation 175

2.2.4 Calculation of System Reliability 177

2.2.5 Assessment of "Simple" Reliability Analysis . . . 178

2.2.6 Additional Refinements 178

2.3 Failure Mode and Effect Analysis (FMEA) 178

2.3.1 FMEA for One Component of Conceptual Design . . . 178

2.3.2 Failure Mode and Effect Analysis — Detailed . . . 180

2.4 Fault Tree 183

2.4.1 Fault Tree for "Gross" Events 183

2.4.2 Fault Tree for "Fine Structure" Events 184

2.5 Decision Tree for Events in Example 2.4.2: "Multiple Outcome" Tree 185

FOREWORD

The Nuclear Safety Information Center, established in March 1963 at the Oak Ridge National Laboratory under the sponsorship of the U.S. Atomic Energy Commission, is a focal point for the collection, storage, evaluation, and dissemination of nuclear safety information. A system of keywords is used to index the information cataloged by the Center. The title, author, installation, abstract, and keywords for each document reviewed are recorded at the central computer facility in Oak Ridge. The references are cataloged according to the following categories:

1. General Safety Criteria
2. Siting of Nuclear Facilities
3. Transportation and Handling of Radioactive Materials
4. Aerospace Safety
5. Heat Transfer and Thermal Transients
6. Reactor Transients, Kinetics, and Stability
7. Fission Product Release, Transport, and Removal
8. Sources of Energy Release under Accident Conditions
9. Nuclear Instrumentation, Control, and Safety Systems
10. Electrical Power Systems
11. Containment of Nuclear Facilities
12. Plant Safety Features — Reactor
13. Plant Safety Features — Nonreactor
14. Radionuclide Release and Movement in the Environment
15. Environmental Surveys, Monitoring, and Radiation Exposure of Man
16. Meteorological Considerations
17. Operational Safety and Experience
18. Safety Analysis and Design Reports
19. Radiation Dose to Man from Radioactivity Release to the Environment
20. Effects of Thermal Modifications on Ecological Systems
21. Effects of Radionuclides and Ionizing Radiation on Ecological Systems

Computer programs have been developed which enable NSIC to (1) operate a routine program of Selective Dissemination of Information (SDI) to individuals according to their particular profile of interest, (2) make retrospective searches of the stored references, and (3) distribute scope and progress information on R&D contracts from the Program and Project Information File (PPIF).

Services of the NSIC are available to government agencies, research and educational institutions, and the nuclear industry on a partial cost recovery basis designed to regain a portion of the expense associated with disseminating the information to the user. A minimal inquiry response is available free. NSIC reports (i.e., those with the ORNL-NSIC numbers) may be purchased from the National Technical Information Service (see inside front cover) while documents indexed by NSIC may be examined at the Center by qualified personnel. Inquiries concerning the capabilities and operation of the Center may be addressed to:

J. R. Buchanan, Assistant Director
Nuclear Safety Information Center
Post Office Box Y
Oak Ridge National Laboratory
Oak Ridge, Tennessee 37830

Telephone 615-483-8611, Ext. 3-7253
FTS number is 615-483-7253

ABSTRACT

Reliability engineering seeks deliberately to increase the likelihood that devices or systems will function as intended. To this end, analytical techniques are routinely applied in such fields as aerospace, providing rational direction and emphasis to the quality assurance activities. Similar methods are applied, but less extensively, in reactor technology.

A survey of the current contributions of reliability engineering to reactor safety is reported, treating three major aspects: reliability goals, analysis effectiveness, and reliability implementation. The consideration of goals extends through formal risk evaluation studies, whose results have given insights toward defining the defense-in-depth protection requirement. Analysis methods, including those underlying the modern computer programs, are described in sufficient detail to support discussions of their capability to identify system failure modes and their limitations with regard to quantitative reliability forecasting. One of the main limitations is that of support data on components, which problem is introduced via consideration of the conclusive statistical information sought vs the fragmentary data available. Brief descriptions of the data banks and other efforts indicate progress in combining information of diverse origins to develop component reliability estimates. Practical expressions of the reliability principles are summarized in terms of system design features, quality assurance measures, and standards.

The report concludes that the reactor quality assurance programs present most features of formal reliability programs in other areas. However, quantitative analysis is slow in gaining acceptance due to three factors: (1) the dearth of support information, (2) difficulty in formulating problems that correspond to reactor contingency conditions, and (3) lack of consistency in analysis execution.

1. INTRODUCTION

From a practical viewpoint, reactor safety is the prevention or countering of a finite range of plant contingencies that have potential accident consequences. The basic problems are mainly understood. To find effectual solutions is a serious engineering challenge, but one that is both realistic and amenable to proven disciplines.

At least with regard to light-water-cooled reactors, the essential performance parameters have already been established[107,108] for systems intended to prevent excessive accidental release of fission products. This report takes up succeeding questions of what is being done to assure that such systems will respond adequately whenever called upon. The major emphasis here is on the application of reliability engineering methods to enhance the practical safety efforts. Some of the work described, however, goes beyond the traditional reliability considerations to address related problems in system and decision analysis.

1.1 Evolution of Reactor Plant Protection Systems

The prime safety concern of the early reactors was the possible uncontrolled reactivity and power excursion which, if not promptly terminated, could result in an accidental release of radioactive materials. To prevent or counteract excursions, these reactors were provided with automatic shutdown or "safety" systems that could quickly reduce reactivity, for example, by inserting neutron absorbers or removing fuel. Fission product accumulations were then small, or at least not concentrated, and reactors were designed to emphasize inherent power excursion limiting or terminating characteristics; even failure of a safety system constituted more of a local threat than a public hazard. Nevertheless, the uncertainties associated with excursions and releases were regarded as sufficient reason for providing containment enclosures. The industrial-type buildings which housed the reactors were generally adequate, although facilities for sealing major openings, controlling ventilation, and filtering exhaust discharges were frequently required.

Practical power production from reactors meant large cores and high power densities, hence substantial inventories of fission products.

Afterheat removal therefore became a major consideration in the large reactors. Forced circulation of the primary coolant and facilities for secondary heat rejection are now commonly provided to handle the shutdown requirements, normal as well as under most contingency conditions. Special provisions are made for core cooling in the event of coolant escape from the primary loop. Containment has continued to be mandatory in the United States and, for the larger reactors, now entails massive structures and complex systems both for closing off penetrations in emergencies and providing containment cooling.

The engineering of systems to perform the above safety-related functions has traditionally evolved from consideration of the more disruptive events or event combinations that could be postulated. Those situations posing the greatest potential hazards have also been the focus of studies to evaluate containment effectiveness and plant siting acceptability; such major contingencies were at one time designated "maximum credible accidents" (MCAs). Emphasis on the major potential accidents in regulatory reviews and public discussions of reactor safety then gave rise to the popular impression of an "MCA approach" to reactor safety.

In a practical sense, it is the most disruptive events which establish the extreme requirements for containment structures and other protection features. As this became recognized, attention shifted to the "design basis accident" (DBA), similar in concept to the MCA but more viable and better able to identify significant ranges of accident conditions. Many general system requirements thus determined are reflected in the AEC design criteria.[28]

In water-cooled reactors, the most challenging accident has generally been the "double-ended" rupture of a large pipe in a primary coolant loop, that is, at a point where massive blowdown flow out both openings occurs. Hence, through usage, MCA and later DBA became closely identified with the double-ended rupture case. Although this problem is still prominent in public discussions of reactor safety, the many less significant accident-initiating events have not been overlooked. Thus, a major area of concern has always been the uncontrolled reactivity addition, protection against which is afforded by features preventing control rod ejection, simultaneous

rod withdrawals, steam void collapse (BWR), and sudden cold water addition. More recent studies continue to reveal additional needs and opportunities to head off potential accidents at early stages. For example, the desirability of allowing essentially no melting of fuel in reactors of high power density, once established, led to adoption of features to ensure cooling of BWR cores in the event of small-to-intermediate ruptures of the primary coolant boundaries. These features were, mainly, emergency coolant injection at high pressure, with automatic pressure relief to advance the time at which low-pressure flooding and spray can be applied.

From the DBA approach evolved the present general plant design objective of "defense in depth" against the consequences of each major disruptive event. The multiple defenses invoke a wide range of functions which are executed primarily by the "engineered safety systems" or "plant protection systems." Additional features counter less severe contingencies, mainly with a view to investment protection but also promoting safety. Closely integrated with the primary safety functions are their supporting auxiliary systems, such as energy source and distribution facilities, equipment lubrication and cooling systems, and monitoring and control arrangements. Conventional plant protection features also factor into the safety problem, including fire and security arrangements and the various equipment safety devices.

1.2 Practical Safety Considerations in Modern Protection Systems

The primary protection functions correspond generally to equipment systems, for example, an array of pumps, valves, heat exchangers, and controls making up a cooling loop. Such systems are semiautonomous in that they utilize mostly equipment dedicated to the basic system function, yet may also call upon some shared facilities and are subject to considerable control interaction with other functions. Most typical of the shared facilities are the sensing and logic subsystems which initiate the main system actions, and the energy supplies which can be common to many systems. Major equipment items like large pumps are permitted to serve more than one system except where such alternate duties would conflict. The control

interactions are primarily to coordinate the various functions by selecting, timing, and sequencing equipment responses; they are effected not only through central control arrangements but also by many individual interlocks and other local control devices.

Different combinations of the semiautonomous protective functions are arrayed to cope with the various plant contingencies. Thus, a master system is formed ad hoc in response to each situation of safety interest and hence presents a discrete problem in system effectiveness. Each such situation has its own set of performance criteria, and each master system offers a set of alternative responses when preferred actions fail or are degraded.

The protection system overall, in addition to its specific functional capabilities, must offer a high probability of responding in sufficient strength to prevent or mitigate every potentially serious accident. Adequate response is sought through (1) extensive review of system design to minimize opportunities for misoperation or improper defeat of system responses, and through (2) assurance of equipment reliability. The sheer number of components and degree of overall system integration demand that such efforts be deliberate, methodical, and comprehensive.

An organized approach to protection system development has the added advantage of thorough documentation. Since much of the progress in these systems has been by adding new features and modifying previous designs, such documentation becomes desirable as a reference basis for examining the overall effects of proposed changes. This is particularly true where the work must be done under pressure of construction schedules or subject to constraints in back-fitting to existing plants.

1.3 Reliability Engineering Scope

Reliability engineering has developed as a separate discipline only since the time of World War II, the same period in which reactors have progressed from laboratory experiment to a practical source of energy. Almost all the reliability concepts and methods were understood and, to some degree, practiced before this time. But it required the impetus of advanced

aerospace and weapons programs to organize a wide range of contributing activities effectively to produce reliable systems on a short time scale. The activities individually should be so familiar to the engineer that he may at first question the exalted status of the "new" discipline. They include system design and design review, emphasizing such features as redundancy and fail-safe (e.g., as in early railroad air brakes); component development and testing to assure qualification for specific severe duty (e.g., modern gear lubricants); quality control (e.g., dimension tolerance control by statistical sampling analysis, vital to machinery mass production); mortality statistical analysis (e.g., as practiced by insurance actuaries and later adapted to depreciation accounting, etc.); and analysis of combined probabilities (practiced intuitively in everyday life and more formally by consistent winners at poker).

The basic premise of reliability engineering is inferred from the customary definition of reliability, that is, the probability that a system or component will perform in the manner intended for a specified interval and under specified circumstances. Via the activities just described, it is sought deliberately to raise the success probabilities to the highest levels consistent with improvement costs and failure consequences.

The major departure of reliability engineering from the traditional approaches is in the extensive use of analysis, qualitative as well as quantitative, to provide rational overall guidance for the support activities. The procedure is far from being an exact science. However, it has added a large measure of discipline to projects by (1) identifying performance goals, (2) evaluating elemental probability factors that can be deduced from relevant experience, (3) introducing speculation in a controlled manner where required, and (4) organizing and allocating resources consistently to meet the requirements. Quantitative analysis has enjoyed favorable exposure due to both the attractiveness of its mathematical approach and some early dramatic successes in aerospace applications. Contrary to popular understanding, however, analysis practice is concerned at least as much with identifying and describing qualitative cause-and-effect relationships as with numerical evaluation of probabilities.

In learning to deal effectively with complex systems, the major reliability programs have accomplished much in the areas of organizing and partitioning the analysis work so as to concentrate on problems of practical significance and yet minimize the burden on technical specialists. The problems have occasioned the development not only of the formal methods described in Chapter 3, but also of many detailed implementation procedures. The procedures primarily facilitate handling of the sometimes enormous quantities of raw data and refined information which are input to the analyses.

Reliability engineering has further been concerned with reducing guidance to practice. As a result, many effective techniques have been developed for expressing reliability considerations ultimately in terms of engineering decisions, technical requirements, and administrative policies. These influence not only isolated design recommendations, but even the direction or formulation of entire support programs, for example, quality control.

Some of the formal procedures used appear tedious in many respects and demanding of expensive manpower. This has tended to limit their use to vital projects. More generally, it means that the costs of using specific reliability methods and undertaking elaborate analyses must be weighed against the potential benefits or against alternative simplified versions.

The fundamentals of reliability engineering now are thoroughly treated by a number of texts, several of which are referenced here.[1–6] Currently the literature is becoming more specialized as attention shifts to problems identified by analysis but not yet satisfactorily resolved. Both the texts and the recent work extensively document reliability practice; however, as might be expected, most of the material emphasizes the mathematics and is strongly oriented toward weapons and aerospace equipment, which have reliability considerations somewhat different from reactor systems.

Attention is called to two modern and comprehensive works. First is the NASA series entitled "Practical Reliability,"[15–19] which presents the fundamentals along with modern aerospace applications. The other is the UKAEA report, "Safety Assessment with Reference to Automatic Protective

Systems for Nuclear Reactors,"[98] covering in detail many reliability considerations for reactor systems. Also noted are the extensive, subject-classified bibliography[68] prepared by the Liquid Metals Engineering Center and the literature review[26] reported by Schultz and Geisler.

Additional reference sources for current developments in the reliability field are the proceedings of two series of conferences: (1) Annual Reliability and Maintainability Conference, sponsored jointly by the AIAA, SAE, and ASME; and (2) Annual Symposium on Reliability, sponsored jointly by the IEEE, SNT, FES, and ASQC. Reviews and abstracts of reliability literature through December 1970 are available in the periodical Reliability Abstracts and Technical Reviews (RATR), sponsored by NASA.

1.4 Reliability Methods Applied to Reactor Systems

There has been no lack of awareness of the potential contribution of reliability engineering methods to reactor safety. In fact, many of the methods and precepts highly developed for military systems have been successfully applied throughout the course of reactor development. Practical difficulties have delayed adaptation of other techniques, notably the application of numerical analysis to assess absolute probabilities in a consistent and convincing manner.

Early recognition of the probability aspects of safety is evidenced by a 1953 internal report[34] at Oak Ridge National Laboratory, in which Jordan expanded on the admonition to "get statistical safety." At the time there was much concern over the unreliability of reactor control equipment, particularly the detection chambers, cables, and electronic gear that comprised the neutron flux measurement channels. "Statistical safety" then was rapidly being reduced to practice via the application of redundant instrument channels in the safety-shutdown systems. Thus, the most dramatic of the reliability benefits that analysis had brought to other fields were capitalized on long before formal analyses were being performed on safety systems.

The "Single Failure Criterion" became a popular and convenient expression of the redundancy concept. Practical refinements of the redundancy principle soon followed, such as independence, diversity, physical

isolation and protection, and fail-safe features, all applied mainly to safety instrumentation. Although these measures were taken initially perhaps more out of consideration for the equipment shortcomings than for other reasons more prominent today, they are recognizable as an early version of "Common Mode Failure Protection" (i.e., preventing function failure due to single event or deficiency affecting redundant equipment). With usage, such practices gained general acceptance as the protection system design principles and are reflected in the design criteria. The same principles are now recognized as applying beyond the instrumentation to all aspects of the protection systems. They have given much of the actual direction to the current safety and reliability analysis work, mostly qualitative, which seeks to assure "defense in depth" against accidents and freedom from common-mode failures.

The equipment comprising the early protection systems (i.e., the safety or safety-shutdown systems) was novel, developing and changing rapidly, and produced only in small numbers. These circumstances were not conducive to obtaining the kinds of experience statistical data needed to support numerical analysis of system reliabilities. Consequently, only limited use was made of such methods. Neither the equipment nor the applications are by any means standardized yet, but considerable progress has been made in gathering what relevant information there is and, where direct experience is lacking, in methodically synthesizing component reliability estimates. Many of the "nonstandard" conditions involve conventional large components like pumps, which are mainly custom designed and installed.

Component qualification was a principal development objective rather than a routine matter of reliability engineering for the early safety systems. Currently it is a central consideration in the refinement phases of reactor equipment development and figures largely in the present reactor reliability efforts.

Quality control at one time was more or less presumed to follow from the high technology environment of reactor projects, an attitude not entirely vindicated by experience. With reactors being reduced to commercial practice, however, it soon became obvious that quality control standards

more stringent than ordinary industrial requirements were necessary for safety-grade reliability. Such standards are now being developed and implemented rapidly. In fact, the effort to achieve effective quality control is presently emphasized perhaps more than any other formal aspect of reactor systems reliability, as a major factor in overall "quality assurance."

A natural extension of certain conclusions developed from analysis has been into the areas of testing and maintenance. For example, where intuition tells us that an item frequently tested will not remain long undiscovered in a failed state, analysis now provides effectual guidance in determining suitable test intervals. Decisions regarding allowable downtime for maintenance are similarly being resolved on an objective probability basis. Ultimately there always remains the question of whether the reliability of a vital system is adequate, and objective methods are beginning to address this problem too.

1.5 Safety and Reliability Guidance from Analysis

Objective quantitative analysis has long promised the ultimate in guidance to reliability efforts by virtue of combining mechanistic, probabilistic, and economic considerations all on a common basis. Stimulated by successes in the aerospace and weapons fields, the prospects for extensive analysis application to reactor systems began to receive serious attention around 1964. The thorough treatment of the subject by the UKAEC, referred to above, appeared shortly thereafter, closely followed by the work of Planning Research Corporation and Holmes & Narver, Inc., and accounts of several actual system analyses. The literature anticipated that the major benefits of analysis could largely be realized at reasonable effort and proposed to attack some very broad problems by such methods.

The initial attempts on the broad problems, as well as the less ambitious practical studies, produced considerable controversy and some disappointment. Most of the controversy centered on defining safety-related reliability goals and on whether objective analysis could ever indeed point the way to complete safety assurance. The controversies are still far from being resolved. But while the principal goals remain those derived from

consideration of specific potential accidents, the present trend toward more objective assessment of both goals and systems must be credited at least partly to the analysis impact.

The extent of initial disappointment has been evident from criticisms of analysis credibility on grounds of questionable data, inadequate depth, and sometimes unrealistic problem formulation. But both the analysis capabilities and the attitudes toward its use are maturing. With understanding has come an appreciation of the practical limitations and, hence, what are the valid and worthwhile applications. The most serious of the limitations is now recognized as being the extent to which we can, as engineers, anticipate the system failure mechanisms; in this regard methodical qualitative analysis has added to our capability. Again, the ease with which analysis combines fact and speculation impartially has occasioned some distrust of conclusions so derived; but speculation has always been honorable in evaluating uncertain situations, and the mature viewpoint requires simply that its use be fully acknowledged.

Attention to the analysis aspect of reliability has perhaps been proportionally greater than its present influence on the larger-scale safety implementation activities. Nevertheless, it represents not only a state-of-the-art trend but also the most satisfactory frame of reference in which to review many of the safety efforts. Accordingly, this report attempts to impart a knowledge of those reliability analysis methods currently contributing to the reactor technology. Most of the subject matter is necessarily devoted to describing the fundamentals and specific techniques. However, the main arguments concern the analysis limitations and quality, what valid insights or conclusions analysis can develop, and how such conclusions can effectively be reduced to implementation practice. It is hoped to provide, in the analysis context, a reasonable perspective of the safety prospects overall.

The report treats reliability from an engineer's standpoint. This statement is partly by way of apology for introducing practical engineering considerations to modify, interpret, and evaluate otherwise pure probability concepts. It further disclaims the need to treat rigorously here all the fundamental concepts called upon, and which are fully developed in

the texts. Instead, a concise tutorial development of those principles directly contributing to an understanding of current computer-aided numerical analysis was attempted via the simplied and highly selective examples of the Appendix, with support from Chapters 3 and 4. The need for a basic presentation was felt strongly by the author, particularly in view of difficulties in extracting underlying concepts from the current literature. It is hoped, therefore, that the examples will serve as a worthwhile review or summary to those readers having a good theoretical grasp of the subject; for others it should provide a relatively painless introduction by establishing the rationale with simple mathematics and preparing the reader for the more advanced treatments, divergent presentations, and sometimes arcane languages of the extensive literature.

2. RELIABILITY OBJECTIVES

The projects under which reliability engineering took form have benefited from clear-cut main goals to which definite values could be attributed. However, resolving these goals into subordinate reliability requirements on the vital functions, systems, and equipment has generally been a persistent problem. The problem is essentially one of optimization; that is, while many avenues are open for improving particular aspects of a system response probability, each must be weighed objectively in terms of relative effectiveness, cost, and possible undesired effects on other response factors.

From time to time similarly objective sets of reliability goals have been sought for reactor protection systems, but with results that were far from conclusive. Some approaches through risk analysis are discussed in Chapter 6. The most serious difficulty seems to be that protection systems, by virtue of both being and having backup facilities, introduce two complicating factors into the goal rationalization: (1) the need for a protective action is conditional on events so rare in a well-conceived plant that their frequency is indeterminate and (2) the consequences of any one protection channel failing to respond properly in a modern plant depend not only on the effectiveness of other protection and operating facilities, but on many chance effects as well. Thus multiple defenses, while enhancing safety, place the problem of reliability goal optimization perhaps beyond a really satisfactory solution.

Possible exceptions to the above are portions of the reactor scram systems and a few other facilities that must respond to fairly frequent operating contingencies, for example, turbine-generator forced outages. For these systems it may eventually prove feasible to base reliability requirements on outage rates experienced by utilities and estimates of direct failure consequences.

In lieu of quantitative goals, the safety requirements for high reliability have gained expression in terms of specific system features and design objectives and quality assurance practices. Interpretation of the

requirements must be somewhat subjective, but with usage has come improved understanding and consistency in application.

2.1 Reliability in Practical System Design

The USAEC regulatory policy regarding reactor plant safety has been to establish broad criteria and to hold the reactor industry responsible for developing detailed design and quality assurance requirements.[122] To a large extent, however, the detailed requirements have been inferred from case conclusions by the Advisory Committee on Reactor Safeguards (ACRS), the AEC Division of Reactor Licensing (DRL), and other agencies. Similar guidelines have been adopted for government-sponsored reactors. Moreover, much of the information needed to justify the specific system requirements has been generated from research activities sponsored by the Division of Reactor Development and Technology (DRDT).

Regarding reliability, the broad criteria in effect require that safety or protection systems be separate from normal operating systems and that independent-redundant facilities be provided to perform those functions designated as protective. Safety analysis studies are performed for each plant to determine the necessary protective functions. The actual degrees of redundancy, independence, and diversity vary a great deal among the various functions. That is, a particular result may be achieved with duplicate or diverse equipment, or both, and some safety functions will be provided with much higher effective redundance than the minimum.

The different reliability treatment accorded the various functions is more than mere engineering expedient. It represents, to a large extent, value judgments on the importance of the functions; such judgments have accumulated to form what now amounts to a very large body of design precedent.

Wherever practical, the precedents are observed and interpreted as a means to evaluate proposed new plant designs, thus contributing to the consistency of the designs and the efficiency of the review procedure. However, there is some concern that this procedure also tends to divert attention from novel opportunities to enhance safety and sometimes burdens plants with protection features of perhaps marginal value. The case for

the first point is the current emphasis on protection systems, with little attention or credit being given to the operating systems' potential for reducing accident risks. Protection value concerns mostly features that have been proposed to back up or enhance systems previously provided; industry has questioned whether some of these need be furnished in duplicate, that is, according to "safety" standards, or even provided at all.

2.2 Goals for Use in System Analyses

Without quantitative guidelines, it is still reasonable to set up transitory standards of reliability for evaluating individual systems or functions. One practical method is to develop reference values by analyzing designs that have been thoroughly (if subjectively) reviewed and found acceptable, i.e., to "observe the tradition." This approach offers convenient bases for comparing reliabilities of alternative designs, evaluating features within systems, etc. In other areas, conservative design practice will routinely yield theoretical reliabilities higher than the level where such numbers are meaningful, thus avoiding the immediate concern over assigning quantitative goals.

Regardless of whether a reliability goal is reached objectively or is adaptive, it should at least be clearly defined with regard to function. This point seems self-evident, which is perhaps the reason it has been slighted in the texts. However, incorrect or inadequate understanding of the critical system functions can easily cause attention and resources to be wasted on trivial features. In some instances this has led to actual unreliability of systems.

Typical of the misunderstandings that arise in defining reliability objectives is the discrepancy between the vital functions of concern in the reactor safety literature and the systems for which reliability analyses have been reported. The literature seems to stress realistically the capability to perform vital functions under adverse circumstances; moreover, the functions often involve sets of, rather than individual, systems. By contrast, the formal analyses have been rather restricted to discrete hardware systems; in addition, indiscriminate use of "average service" component reliability data in the analyses suggests neglect of special

operating conditions. Such discrepancies, without supporting justification, tend to discredit analysis-based claims of reliability. The remedies, discussed in later chapters, amount to a broadening and clarifying of the reliability problem objectives and more intelligent use of the data.

2.3 System Serviceability

Hanauer and Walker[37] define serviceability as ". . . the propensity to be free from safe failures," and regard a "safe" failure of a protection system as one in which the system is actuated when not demanded by plant conditions. A safe failure sometimes implies an economic loss. Whether such a failure is always benign with regard to overall accident risk is questionable, since it may stress critical equipment or may induce a safety requirement for another protective action. Therefore, the serviceability aspects of protection system reliability deserve special consideration in establishing the reliability goals.

Serviceability of operating systems has similar safety significance, but the economic incentives here appear well enough recognized to assure adequate attention.

2.4 Reliability Optimization: A System Analysis Problem

The theoretical reliability of a system or subsystem can be represented, by methods shown in Chapter 3, as the combined probability of fulfilling a number of specific requirements. If those individual factors which correspond to design features are then manipulated within the formal problem setup or model, their effects on overall reliability can be studied methodically. Assigning costs to each alternative expands the problem to one of cost-effectiveness optimization.

Valuable guidance with regard to design decisions and placement of emphasis in other reliability implementation efforts is gained from such optimization studies. However, the need for realistic problem formulation, discussed in the preceding section, is especially acute in this area.

Optimization problems, being iterative and demanding of accuracy, tend to be burdensome in regard to calculation effort. Where many were previously impractical for hand methods, the computer is now expanding the

opportunities. Moreover, it is no longer necessary to resort to reliability models so simplistic that they hopelessly obscure comparisons of system features.

2.5 Implementation Goals

The objectives discussed thus far have been in terms of probabilities of successfully executing defined functions. To adopt such goals implies a readiness to undertake all practical measures to implement the reliabilities assumed in or promised by the theoretical considerations. The practical measures have subsidiary goals of their own, some self-evident and others identified from formal reliability studies, as described in Chapters 4 and 5.

2.6 Formal Definition of Goals

In addition to the reactor manufacturers, several organizations are actively engaged in establishing useful reliability objectives as the bases for standards or criteria. These include the Joint Committee on Nuclear Power Standards of the Institute of Electrical and Electronics Engineers, Subcommittee 5, Reliability; and the AEC Division of Reactor Development and Technology in cooperation with the Standards Program of the Oak Ridge National Laboratory. These efforts are discussed further in Chapter 5.

3. RELIABILITY ANALYSIS

Much of the modern development of reliability as a discipline has centered on techniques for determining how a complex system can fail and estimating the chances that it will fail. The ultimate analysis expression is the system probabilistic model, which has evolved to various highly refined forms from the simple premise that the success or failure probability of an array of functionally dependent, failure independent elements is determined by the elemental probabilities. Computers now handle the vast amount of mathematics entailed in combining the elemental probability functions for large systems, and efficient procedures are available to organize the input information.

The main intent of this chapter is to describe the present and potential applications of reliability analysis methods to system problems in reactor safety. Since the considerations are largely technical, the subject background is developed from the logic and probability fundamentals through sufficient method detail to convey an appreciation of the useful capabilities of analysis as well as its practical limitations. Two main analysis aspects, model construction and probability evaluation, are first considered separately and are then combined in the discussions of the computer methods. Up to Section 3.9 the material is fairly general; however, many implications with regard to reactor problems are expanded upon. Section 3.9 focuses the preceding material on reactor system analysis applications so as to explain the current status, difficulties, and development aims in this area.

The examples in the Appendix supplement the text in this chapter. Part 1 develops the basic logic and probability concepts in a sequence leading to their ultimate application in computer analysis programs. Part 2 simulates a protection system case study, emphasizing qualitative methods and practical analysis difficulties.

3.1 Rationale of Analysis

The intuitive approach to an unfamiliar problem is to assemble and diagram all the information one can bring to bear, however diverse. Reliability analysis extends this approach. Thus the various modeling techniques emerge as refinements on problem diagramming, whereby individual considerations are reduced to common terms, ordered logically, and placed in perspective with regard to importance. And while analysis alone cannot introduce a consideration until it has been envisioned in a physical sense, the methodical exercise is very useful in directing attention to factors that otherwise might be overlooked.

3.1.1 Logic Modeling

The logic analogies to actual system functions as well as to block diagrams are readily apparent for switching matrices; in fact, telephone exchange switching problems stimulated much of the work underlying modern systems analysis practice. Thus, switch arrays effectively form "and," "or," etc., configurations, all subject to the classical rules of combination. Extending the analogy to more general functions was quite natural. The early models corresponded directly to the system components, consideration of which was restricted to simple ability to sustain or impede the system function. Subsequently it was sought to represent a broad range of actual reliability considerations as events of logic or decision significance.

The diagrams in Examples 1.2.1.1, 1.2.1.2, 1.2.1.5, and 1.2.1.6 of the Appendix illustrate a few simple logic relationships of the type just described. Each box shown could represent a switch function or any other explicit requirement for meeting an objective that corresponds to a completed circuit path across the array. For analysis purposes, the logical objective may just as well be system failure as success; in failure arrays, the "closed switch" then represents a system requirement not satisfied, for example, a vital component broken. The block diagrams for Examples 1.2.1.3 and 1.2.1.4 do not adequately represent the associated logic statements, although they do correspond to physical connections among components. A switch diagram accompanying Example 1.2.1.3 illustrates the necessary diagram modification to achieve a rigorous logic model.

Where reliability considerations are reasonably simple and straightforward, diagramming may provide immediate insights merely by inspection. Often from the diagrams alone one can not only identify directly which factors are vital but form some opinion on their likelihood and project desirable system improvements. Complex systems, not so readily visualized, require formal truth-table analyses to identify combinations leading to ultimate system outcomes; here the computer is called on to test endless combinations of logic element aspects in a large array. Example 1.3.1.2 illustrates the computer approach to a truth-table solution.

3.1.2 Probability Modeling

By assigning a probability factor to every elemental condition or requirement in the logic model, one places each consideration in perspective as to its relative importance to system reliability. The array of such factors comprises the probability model about which system quantitative reliability problems are formulated. There are various ways to express the elemental probability factors, for example, as instantaneous values or as functions of time, and in each problem it is necessary to select those consistent with both the problem statement and the data. Evaluation of the combined probabilities follows methods derived from game theory.

The two basic assumptions implicit in all probability modeling are event independence and event randomness in time. Since interpretation of these concepts is sometimes troublesome, they deserve attention at this point.

The event independence of reliability interest usually pertains to component failures. For the simplest models, the meaning is clearly that no component failure explicit in a model is the immediate and direct cause of another failure in the same model. More complex models may include hierarchic failure sequences, whereby some failure of system significance may develop in any of several ways; although that failure is evidently no longer independent in a physical sense, the model requirement is still satisfied if all the initiating events at the front of the failure sequence are indeed independent. Modeling techniques can readily accommodate the independent event which simultaneously causes multiple dependent events.

In addition, event independence does not preclude dependent probabilities, for example, where the probability of one event in the model is conditional on the actual occurrence of another. Such dependency expressions tend to be complex, however, and their use in practical analysis work is rather limited. Several such expressions are given in Example 1.2.2.3.

According to the randomness concept, individual events or conditions represented in the probability model occur at unpredictable times within prescribed intervals or at unpredictable points in any sequence of trials, if they occur at all. Were they to occur predictably, we would have to treat them as certainties instead of probabilities. The assumption may apply also to conditionally dependent events as well as to independent initiating ones.

Actual event randomness is not inconsistent with the random selection analogy sometimes used to describe characteristic variations of component failure or other probabilities with time. The analogy supposes an infinite population of like components, whose individual members initially differ only to the extent of expected construction variations. By placing all the components in service simultaneously and subjecting them to the range of operating variables corresponding to the intended specific application, failures accumulate with time. In choosing one component by blind, or random, selection at any time after the group startup, there is some chance of finding a failed unit, which probability is equivalent to the proportion of failed units at that time. The latter, of course, is the characteristic probability value sought. Several extensions of this analogy are useful in visualizing special situations, for example, testing and repair of components. Here, the "good as new" approach is usually expedient, corresponding to restoration of the infinite population to new condition at repeated intervals. Similar treatment is sometimes given to external events, such as storms, where probability of occurring within an interval is the factor of interest.

As mentioned in Section 3.1.1, a given set of basic considerations can be expressed equally well as a system success or failure model. While true in theory, results from practical models developed in such opposite ways almost never agree exactly. The differences arise mainly in the

details of structuring success and failure arrays, the tendency being to identify events or states for one model objective that do not have exact counterparts in the other.

3.1.3 Qualitative Analysis

So far this chapter has stressed the probabilistic modeling aspects of analysis. There are practical limits of complexity, however, beyond which probability models are either altogether unsatisfactory or must be preceded by the development of input information. Such limits are soon encountered whenever it is attempted to analyze a system in great detail or to evaluate the conceptual design of a system having many major components, components with multiple functions, etc.

The problem then reduces to one of methodically identifying and accounting for many detailed considerations. Addressed to this need are the so-called qualitative analysis techniques, several of which have proved very useful and are currently applied even more as independent evaluation methods than as a prelude to probability modeling. Their approaches generally consist of either listing components and considering malfunction consequences for each or postulating significant events and diagramming possible contributing conditions. Overall they extend our capability to envision the more obscure failure mechanisms.

3.1.4 Evolution of Analysis Practice

The reliability models of 25 years ago described systems in terms of relatively few main components and their direct functional relationships. Straightforward problems in probability or probability vs time were formulated around the models and kept simple enough to be solved by hand calculations. The problem limitations presented by capability to perform the calculations were so severe that many situations of interest just could not be represented adequately. The parallel development of digital computers, however, effectively removed such limitations, and now it is at least feasible to model almost any situation we are capable of describing. As in other areas, the impact of the computer was no less than to dictate entirely different methods of problem solving, that is, the "open" or successive trial approach as opposed to the setup and direct evaluation of great convoluted equations.

Sections 3.2 through 3.5 describe specific methods of analysis and trace the progression from the early simple models to the quite sophisticated ones now routinely executed. References 1 to 6 cover the basic material but at much greater length and with the alternative techniques more fully developed. For instance, the same conclusions regarding combined probabilities reached by direct or conditional probability sequences here (i.e., in Part 1 of the Appendix) can also be derived according to set theory or Boolean notations.

Before discussing the specific reliability techniques, it is well to consider briefly how each contributes to a practical reliability investigation. The general procedure is outlined below.

1. Define accurately each significant performance objective of the system.
2. Define the actual scope of the system intended to fulfill the objectives; the definition must be arbitrary, but this is no particular problem provided that all significant boundaries and interfaces are accounted for properly.
3. Define levels of performance below which system is considered to have failed.
4. Reduce system to an ordered set of elemental components, each subject to random failure of reliability significance; assign a probability factor or characteristic to each if possible. (Alternatively, problem may be reduced to random events.)
5. Identify and describe secondary random effects that can contribute to system failure; these are likely to originate outside the defined system boundaries and include independent catastrophic events such as fires.
6. Develop conclusions regarding the overall capability/reliability of the system to meet the defined performance objectives; probability modeling is commonly applied.
7. Identify opportunities for system improvement and optimize the system design; quantitative cost-effectiveness techniques may be applied in addition to qualitative studies.
8. Identify special measures required to achieve predicted reliability, for example, special component qualifications and quality assurance efforts.

Considerable judgment as well as a substantial knowledge of the system under study is implicit in each of the steps. It is up to the analyst in particular to select techniques appropriate to a problem, to apply each at an optimum level of detail, and to temper the conclusions according to recognized limitations in problem understanding.

3.2 Reliability Models

3.2.1 Reliability Analysis Model

The early practice of representing a system by an array of logic elements, each corresponding directly to a physical component, is now termed "reliability analysis" or "hardware" modeling. Its effectiveness was demonstrated originally for aircraft and missile systems which, while sometimes complex, had fairly straightforward reliability objectives. Thus, in typical problems oriented toward such systems, hardware models provided a satisfactory basis for direct calculations of probability vs time (i.e., after startup) that an initially all-good system would still be unfailed. Final solutions then were usually obtained in terms of probability of completing a mission of definite duration, or of time until system failure probability reached an unacceptable level. Example 2.2.4 illustrates hand calculations on a hardware model.

The basic method remains very popular and its capabilities have been greatly expanded. Current versions of the hardware model may represent systems in great detail since evaluation is no longer restricted to hand calculations, and other refinements have enabled more accurate representation of the component reliability characteristics, as will be discussed later.

3.2.2 Reliability Analysis Model: Addition of Events

The basic reliability analysis model can easily accommodate considerations other than simple success or failure of components. Examples 1.2.1.7 and 1.2.4.1 illustrate methods whereby events may be represented either as affecting component reliabilities or as independent logical factors in the system model.

3.2.3 Event Tree

When it becomes necessary to investigate in depth a reliability situation dependent on many diverse influences, it may prove impractical at first to structure the problem as a hardware model. The sheer complexity that would be required in such a model might well defeat the major aim of the study, namely, to provide insight of the system failure mechanisms. More flexible diagramming methods are then in order. Addressed to this need is the "event tree" form, which was developed originally by Bell Telephone Laboratories and has since been widely adopted.

The event tree describes a situation as a hierarchy of events logically leading or contributing to an ultimate event of interest. It may take either of two forms, "fault tree" or "success tree," depending on the approach the analyst wishes to emphasize. Tree construction ordinarily begins with the top event and works downward. Subevents are first described briefly as engineering considerations, which are then connected through appropriate logic symbols (see Fig. A.2.1, Appendix). Thus the tree is initially an aid to qualitative analysis.

Example 2.4 illustrates fault tree applications intended to provide direct qualitative insight of factors that could lead to system failure. In it are a number of detailed considerations whose probabilities would be virtually impossible to assess; thus in "raw" form this diagram is not directly amenable to probability analysis.

To develop a probabilistic model out of a tree diagram is fairly straightforward. First, it must be decided which considerations (i.e., events) shall retain their identity in the model and be assigned probability characteristics. The remaining considerations are either discarded, if trivial, or somehow combined into nontrivial expressions. Having thus reduced the model to a tree of probability expressions, it is ready for evaluation directly by computer programs designed to handle input so structured. In some cases, however, rearrangement is necessary in order to obtain logically equivalent structures that are compatible with the available computer programs.

The fault tree has generally gained precedence over the success tree because it is deductive rather than inductive. Deductive analysis is

claimed to be the more efficient since it concentrates on the smaller number of failure combinations instead of the larger number, success paths. Failure considerations may also have more dramatic value than success, stimulating more effective action in system improvement. Occasionally both fault and success trees are applied to the same problem in order to bracket the difference between the two approaches.

3.2.4 Decision Tree

The decision tree, another diagrammatic method for representing reliability problems, is somewhat more comprehensive than either the block or fault tree methods in that it can represent events as well as components and at the same time display all the steps for convenient numerical solutions by hand. Even the steps for conditional probability calculations are diagrammed (e.g., for cross-linked dependencies). However, the arrangement of elements is not always as "natural" as for other methods described, and the diagrams tend to become so complicated that they are difficult to review by inspection. Example 2.5 illustrates the decision tree for comparision with block and fault tree diagrams of the same system problems.

The true strength of the decision tree approach is realized in the situation where a logic or probabilistic model is partitioned and the subordinate portions have multiple outcomes, each of which must be considered in the overall problem. Such situations are typical of systems that have degraded operating modes, diverse redundant backup capabilities, etc., as is often the case for integrated protection systems in reactors.

3.3 Qualitative Assessment of System Reliability

The models just described all provide qualitative insights of the system failure causes, the event trees being particularly effective. Several other review techniques have also gained favor for their ability to ferret out more obscure deficiencies in system designs.

3.3.1 "Failure Mode and Effect" Analysis (FMEA)

Although under "Event Tree" it was suggested that deductive analysis methods were generally preferable, there are some good arguments to be made

for the inductive methods. In particular, they tend to focus attention first on the elemental components. The methodical examination of a system inductively, piece by piece, is now termed failure mode and effect analysis. Typical arrangements of the information developed by this technique are given in Example 2.3.

Failure mode and effect analysis not only provides some immediate insight to local problems but is frequently used to generate information for input to the larger system modeling problem. It is especially effective in identifying multiple effects on the system that can be produced by single components and may signal where further detailed study of a component would be appropriate.

3.3.2 "Common Mode Failure" (CMF) Analysis

According to probability theory, any desired degree of reliability can be imparted to a system merely by providing sufficient redundancy. A recognized practical limitation to this notion is that events may occur which simultaneously disable all of a set of redundant elements. The deliberate search for such common disabling causes is becoming established[49] as a separate discipline within the broad context of system analysis and is designated common mode failure analysis. Typical common mode failure causes include equipment functional deficiencies, design errors, maintenance and operating errors, and external events.

The results of CMF analysis are applied mainly as feedback on detailed designs, that is, as a means to debug or improve a design. They may also be helpful in developing criteria for component qualification, quality control, and system operation.

3.3.3 "Single Failure" Analysis

Without recourse to formal modeling, some analyses of reactor protection systems are done from the standpoint that virtually complete redundancy of all functions is required to assure adequate reliability of vital systems. Further required is a high, but not complete, degree of independence among redundant elements. Detailed investigations are then undertaken to discover and assess points of significant vulnerability either in the system design or as constructed. Such studies are now designated single failure analysis.[123]

In practice, all system common elements (i.e., not independent-redundant) are suspect, regardless of whether a formal model might disregard them as having too low a probability of random failure to be significant. Particular attention is given to elements exposed to damage either due to location or as a consequence of some system condition (e.g., a voltage surge causing a cascade of transistor failures in a voting logic matrix).

3.3.4 System Performance Analysis

Many so-called system failures, notably in instrument systems, are more properly described as performance degradations below threshold levels or as calibration drifts. This situation has been considered exhaustively in articles and texts on instrument application. An interesting aspect of the problem is that a performance deviation may be represented as a distributed variable, and the probability of deviating beyond a limit can therefore be estimated like a failure probability. Section 9 of Ref. 18 and Chapter 5 of Ref. 98 treat this topic explicitly with regard to system reliability under the category of "bound-crossing."

3.3.5 Network Simplification

In the design of complex logical arrays, one of the major challenges is to execute all the intended system functions with the minimum number of elements. The Boolean methods were developed originally as aids in simplifying the design of switching matrices but have since been extended to more general design applications and for use in system reliability calculations. The methods are of interest here since they represent one means for analyzing an early design in order to improve it by eliminating unnecessary redundance (i.e., that which detracts from reliability). An introduction to the use of Boolean methods is provided in Ref. 1, and a more comprehensive development is offered in Ref. 7.

3.4 Numerical Analysis

The purpose of numerical analysis in reliability studies is to calculate the probability either that no critical combination of undesired events will cause system failure or that some combination of desired events will produce system success.

3.4.1 Probability at a Fixed Point in Time

To introduce the calculation methods, it is convenient first to ignore the whole question of time dependence and concentrate on immediate probabilities. Accordingly, Example 1.2.1 develops, through logical reasoning processes, the failure and success probabilities of various system combinations of elements. The very important concept of conditional probability, popularly attributed to Bayes, is demonstrated in the expressions for the dependency situations, including cross-linked element, standby element, exclusive shared element, and element whose stress (and hence failure probability) changes because of some predictable influence. A few exaggerated numerical examples are provided to consolidate various steps.

3.4.2 Probability as a Function of Time

In theory, at least, the transition from the discrete probabilities of Example 1.2.1 to probabilities that are functions of time is simple. Noting that the discrete probability relationships are always valid, all that is required is to replace each elemental probability with a function that properly describes how that probability varies with time. It follows that whenever all the functions are evaluated for a system for the same instant in time, a set of discrete probabilities (or an overall system probability) is produced equivalent to those in Example 1.2.1. The time functions are developed in Example 1.2.2, first as general expressions, each of which can represent a function as simple as constant with time or as complex as practical. But the most commonly used is that of constant failure rate or exponential distribution of failures in time, [$P(t)$ that component is failed] $= 1 - e^{-\lambda t}$. Accordingly, Example 1.2.2 also develops each of the general relationships assuming an exponential distribution for each element. Other distributions are described in Chapter 4 and Example 1.4.

The exponential forms are typical of those used to make up the common hardware analysis model. Evidently they permit direct model evaluations of system reliability in terms of success or failure probability as a function of time, or for intervals, etc. The continuous, independent expressions are readily combined. The expressions for dependent elements represent discontinuities, for example, from standby service to operation; therefore they are derived from time-integral forms, with multiple integrals necessary to describe compound dependencies. Several such compound dependencies are worked out in Example 1.2.2.3.

3.4.3 Systems with Repairable Elements: General Method

So far the discussion has concerned systems that continuously (or "monotonically") become more degraded after startup. Many real systems, however, are subject to renewal on a periodic or a continual basis. The periodic renewal is usually treated simply as a repeated interval reliability problem. With continual renewal of failed components, it may be attempted to evaluate system reliability as a single problem by methods derived from the Markov chain approach.[5,45] This method essentially develops a set of simultaneous differential equations, each representing the combined probability of transition by all routes into or out of one possible system "state"; every possible state (i.e., combination of failed and unfailed elements) is acknowledged in the general problem. Solving the set of differential equations yields a set of probability vs time functions, again one for each possible system state. From among the latter functions are selected those which correspond to the system condition of interest, for example, all combinations by which the system has not failed. The selected functions are then evaluated for intervals of interest. It is further possible to apply this method successively, the results of one application providing the initial conditions for the next; such procedures might be used to evaluate system availability vs time and then, following demand, the probability that the system could function for a desired interval.

Example 1.2.3 illustrates the essential steps and resulting expressions typical of the Markov approach. Considered first is the "probability history" of one component (i.e., a "system" of one component) subject to

defined failure and repair completion rates. Evidently, the equations presented describe a total success probability vs time function that is compounded of an infinite series of contributing functions of the following type:

1. $+ P(t)$ that component has not failed the first time.
2. $+ P(t)$ that component has failed the first time $\times P(t)$ that component has been repaired after first failure $+ \cdots$.

⋮

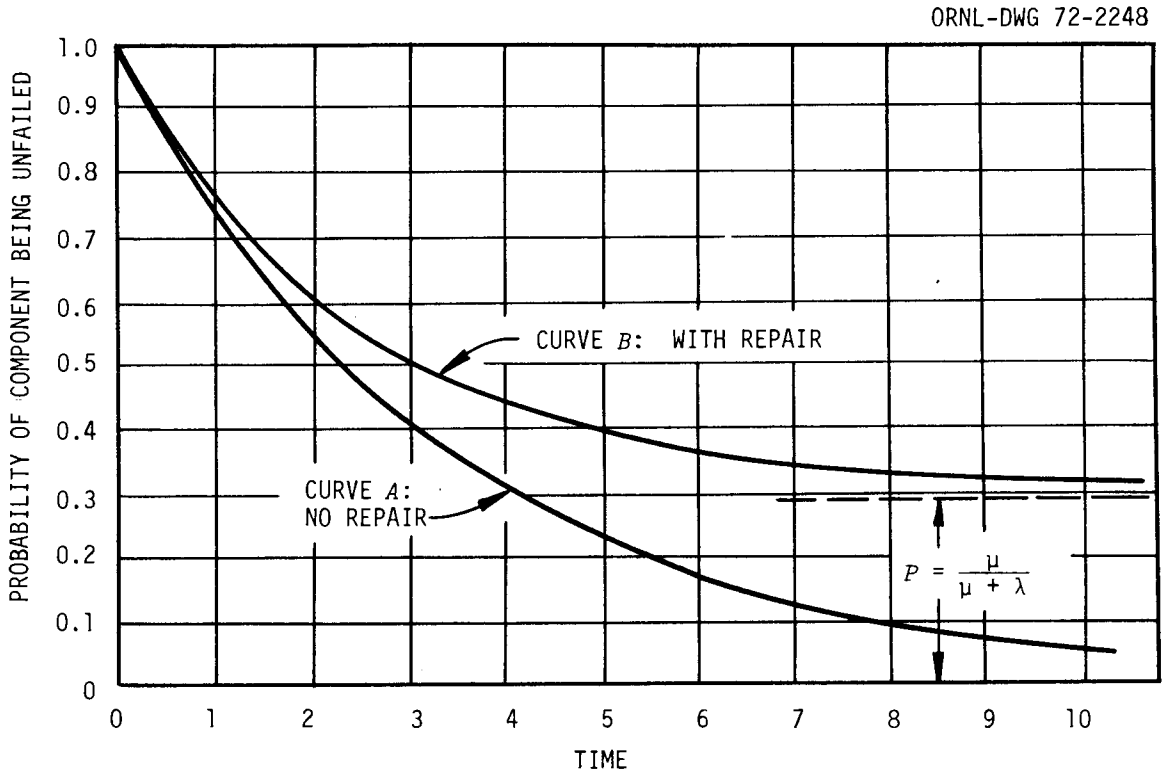
N. $+ P(t)$ that component has failed the Nth time $\times P(t)$ that component has been repaired after the Nth failure.

Early in the system history, the first term dominates, and later the others become more important. Figure 3.1 illustrates this for the single-component system with assumed failure and repair rates; the first term and curve A correspond to the ordinary failure without repair, while curve B represents the entire series of terms for failure with repair. In the example, a set of differential equations is then developed for a two-component system, and the solutions are given in terms of a reliability problem.

3.4.4 Systems with Repairable Elements: Steady-State Reliability

The rigorous and elegant Markov methods serve nicely to provide insight into the general reliability problem for systems subject to repair and/or other discontinuous conditions. However, they are too complex for hand calculations. At least the repair situation can be handled by simple, straightforward calculations based on the "infinite time" approach. To introduce this approach, we consider first the relamping situation.

Figure 3.2 illustrates how the failure rate for a lamp population will initially oscillate and then dampen out toward a steady-state value, assuming each lamp is replaced shortly after it fails. For any given pair of failure and repair time distribution functions, it is not difficult to estimate the average fraction of the lamp population that will be out of service over a long interval. Further assuming that the failures are randomly distributed among the lamps, the average fraction of time that any one lamp is out of service is then considered to be numerically equal to the average population fraction disabled, and the same number is used as



EXPONENTIAL FAILURE RATE = λ
EXPONENTIAL REPAIR RATE = μ

CURVE *A*: (NO REPAIR)

$$[P(t) : \text{COMPONENT NOT FAILED}] = e^{-\lambda t}$$

CURVE *B*: (WITH REPAIR)

$$[P(t) : \text{COMPONENT NOT FAILED}] = \frac{\lambda e^{-(\lambda + \mu)t} + \mu}{\lambda + \mu}$$

Fig. 3.1. Component failure probabilities with and without repair.

ORNL-DWG 72-2249

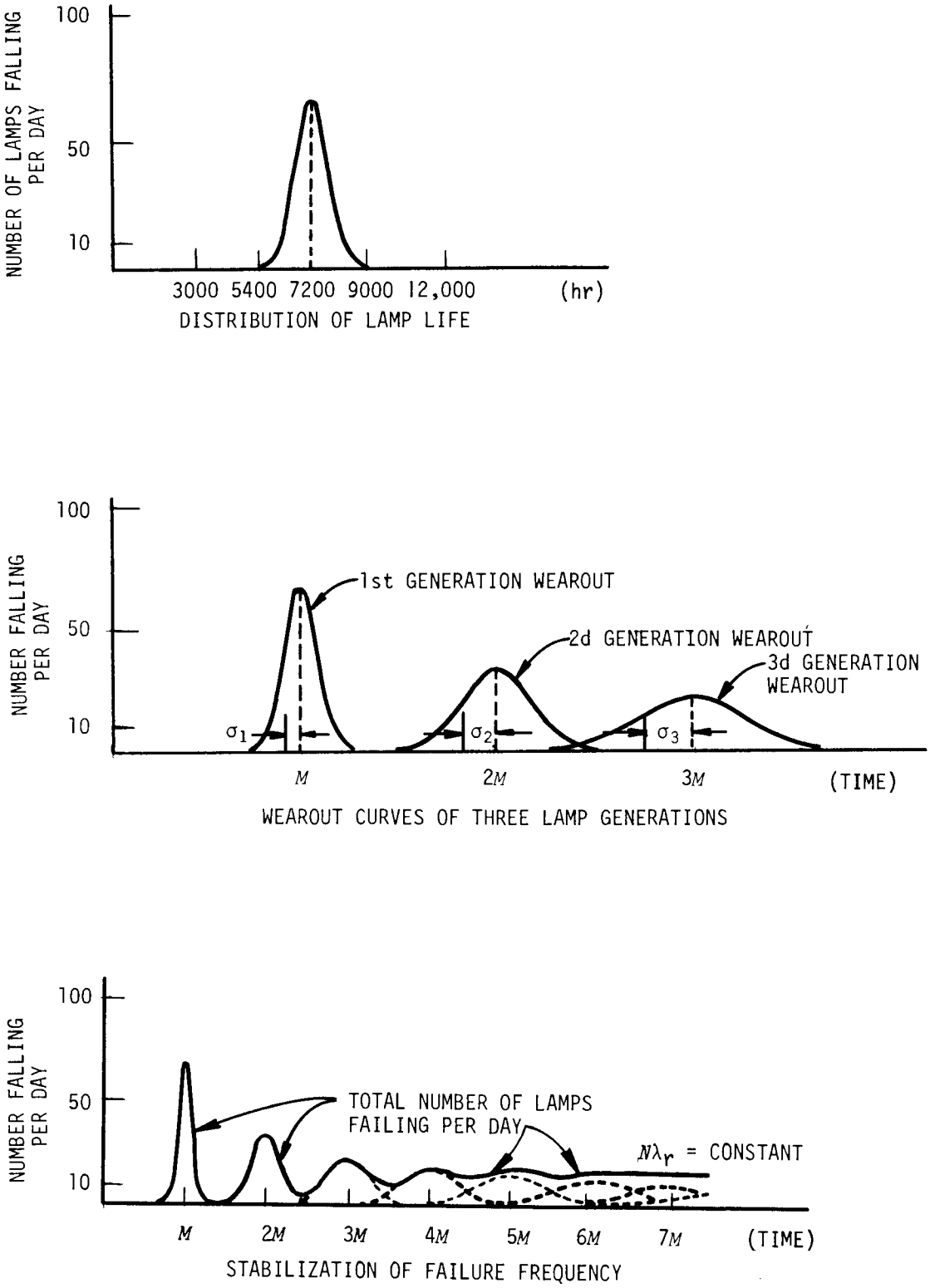


Fig. 3.2. Stabilization of failure frequency.

the probability that any given lamp will be found failed at any time we choose to look. Extending this concept to systems, the reliability problem reduces to evaluating probabilities of coincident situations such as combinations of component failures leading to system failure. This is precisely the simple method of Example 1.2.1, but now utilizing the steady-state instead of instantaneous probability values for the components.

3.4.5 Reliability Measures: Calculation Objectives

Table 3.1 lists the basic reliability figures of merit and defines them in terms of calculation objectives. In practice, simple problem formulations can often be substituted for rigorous ones, reducing calculation effort without significant sacrifice of accuracy. The analyst must, however, avoid those simplifications which do introduce serious errors.

Reactor protection systems are essentially standby systems. Their probabilities of functioning when needed are, therefore, best described by "availability" or "mission reliability" formulas, depending on the specific application. Availability then implies simply that for the equipment or system to have survived to the moment of demand is enough; if it is not broken at that moment, it will function on demand. This concept often represents sensors and instruments adequately, but standby machinery perhaps not so well. To characterize standby elements which begin their essential function on demand, mission reliability factors together availability (i.e., up to the moment of demand) and probability that the equipment will survive a subsequent operating cycle or interval of interest. Actual operation may be under very severe conditions, which must then be properly accounted for.

Most elements of protection systems are tested periodically, and it is deliberately sought to replace or renew their equipment before it is subject to wear-out mode failures. Hence, the component or system renewal assumptions described in the preceding sections apply. The long-term average system reliabilities then are considered to be the same as those for a "major" test interval, that is, an interval between overall system tests or in which all components have been tested at least once. In practice, this generally works out equivalent to the reactor fuel cycle, since elements not tested on line are tested during refueling shutdowns.

Table 3.1. Reliability Measures for Devices and Systems*

1. Probability		
1.1 $[P$: (descriptor)$]$	$\equiv$	Immediate probability of condition described, e.g., the simple probability that a particular event will occur sometime in a given time interval
1.2 $[P(t)$: (descriptor)$]$	$\equiv$	Probability of condition described, as a function of time
Also		
$[P(c)$: descriptor$]$	$\equiv$	P as a function of trials or cycles
1.3 $S(t)$	$\equiv$	Probability that device or system is not failed, as a function of time
Also		
$S(c)$	$\equiv$	P as a function of device or system cycles
2. Reliability		
2.1 Reliability function		
$R(t)$	$\equiv$	$S(t)$
	$\equiv$	$\exp\left[-\int_0^t \lambda \, d\tau\right]$ in most general case (see ref. 2, p. 26); λ is the variable, $-1/R \; dR/d\tau$, i.e., the rate of population change (pos. as well as neg.) with respect to the surviving fraction. Note that $dR/d\tau$ = probability density function (pdf), per Sect. 4.2.1. If λ is constant, pdf is for exponential failure distribution and $R(t) = e^{-\lambda t}$

*Although most of the terms appearing in this table can be found in other published work, they are not standardized nor necessarily common. Moreover, the meanings attributed to them in the literature are not entirely consistent, particularly where simple problem forms are substituted for more rigorous ones (see Sect. 3.4.5).

Table 3.1 (continued)

Also

$R(c) \equiv S(c)$

2.2 Average reliability

R ≡ Average probability that a system or device is not failed at any time during a specified interval T after being placed in service or otherwise renewed

$$\equiv 1/T \int_0^T R(t)\, dt$$

$R \approx R(T/2)$ for reliable apparatus, e.g., where T is the test interval

$R \approx R(T)$ as a more conservative estimate of the above

2.3 Inverval reliability (also "mission reliability," 4.1 below)

$R_i\ (t_1, t_2)$ or $IR\ (t_1, t_2)$ or R_M

≡ " . . . the joint probability that the system will be up at the time t_1 and will also remain up until the time t_2, which is greater than t_1, given that the system was fully up at $t = 0$." (Ref. 45, p. 17)

$$= \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} R(t)\, dt$$

Note that $R(t_1)$ must be determined separately, and may represent more than one factor, e.g.: $R(t_1) = [A(t_1)]^{\dagger}$ [P : Starting device operates]

Alternatively, $R(t_1)$ may be a long-term average value, e.g.: $R(t_1) = A^{\dagger}$ or $SA^{\dagger}$

---

†See expressions for "availability," items 3.1, 3.2, etc.

Table 3.1 (continued)

2.4 Reliability with repair (see Example 1.2.3 in Appendix for typical expressions)

RR, $RR(t)$ $\equiv$ R, $R(t)$ for repairable devices or systems in which some or all elements are subject to repair; in actual problems, each repair vs time characteristic is specified

[2.5 "Steady-state" reliability, R_s or SR, for repairable devices or systems: Not usually of interest for standby systems; in theory, however, it is analogous to steady-state availability, per 3.5 below.]

3. Availability: The expressions for availability are the same as for reliability but imply that the systems or devices are in standby. In many cases, the fact that no failure has occurred during the standby interval is considered equivalent to successful operation when called upon, e.g., a normally energized relay coil. In other cases, standby represents a mild stress in contrast to a greater stress in operation or on demand, e.g., a sensor to detect a severe transient. Standby may also involve idle degradation, e.g., gumming of lubricants, corrosion, etc.

3.1 Availability function

$A(t)$ $\equiv$ $S(t)$ for standby conditions

3.2 Average availability

$$A \equiv 1/T \int_0^T A(t)\, dt$$

$A \approx A(T/2)$ (see 2.2)

$A \approx A(T)$ (see 2.2)

3.3 Interval availability (also "mission availability," 4.2)

$$A_i \text{ or } MA = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} A(t)\, dt$$

3.4 Availability with repair [same as $A(t)$, A, but for repairable elements]

Table 3.1 (continued)

3.5 "Steady-state" availability for repairable devices or systems

SA ≡ Asymptotic value of $A(t)$, i.e., $A(t \to \infty)$

SA = A for devices or systems renewed at regular intervals

4. Mission parameters

4.1 Mission reliability: same as interval reliability (see 2.3)

4.2 Mission availability: same as interval availability (see 3.3)

5. Time to failure

5.1 Mean time to failure (MTTF) or mean time to first failure (MTFF) of a simple device or system <u>without repair</u>

$$\text{MTTF} = \text{MTFF} = \int_0^\infty R(t)\,dt^{\ddagger} \text{ or, for standby service,}$$

$$\int_0^\infty A(t)\,dt$$

5.2 MTTF or MTFF for systems with repairable elements: Find by unbiased Monte-Carlo simulation or by matrix solutions as indicated in Example 1.2.3.2 (i.e., with special constraints)

5.3 Mean time between failure (MTBF) for simple devices or systems which are "renewed" after each disabling failure

MTBF = MTTF = MTFF

5.4 General MTBF for systems with repairable elements:

a) Find by unbiased Monte Carlo simulation with long runs, using appropriate repair time distributions for each repairable element

b) If steady-state reliability R (or availability) is known and average outage time per failure can be estimated for all failures:

$$\text{MTBF} \approx \frac{T_R\,R_s}{1 - R_s}$$, where T_R is average outage time per system failure

‡Reference 2, p. 80.

The table expresses reliabilities both as instantaneous functions of time and as integrated averages over time intervals. Although it is generally the long-term average values that are really of interest, the simpler instantaneous expressions are more often used. Conservative approximations of interval average reliability items can be obtained by evaluating the reliability function at the end of the test cycle interval.

The distinction is drawn between availability of standby equipment and reliability of operating equipment. Nevertheless, the term reliability is sometimes applied to quiescent systems or components, causing confusion. The usage here is mainly to simplify, and, if the data then applied are for equipment in operation the reliability evaluation should be more conservative than actual availability.

The basic availability or reliability calculations are applied in a wide variety of practical problems, many of which are directed toward specific decisions. For example, design cost-effectiveness optimization may involve repeated reliability evaluations along with cost estimates for alternative designs or design modifications. Decisions concerned with testing have occasioned the special problem considerations described in the next section. And another area just beginning to be explored objectively is that of operating decisions, for example, determining policy in regard to outages of particular portions of the protection system.

3.4.6 Evaluating Effects of Component Testing

One particular class of analysis problems, mentioned above, assesses the effects of testing on system reliability. This may be done in order to provide some basis for deciding where on-line test facilities should be provided or to optimize test frequencies. References 50 and 51 treat the subject in detail.

Underlying most such calculations is the assumption that the "successful" test (or repair) of standby equipment simply removes all the accumulated probability of failure; that is, a device or system becomes "good as new." Equipment in continuous operation or very effectively monitored is regarded as being under continuous test and hence may be represented by failure-with-repair techniques (Sects. 3.4.3 and 3.4.4).

The immediate problem aim for reactor systems is usually to determine average availability in standby over the interval of a fuel cycle. Minimum availability during the cycle is occasionally of separate interest, since with testing, it does not necessarily occur at the end of the cycle. Rigorous calculations of average system availability, where components or subsystems are tested at different intervals, may become too difficult for hand methods. This is suggested in Part *a* of Example 1.2.4.5, which shows how the average must be obtained by integrations of the $A_s(t)$ function in successive time increments up through the system interval of interest. A valid method of simplifying the calculations is then to evaluate the problem in steady state according to Section 3.4.4. Two further approximations are satisfactory for highly reliable components: (1) use component availability value at the midpoint of its test interval in place of actual steady-state average value, and (2) where the availability vs time characteristic is exponential, substitute $1 - \lambda t/2 \approx e^{-\lambda t/2}$ for the midinterval value.

In some problems for optimizing test frequency, the time that a system or part of a system is out of service for testing is significant to the system reliability. Reference 51 develops this consideration by differentiating an expression for average availability of one component in a variable test interval (T) with a fixed test time (t), setting the derivative equal to 0, and solving. The result for a component with exponential failure distribution is $T_{opt} \approx \sqrt{2t/\lambda}$. In other problems, the test itself could be considered to wear the item tested, thus affecting its failure probability in subsequent service.

3.4.7 Level of Analysis Detail

Current methods permit evaluation of reliability models representing hundreds of components and events. The capability is applied not only in studying very large systems but also in examining smaller ones in more detail. Deciding the appropriate level of detail at which to conduct each phase of a study is an important responsibility of the analyst, for the choice can strongly affect the derived conclusions as well as the prospects for developing useful quality assurance information.

In regard to qualitative analysis, usually the more considerations examined, the more opportunities arise to discover and correct potential causes of system failure. The main practical limitation, then, is the effort one can afford to devote to a study, although at some point trivia will begin to distract attention from the main study objectives. It is generally worthwhile, however, to carry qualitative analysis somewhat beyond where meaningful probability data are available or even reasonably obtainable. There is no particular need for qualitative studies to be consistent in level of detail throughout.

For numerical analysis there is some incentive to view systems in terms of major components rather than minor. Not only is the question of evaluation effort involved, but also the tendency of increasing detail to diffuse the study results. The latter is a consequence of expressing elemental reliability characteristics as ranges instead of individual values; thus the spread between average and boundary worst case problem solutions widens rapidly as a given situation is modeled in greater detail. Practical limits to simplification, on the other hand, usually are determined by the individual problems, often with regard to either distinguishing among significant failure modes or sensitivity to system design alternatives being investigated.

Consistency of detail, as well as level, is important in studies intended to compare systems or features. There, different treatment of the alternatives in conjunction with use of conservative reliability values for the components could bias the problem solutions unevenly, perhaps to the extent of forcing wrong conclusions. Or, using ranges of reliability values, the diffuseness of the results might then merely obscure the intended comparisons.

3.4.8 Simplification of Analysis: Depth Control and Cut Sets

Example 1.2.1.3 illustrates how the "total probability" of any system (equal to "certainty") is conceived as the sum of the probabilities of all possible system states. There are 2^N states for an N-component system in which each component can only be "failed" or "good"; a substantial proportion of these states correspond to system failure, and the remainder

are system success. However, further consideration reveals two opportunities for reducing the number of terms to be evaluated in order to determine the system failure or success probability. First many of the system states are extremely unlikely in that they require concurrence of several improbable events. Thus, state $F_1F_2F_3$ in Example 1.2.1.3 might have the probability of 10^{-9} if $F_1 = F_2 = F_3 = 10^{-3}$. A simple way to reduce the burden of calculating such trivial state probabilities is by "depth control," whereby the number of concurrent failures allowed in the system is limited arbitrarily. The basic method is shown in Example 1.2.4.2, and its application in a computer program is described in Example 1.3.1.2*b*.

The other simplifying procedure is indicated in Example 1.2.4.3. From the diagram for the example, it is apparent that only three "minimum" combinations of component failure are responsible for all system failures; any other combinations must include at least one of these and hence are not minimum. Identifying only the nontrivial minimum cut sets is done most effectively by biased simulation, as suggested in Example 1.3.3. It appears that for a given degree of analytical solution accuracy, the minimum cut set evaluation should be more efficient that depth-controlled evaluation because the latter may still require probability calculation of many trivial terms. Both methods are approximations, and the magnitude and direction of the errors thus introduced depend on individual problem factors such as depth limit, values of contributing component reliabilities, system configuration, and, for simulation to identify sets, the biasing procedure and number of iterations. The "success" corollary of the cut set is the tie set.

3.4.9 Effects of Problem Variations: Sensitivity Analysis

It is frequently desirable to investigate the effect of varying the reliability characteristic of one component or subsystem on the overall reliability forecast for the system. When this is done methodically, by successive trial solutions over a range of values for the variable portion, the procedure is called sensitivity analysis. The results may determine a threshold reliability value for the component of interest, below which system reliability becomes unsatisfactory and possibly begins to drop off

rapidly. If the threshold value should turn out to be higher than the most pessimistic interpretation of the component data, one might justify additional redundancy in the system. Alternatively, the threshold value could be made the basis for a quality assurance requirement.

Direct expressions for partial effects can also be developed out of conditional probability, and these are sometimes differentiated to obtain rates. Example 1.2.4.4 illustrates such expressions.

3.4.10 Some Practical Aspects of Modeling

Example group 2 of the Appendix illustrates and compares some of the modeling approaches that have been described as they might apply to an emergency core cooling system. The contrived system is considered first in overall conceptual design state, and then one portion is developed and analyzed in detail. Example 2.1 describes the basic system and its performance objectives.

Example 2.2 traces the procedure to set up and evaluate a simple reliability analysis model of the system conceptual design. Only the "gross" components, those directly involved in the system function, appear in the initial logic diagram, Example 2.2.2; many of these actually represent small subsystems, such as the "pumps" which include drive motors, switchgear, etc. Some components also depend on support systems such as power supplies; these systems are therefore considered as within the problem domain, and their reliability factors must be properly acknowledged. In Example 2.2.3.2 and 2.2.4, it was elected to express all the energy supply reliability factors together as a separate system element, but to consider lube oil systems, etc., as integral "parts" of components served.

The conceptual design analysis suffers somewhat from being able to express only vaguely many of the functional relationships among the components that would exist in a real system but are as yet undefined. How serious a deficiency this can be is seen from a comparison of the initial treatment of the complex pump and valve controls with the subsequent model development for the detailed designs. Thus, to represent the controls at all in the conceptual model requires a good general understanding of approximately what to expect from such equipment.

The remaining major difficulty in setting up the example model is obtaining the component reliability information and adapting it to the problem objectives. Chapter 4 is devoted to the fundamental component data. Typical expressions for the problem input data are given in Example 2.2.3; evidently those which are time dependent describe failure rates under continuous service conditions, while most of the problem concerns standby service. In addition, some of the rates are based on operating cycles rather than time. The example problem takes recourse to simple ways of applying the data, whereby all equipment is assumed to be "good as new" at the beginning of each reactor operating period and fully stressed throughout each entire period. To convert the cyclic reliabilities, reasonable numbers of cycles were assumed for each demand upon a component so rated. The example expedients just mentioned tend to make the numerical analysis results conservative, which may or may not be desirable. Should the results be intended merely to demonstrate adequacy of the conceptual design, there might be little incentive to attempt a more rigorous analysis; on the other hand, if alternative and much different conceptual designs were being compared, the conservative treatment could bias the numerical results sufficiently to force wrong conclusions.

Example 2.3.1 shows how failure mode and effect analysis (FMEA) may be applied at the conceptual design stage to develop guidance information for subsequent design phases. The subject of Example 2.3.1, a portion of the controls, is then expanded as a detailed but unrefined design in Example 2.3.2.2. An FMEA is performed on the detailed design in Example 2.3.2.3 to demonstrate design review capabilities.

Example 2.4 shows how the same system might be modeled by fault trees, first in terms of gross events affecting the major functions and then proceeding down through the fine structure of the controls. Finally, a portion of the controls is recast as a multiple-outcome decision tree in Example 2.5.

The purpose in selecting just one area for expansion was merely to emphasize some points tutorially. But it also suggests how an actual case study may become similarly unbalanced. In the real case, however, the situation likely would arise from attempts to simplify an analysis or to

concentrate on portions of the system where difficulties are anticipated. Particular efforts would then be necessary to avoid the problems of inadvertent biasing discussed in Section 3.4.7.

3.5 Computerized Analysis of System Reliability

The basic rules for combining elemental probabilities have been developed in the preceding sections and Example group 1.2. Attempts to apply these general rules to systems with many components can lead to mathematical expressions that are intractable to hand calculations. It is not so much the sheer number of components that causes difficulty, but rather the existence of one or more of the following system characteristics:

1. complex functional dependencies such as events that affect several functions, components that serve multiple functions, cross-linked or M-of-N subgroups, etc.;
2. component failure probability distributions which, while independent, are not simple functions of time;
3. component failure probabilities that are dependent on other components or system factors;
4. changes in system role, operating conditions, or composition during an interval of interest.

Thus the reliability of the simplest N-component systems might be calculated with no more than a few arithmetic steps, the worst of which is adding together perhaps $N/2$ simple factors. More complex systems generally require separate evaluation of many combinations of failed and unfailed components, with some of the combinations themselves represented by complex expressions.

Some very ingenious methods have been developed to apply computers in solving reliability problems for large systems. At one time, these methods were clearly classifiable as "analytical" or "simulation," but now various of their features have been combined and the distinction is blurred. The analytical techniques essentially set up and solve problems in combined probability along the lines followed by hand methods. Simulation involves subjecting a system logic model to random component failures and observing the occurrence of system failures over repeated

runs. In theory, any of the basic methods to be described could be developed to handle problems of any complexity and to any degree of accuracy desired. The practical programs have accomplished this to a remarkable extent, but with some compromises to improve efficiency.

Each expedient used in a program to improve efficiency imposes limits on the user with regard to the kinds of reliability problems that can be handled effectively. This must be clearly understood by anyone considering the application of computers. Most of the "shortcuts" seek to emphasize significant probability combinations and to discard trivial ones, usually resulting only in minor sacrifice of accuracy. Others disregard repair capability or can accept only the simplest of component failure and repair distributions; such programs might be entirely acceptable for some problems, unacceptable for others, or else require extensive adaptation of system models to obtain satisfactory analyses.

The following descriptions cover some of the earlier computing methods that represent analysis and simulation in their "purer" forms. They are intended to convey the basic organization of all computation schemes. The current development trends are then summarized by simplified explanations of a few of the more modern programs.

3.5.1 "Automatic Reliability Mathematical Model" (ARMM)[20,46,113,41]

The original ARMM program was developed circa 1963 by the North American Aviation Company to model test flights of the B-70 aircraft. An improved version, coded for the IBM 7090-94 digital computer, was introduced in 1965, and the program has been undergoing continual refinement ever since. It is analytical and designed mainly to evaluate complex aircraft systems in multiphase missions. Systems of 500 components can be analyzed.

The basic approach of ARMM is to identify all significant combinations of component failures in a system logic model and then to evaluate the probability of each failure combination at some selected "age" of the system. The total of the (exclusive) failure combination probabilities is the probability of system failure at one point in time.

A problem may be partitioned into as many as 20 consecutive intervals (1965 version), each corresponding to a time period of any duration desired by the user and each essentially treated as a separate problem.

From one interval to the next, the main problem may be altered with respect to system configuration or system functional objective. However, there is no carry-over of the accumulated probability of any component or subsystem failure; that is, each component starts "new" at the beginning of every interval. In most problems the system failure probabilities found in each interval are simply restated as success probabilities ($P_s = 1 - P_f$) and multiplied together to obtain the overall mission success probabilities.

All combinations of more than a preselected number of component failures are arbitrarily ignored. That is, they are presumed to be statistically insignificant relative to the combinations of lesser numbers of component failures that are accounted for. The user selects the "depth," or number of component failures to be considered, up to a maximum of eight.

Example 1.3.1 illustrates the major steps of the computer in solving a problem in availability or interval reliability. The first procedure methodically tests the logic model in a minimum number of steps to identify the state combinations that can contribute to a system failure, given that no more than the preselected total number of components fail. The scheme amounts to a "truth table" method of developing a conditional probability statement. Failure probabilities are computed individually for each significant component over each interval in which it is significant by numerical integration of the failure probability density vs time functions; exponential and Weibull distributions can be handled. Finally, for each interval, the combinations of component failure or no-failure probability are multiplied out and the results summed.

The ARMM does not treat problems involving component failure-with-repair rigorously. However, good approximations can be obtained for many such cases by proper manipulation of the model parameters.

A standby-redundant pair of components can be represented as a single component. The composite failure probability is then expressed in the program as the failure probability of the "most dependent" element as in Example 1.2.2.3.

The program also ranks and evaluates the various factors contributing to system failure probability, including both individual components and functional groups of components.

3.5.2 Analog Computation

Brief mention is made of analog computation methods for completeness rather than to suggest that it is current state of the art. The simplest applications employ the computer only as a logic matrix to test combinations of failed and unfailed elements. More elegant are the setups to solve simultaneous sets of differential equations of the kind shown in Example 1.2.3.2. Although such differential equations can be modeled directly on the computer, the very large models necessary for typical problems do not usually yield accurate results.

Analog computation was used also as an adjunct to digital methods, that is, a "hybrid" application, in an early version of the "Monte Carlo" method to be discussed next.

3.5.3 "Monte Carlo" Method

The term "Monte Carlo" represents generically the many computer programs which simulate all manner of chance factors in physical problems. By its very nature, system probabilistic modeling invites the application of such methods.

The first significant use of Monte Carlo techniques for reliability simulation was to evaluate fault trees for the Minuteman missile system. This was reported by the Boeing Company around 1965 (Refs. 42, 43, 44) and involved a "hybrid" program arrangement of digital and analog computers. The digital computer simulated the random effects and directed the overall program, and the analog determined time-dependent component reliabilities as instructed. The Boeing concept of using a hybrid arrangement was modified by Holmes & Narver, Inc.,[20] for all digital execution by using a subroutine LOGIC in place of the hybrid analog of the fault tree "and" and "or" gates. The subroutine LOGIC thus represented the system being studied. This led to the development of the SAFTE (systems analysis by fault tree evaluation) series of programs which incorporated models with and without repair and using direct and biased Monte Carlo. The early programs, SAFTE-1 to SAFTE-5, simulated the system behavior by stepwise progression through all time intervals. This approach was later abandoned in favor of programs performing calculations for a specific time interval.[114] These later SAFTE programs are described in Section 3.5.5.

3.5.3.1 Simulation method. The basis for the current simulation procedures is that a population of N new components will fail in order 1 through N and that the number of components failed at any time after start-up is in accordance with the failures vs time characteristic for that class of components. Chance is introduced in deciding which of the original N components is the particular one in the system being evaluated; the selection is made in a manner equivalent to spinning a roulette wheel with N detents. A number K is thus determined randomly and related to age at failure, t, as follows for the exponential failure distribution:

$$\frac{0 < K < N}{N} = 1 - e^{-\lambda t} ,$$

or

$$t = \frac{1}{\lambda} \ln \left[\frac{1}{1 - (K/N)} \right].$$

In practice, all calculations are normalized so that $N = 1$ and the computer random number generator selects a K so that $0 < K < 1$. The method is perfectly general and may be applied to any failure, event, or repair distribution.

The remainder of a Monte Carlo program concerns evaluating the system effects of each event and the bookkeeping. Typically, the program is executed repeatedly, each iteration representing a time interval that corresponds to the operating cycle of the system modeled. The iterations continue until statistically significant results are obtained. A single extended run representing almost infinite time for the system could in theory obtain similar (not identical!) data, provided all components are repairable and all events "reversible," but this amounts to a steady-state problem and can be solved by easier methods.

Example 1.3.2 illustrates the scheme of a Monte Carlo reliability simulation, complete with typical observations and data analyses. For each run the first procedure is to determine the status of each component or possible event throughout an interval of interest. A given component may have failed and been repaired several times or may not have failed even

the first time. Next, a system timetable of events is constructed and placed into a system condition vs time master list. Each overall system condition is tested on the logic model, which determines system "failed" or "unfailed" for the interval from when a condition was first reached to when the next condition is effected. Finally, the statistics of problem interest are generated from the times and the corresponding system conditions.

The literature[20] indicates that SAFTE-1 evaluated the following reliability parameters: (1) interval reliability (or availability), (2) system failure probability rate of increase (i.e., probability density) vs time for a prescribed interval, (3) probability of system failure vs time within a prescribed interval, and (4) for each component, the probability of its failure being the ultimate event that caused system failure.

For systems comprised of very reliable components, an enormous number of iterations may be needed to reach statistically valid conclusions. Some idea of just how many interations are required can be obtained from a few simple considerations. Recall first that we are mainly interested in an overall probability of system failure and that failure can occur in many different ways. To place some boundaries on the problem, we say in effect that we want to evaluate and sum up all the individual probabilities (combinations) of system failure that are, individually, greater than some limiting value P_L. In order to "know" any one of these individual probabilities statistically within 10% (i.e., $\sigma = 0.1$), we have to observe it about 100 times in the simulation exercise.[48] The number of iterations to observe a condition of the limiting probability P_L would then be $100/P_L$. Thus, for example, if we are concerned with event combinations of $P_L \geq 0.001$, it would be necessary to iterate 10,000 times. For reactor protection systems intended to have overall interval failure probabilities of perhaps 10^{-5}, the individual contributing combinations would have much smaller failure probabilities, implying a need for 10^8 or more iterations!

3.5.3.2 <u>"Importance sampling."</u> Better simulation efficiency can be obtained by importance sampling, a method for biasing the input data (e.g., failure rates) and compensating the output results. Example 1.3.2.3 suggests both the proper and improper applications, the latter leading to extensive compensating calculations that void the method's usefulness. In

essence, the technique is suitable for interval reliability problems but unsuitable for determining mean time to first failure (MTFF) or similar quantities.

3.5.4 "The Generalized Effectiveness Methodology Program" (GEM)

The U.S. Naval Applied Science Laboratory in 1968 described[45] an analytical program to evaluate reliability of complex naval systems that are subject to variables not explicitly represented in other programs. In particular, these variables include such factors as availability of spare parts and repairmen, repair priorities, shared facilities, etc., which are evidently significant in optimizing certain systems. The program is implemented for the CDC 6600 digital computer.

Of interest in this study is the capability of GEM both for straightforward reliability calculations of the type shown in Example 2.2.4 and for Markovian problems in the manner discussed earlier under "numerical analysis" and illustrated in Example 1.2.3.2. From the description provided in Ref. 45, it appears that large problems involving many components or multiple phase missions, or both, are partitioned into subordinate problems that are each within the program capability. There is a basic limit of 6000 system states that can be kept in memory during a Markovian problem execution. The 6000 states could represent as few as 12 or 13 components (i.e., 12 components can provide $2^{12} \approx 4000$ combinations of failed and unfailed); however, by eliminating trivial states and combining series strings manually, it should be possible to allow many more components. It appears also that GEM can accept the output from one set of calculations as initial conditions for a succeeding set.

The "effectiveness" parameters evaluated by GEM are (1) reliability without repair; (2) availability — instantaneous, steady-state, and mission; (3) reliability with repair; (4) interval reliability; and (5) mean time to first failure. It is proposed to add the additional parameters of restore time distribution and interval reliability without repair (actually, with no repairs allowed in portions of a multiphase mission). Standby redundancy can be handled, provided the components involved are identical and have exponential failure distribution. Where only active redundancy is considered, any component may have exponential, log-normal, truncated normal, Weibull, or gamma failure distributions.

3.5.5 Later Programs Developed by Holmes and Narver, Inc.

In conjunction with their program to evaluate the reliability of reactor protective systems, Holmes & Narver, Inc. (H&N) have developed several simplified analysis programs for the digital computer. They are generally less rigorous than those just described but are faster and more economical of computer resources. When applied to problems for which they are suitable, the simplifying assumptions and problem truncations should not distort the results appreciably. Reference 46 describes the following programs out of the SAFTE series in greater detail:

A. QUIRC — An analytical program that solves system networks of only series and parallel component combinations for failure probability at a specific time. Component failure or event probabilities are calculated individually for the time of interest from their exponential or Weibull distribution parameters.

B. NOREP — A Monte Carlo simulation program corresponding to Example 1.3.2, but with no repairs allowed. It is primarily intended to develop system mean time to first failure and probability of failure vs time statistics for a given system operating interval. For the reasons suggested by Example 1.3.2.3, no importance sampling is used; consequently, many runs are required for systems of low failure probability.

C. MINCUT — Uses a biased Monte Carlo simulation to identify the minimum cut sets of a problem (see Example 1.3.3) and then determines system interval reliability analytically by calculating and combining the contributions of all sets initially identified. There is no need to unbias the simulation results since the bias is used only in the set identification phase and does not enter the actual reliability calculation. No repair is considered explicitly in the program. The program should be able to give accurate evaluations, provided the simulation is carried out over enough iterations to identify all the more probable combinations.

D. CONREP — Similar to MINCUT, except that any component is repairable in a constant time that is a preassigned characteristic of that component. The program has undergone a series of modifications and is presently the workhorse program used by H&N.

E. GINNY — Similar to CONREP, but introduces repair by assuming component steady-state reliability parameters.

3.5.6 "Kinetic Tree Theory"

Idaho Nuclear Corporation in 1969 introduced[47] a combined simulation and analysis method somewhat resembling the H&N program CONREP but capable of generating problem solutions conveniently for a series of points in time. Their program is implemented for the IBM 360-75 computer.

By the kinetic tree method, minimum cut sets or minimum tie sets of a fault tree are identified by a biased Monte Carlo simulation program called FATE. Expressions representing the probability of each identified set as a function of time are developed, including factors like those in Examples 1.2.2 and 1.2.3.1 for the contributing components. Summing the cut or tie set probabilities yields expressions, respectively, for system failure or success probability vs time that can then be solved for any time of interest. Either of two programs executes the analytical work, KITT-1 for no repair or KITT-2 with repair. Only exponential failure distributions and constant repair times are considered.

3.6 Advanced Analysis Methods

Beyond the straightforward probability analyses discussed thus far are a number of methods for evaluating more obscure effects on system reliability. Most of these have developed with the aerospace technology and are so oriented. The NASA comprehensive series Practical Reliability (Refs. 15–19) discusses many of the advanced techniques along with a more extensive development of the basic material in this report. The topics include "Parameter Variations Analysis," "Bound Crossing," "Sensitivity and Tolerance Analysis," "Reliability Cost Tradeoff Analysis," etc., which generally represent extension of basic analysis methods.

Some of the current analysis work on reactor systems tends toward the decision tree form of logical structuring, as discussed in Section 3.3.2. In conjunction with these applications, it should be noted that either analytic or simulation means can be used to identify the statistically significant combinations and that depth control and importance sampling are also helpful in simplifying the problems.

3.7 Reliability of Operating Systems

The reliability of systems in service is monitored to verify that the requirements on an individual system are being met, to identify system failure modes originally unsuspected or component weaknesses not anticipated, and to establish the reliability of a class of systems or components under particular operating conditions, perhaps to form comparison bases.

Practical observations of protection systems involve mainly test and maintenance. Most of the findings are of a routine nature, requiring at the most improvement of components. Excessive failure rates of components or unusual failure circumstances occasion special attention in regard to potential effects on system reliability. Since the emphasis in such an investigation is on removing the weakness, the consequent corrective actions tend to invalidate unfavorable component or system reliability data for use in predictions of future reliability.

Disabling failures are rare in protection systems since the systems are made up of redundant channels or elements and most portions are in standby most of the time. Moreover, the few major failures that do occur are likely to be of the "common mode" class (see Sect. 3.2.2), and hence subject again to special corrective measures. The situation suggests that the experience in protection system total failures will produce no meaningful statistics. Some degree of synthesis, therefore, appears desirable in evaluating the overall reliability of an operating system. Perhaps the most promising approach is to assemble the separate experience data from major redundant subsystems and channels and their interfaces in the sense of a reliability model; such experience not only represents essentially all the system functions, but is enriched by including all the system partial failures whose consequences are limited by redundancy features.

Much the same considerations apply in evaluating reliability for a class of systems. Again, subsystem experience may prove more viable than data on disabling failures. And for the reasons developed earlier, any experience summaries will be more enlightening if they distinguish between early and mature system operations.

3.8 Analysis Precision: Boundary Solutions and Confidence

When probabalistic modeling or operating statistics are used to forecast future reliability of a system, there is always the question of how "good" such point estimates are. The chapter thus far has described many analysis practices that will strongly influence any calculated results. Beyond such considerations, however, are the acknowledged uncertainties in the elemental data applied. The effects of the uncertainties on problem solutions can, to a limited extent, be evaluated formally by confidence techniques or more generally just by observing the spread between boundary case solutions obtained from the data extreme values.

3.8.1 Confidence in Operating Statistics

Confidence is derived from a branch of probability theory dealing with finite samples randomly drawn from parent populations. The theory describes the likelihood that the sample statistics will approximate the characteristics of the known parent to within any arbitrary pair of limits or interval; as one might expect, it confirms that larger samples tend more to resemble their parent populations than do individual small ones. In practical analyses, sample observations are referred to assumed forms of parent distributions which may be unknown. Hence, the term confidence is used instead of probability to express the calculated chances that an interval, sometimes about a point estimate, will include the "true" value, that is, the value which would hold if the parent distribution was indeed of the form assumed. Additional background on the topic is given in Example 1.4.

The operating statistics of interest here concern mainly time to failure of devices, subsystems, or systems, as discussed in Section 3.7. Examples 1.4.2.1 through 1.4.2.4 illustrate how such failure data might be analyzed. The first case represents a system that is subject to repeated random failures. Next considered is the replaceable component in a system, assuming initially that the actual failure distribution* is exponential (Ex. 1.4.2.2) and then that the distribution is normal (1.4.2.3 and 1.4.2.4). Confidence for the component exponential distribution example is calculated

---

*See Section 4.2 for discussion of failure distributions.

according to a formula for a test with fixed truncation time; the formula derivation, beyond elementary reliability texts, is based on the Poisson probability law for number of failures observed in a fixed time. A similar formula is available to evaluate confidence for tests ending with fixed numbers of failures; the derivation is again complex, but now based on the Gamma probability law for waiting time to a specified number of failures.

The results for the numerical examples illustrate that the confidence intervals tend to become broad when the data are thin. In other words, one can hardly expect precise definition of a characteristic failure distribution from just a few random points. Treatment of data similar to Example 1.4.2.1 for disabling failures of very reliable systems would presumably produce very poor resolution for the reasons covered in Section 3.7; if the data were satisfactory, it would only be because of excessive failures, correction of whose causes would become mandatory long before confidence calculations confirmed the obvious.

In practice, often only the lower limit of reliability is of interest. "Single ended" confidence is then calculated, that is, a value corresponding to the appropriate distribution curve area with just one tail excluded. The full significance of few or even no failures is expressed more effectively by this criterion since the confidence figure is not diluted by consideration of what the highest reliability might be.

3.8.2 Confidence Calculations to Establish Test Frequencies

In Section 3.4.6, it was indicated how analysis can be applied to determine the need for test facilities or the frequency at which tests should be conducted. It was assumed there that failure distributions were exponential and the failure rates (i.e., λ values) known. Actually, the failure rates are better learned from operating experience. One approach to assuring reliability while such experience is being developed is to apply confidence techniques to establish test intervals. Jacobs outlines such a method in Ref. 51, whereby the λ value is progressively updated from continuing observations of failure.

The method assumes exponential failure distribution and essentially determines lower confidence limits in λ, based on observed failures,

running time, and the desired level of confidence. Arranging the expressions to yield the test interval produces the following formula:

$$\tau = \frac{4(1 - R)\, nT}{\chi^2_{(2r+2),\alpha}} ,$$

where

R = required average reliability over test interval,

n = number of components or channels observed,

T = total time of observation,

r = number of failures observed,

α = confidence level,

χ^2 : chi square, from tables.

Applying the formula first to systems intended to be very reliable, one finds generally that the calculations indicate system tests at prohibitive frequencies. Jacobs notes, for example, that even after observing a system to be trouble free for 114 years, it is still necessary to test every 8 hr in order to demonstrate 10^{-5} or lower average failure probability with 95% confidence. Such high test frequencies appear practical only in unusual cases, perhaps where instrument systems can be tested by perturbations that are automatically programmed and monitored. More modest reliability and confidence goals, of course, result in more realistic test intervals. For example, if three instrument channels were trouble free for 10,000 hr and only 0.99 average reliability was required of each channel, a test interval of 260 hr would assure the reliability with a confidence of 90%.

Complete dependence on the confidence-based formula invites a compromise of reliability under certain not uncommon circumstances, namely, a rapid increase in wear-out failures following a period of perhaps several years of satisfactory operation. The calculation results would then change only to the extent the chi-square value responded to the additional failures. Thus, where a reduction of test interval of maybe 25% might be indicated, actually very frequent testing or even group replacement would be more in order.

3.8.3 Confidence in System Probabalistic Analysis Results

The concern here is with values of reliability predicted for systems not yet operating. Such predictions, since they are not based on direct observations of the system, are statistically "absolute," not subject to confidence evaluation. Nevertheless, the supporting component data presumably are from observations which would allow confidence to be calculated. And even with inadequate data, a reasonable estimate often can be made for a component of the interval corresponding to a desired confidence level.

In selecting a system confidence level, then, it would be fairly simple to find and apply the corresponding component reliability interval extremes to determine a pair of bracketing system solutions, one all-pessimistic and the other all-optimistic assumptions. However, the fallacy in such an approach is that the individual deviations rarely if ever accumulate all in one direction. Vesely,[53,125] of Idaho Nuclear Corporation, attempted to resolve this problem by applying dimension analysis techniques in which the magnitude and direction of each component reliability deviation from "best estimate" is treated as a distributed continuous variable,* hence itself subject to probability estimation. The probability distributions for the usual single-valued estimates in a system analysis are substituted so as to weight the effects of the individual deviations on the system reliability outcome. The overall effect is essentially one of synthesizing a system confidence interval.

There could be a temptation to construe distribution of system failures vs time from the statistics of ordinary Monte Carlo simulations and for these to derive "confidence" limits. However, such values would be totally worthless with regard to the real systems represented, since the only basis for the "pseudo-distribution" would be the artificial nature of the simulation.

---

*All components assumed to have exponential reliability function, and each failure rate (λ) is assumed to be a log-normal distribution rather than the usual single value. The distribution parameters for each component λ reflect the uncertainty associated with the failure rate of that component.

3.8.4 Analysis Evaluation by Boundary Solutions

The preceding section suggested that analysis problems could be solved in turn with pessimistic, average, and optimistic data. Regardless of the fallacy that was pointed out, such a boundary solution procedure does provide a crude measure of prediction "closeness" in lieu of confidence. A further consequence of the fallacy should be recognized before attempting to evaluate prediction excellence by this approach: the spread in results tends to become absurdly large for analyses involving many components.

3.9 Analysis of Reactor Systems

Analysis principles and practices have undergone development from the original simple reliability models through sophisticated modern techniques for handling generalized event probabilities. Most of the credit is due the weapons and aerospace programs, where efforts were spurred by the necessity to produce highly novel and complex systems at a hitherto unheard of pace. By drawing attention to the significant analysis advances in these programs, the literature of the early 1960's stimulated serious interest in similar approaches to enhance reactor safety.

The ensuing application studies at first were concerned with straightforward problems of adapting analysis techniques so that they could adequately represent reactor systems. In matters of modeling and calculation capability, the early results were promising. However, difficulties were soon encountered in finding the necessary support data, and further confusion arose regarding what situations should be examined in the course of evaluating protection system reliability. Substantial progress has been made in resolving these problems, and, in maturing, analysis has emerged more in roles of implementing design and quality assurance than as an instrument for absolute prediction.

3.9.1 Salient Aspects of Protection Systems

It has been indicated throughout this chapter how reactor protection systems as a class are subject to particular reliability considerations that strongly influence the formulation of analysis problems, nature of

conclusions sought, and types of relevant supporting information. These factors have not merely required special structuring of computer analytical programs but have occasioned departures from traditional methods of acquiring data. Moreover, attempts to account for them have had the beneficial effect of promoting risk analysis beyond the usual limits of equipment reliability.

In reviewing some of the more apparent of the factors, reference is again made to Example 2, which was contrived partly to show how they may affect a simple reliability model:

1. Protection systems, except for their active sensing elements, typically serve in standby for long periods; some functions may never be called on outside of tests, while others may be demanded on the average of perhaps twice per year.

2. The primary system function is vital to plant safety; required reliability levels for any particular system or subsystem, however, depend on demand frequency, failure consequences, and effectiveness of backup facilities.

3. Typical protection systems consist mostly of conventional equipment, of which the main items (e.g., large pumps) may be virtually custom built; some systems require equipment that is novel, complex, or otherwise exotic.

4. When demanded by plant emergency conditions, the system must respond promptly; some equipment then continues to operate but for intervals very short in terms of ordinary service life expectations.

5. Most of the equipment is conservatively applied and subject to a normal industrial environment. Some components are required to withstand hostile environments or transients that challenge state-of-the-art limits. Moreover, entire systems are expected functionally to survive DBA conditions such as earthquakes, missiles, etc.

6. Particularly with highly integrated systems, some components, subsystems, etc., are subject to alternate failure modes, which will have different effects on system performance. Some failures may even defeat operation of backup facilities, hence constitute common mode failures.

Item 5 draws attention to accident conditions. Evidently, for equipment to perform effectively in mitigating DBA's may involve a great deal

more than ordinary quality or reliability. One of the principal aims of safety research is to define the conditions under which certain equipment must survive. Once defined, at least in the extreme, the requirements can be factored into equipment design as well as reliability assessments. In advance of complete information, however, dependence has been placed on very conservative design.

3.9.2 Emerging Application Roles

The benefits of redundancy features in systems quantified by the earliest analyses of missiles and aircraft were exploited in designs of reactor safety instrumentation and scram actuator systems long before it became popular to perform reliability studies on such equipment. Interest in formally evaluating the reliability of safety shutdown systems developed during the late 1950's. At that time, some straightforward modeling of the designs was being done to provide a basis for reliability predictions as well as to compare alternative system configurations.

The techniques then used were the simple ones appropriate to hand or analog computer calculations. Support data rather than modeling capability, however, placed the main limitations on the validity of the analysis results. The difficulty lay in defining life and failure characteristics of equipment which was novel, changing rapidly, and produced either experimentally or only in small quantities. In attempting to resolve the data problem, some consideration was given to the military programs that had logged experience with instruments and electronic gear at least generically like the reactor instrumentation. Moreover, the military were attempting to synthesize electronic device reliabilities from parts data obtained by extensive tests. Although some minor attempts to analyze reactor equipment by parts followed in this country, the UKAEA has since pursued this approach at length. Meanwhile, the equipment characteristics have become better understood, and more elaborate analyses, using modern techniques, are presently being performed in conjunction with the further development of safety shutdown systems.

Protection functions beyond reactor shutdown had assumed major importance by 1965, and difficulties were being experienced in evaluating the highly integrated systems proposed to perform the functions. The

USAEC at that time launched development efforts through contractors to demonstrate the feasibility of applying advanced analysis techniques to assess broad safety-reliability problems. This work produced, first, a comprehensive fault-tree study by Atomics International[54] of the safety system for a conceptual plant, the Heavy Water Organic Cooled Reactor. Longer range studies were undertaken by H&N who adapted computer programs to express reactor system considerations and sought means for providing analysis support data. Their work resulted in the SAFTE programs, described earlier, in addition to a pilot data collection effort discussed in Section 4.4.2.2. Although the pilot effort was a major step in reducing concept to practice, it did not offer immediate prospects for fully objective assessments of the reliability aspects of safety. Clearly, such capability would have to wait on a more complete knowledge of component failure characteristics and accident mechanisms.

Subsequent development and application of analysis methods has continued in this country, mostly in the private sector. Since the studies are mainly proprietary, they are little publicized; thus the current literature is not a good index to the present level of activity. Several reactor manufacturers now routinely perform analyses which aid in optimizing design of systems to perform specific protection functions or which enhance the design review process.[120,121] Their efforts employ the qualitative methods perhaps more than quantitative. References 56 to 58 describe recent analyses of systems for AEC-sponsored reactors, while Ref. 55 describes an earlier private study.

The bulk of the current studies deals with more-or-less isolated reliability problems, but does not really address the broader protection system evaluation and optimization questions. The latter concern not only straightforward safety assurance but such problems as determining the overall effectiveness of each major safety feature proposed. Responding to the added challenge, the UKAEC and, in the U.S., the General Electric Company, have developed extensive analysis capabilities with which to model and resolve the more complex problems. Both organizations employ event modeling, augmented with such considerations as time dependencies and effects of degraded performance of functions. The many alternative outcome situations

encountered are represented by decision trees (see Ex. 2.5). Reference 32 discusses some decision aspects of reliability analysis, while Ref. 101 describes the UKAEA approach to the overall problem. To overcome the data deficiencies, the UKAEA has developed a sizable information bank and General Electric is attempting to synthesize device reliability estimates out of engineering considerations; these efforts are discussed in Chapter 4.

In only a few instances have analysis case studies or their conclusions been introduced directly in support of commercial reactor license applications.[27,122,123] The practice has not been encouraged, partly because the studies themselves tend to be too complex to review properly. Moreover, analyses of diverse origin would at least appear inconsistent, thus inviting criticism and debate to distract from more solid issues.

The recent USAEC-DRDT Standard for Protection Systems[90] requires (1) that quantitative goals be established for subsystems as a part of the design basis and (2) that the goals be met as a general functional requirement. However, it is not specific on the role of analysis in evaluating the systems. One possible outcome may be to stimulate development of some "rules" for simple and consistent modeling along with uniform data for use in such models.

3.9.3 Current Status and Trends: An Evaluation

The present trend shows reliability analysis applications gaining sharply in the area of reactor systems development, and with wider usage we may expect continual refinements to improve the quality of the case studies.

Clearly, formal reliability analysis has not had an impact on reactor development comparable with that in weapons and aerospace projects. To draw parallels between the applications is inevitable as well as instructive. Several of the major aerospace projects were very bold in concept and initially presented large areas of uncertainty. Reliability analyses for these were then quite speculative in the sense of absolute prediction, since neither the device characteristics nor the stresses which components would encounter were well known. Hence the assumptions came to be regarded constructively as quality assurance goals. To expand even the vaguest conjecture to realistic engineering considerations became a principal role of

analysis: specific capabilities to be developed, special characteristics to be verified by test, or particular properties amenable to quality control. The prospect of unanticipated effects causing system failures had to be accepted, but it was felt that the massive quality assurance support could take care of these in due course. Qualitative analysis down to fine detail was an essential element of this confidence.

Scale factors of time and quantity were both quite favorable to the analysis approach in these essentially military projects. Thus, with a system being conceived, built, and operated within the span of a few years, there was ample opportunity for effective information feedback. Moreover, many of the systems of interest — weapons, missiles, aircraft — were produced and tested in numbers that permitted statistically satisfactory confirmation of their ultimate performance.

Thus to a large extent quality assurance imparted credibility to analysis in the weapons and aerospace programs. The increasing private applications of analysis in reactor systems development suggest that progress there is following a similar course. However, confirmation of reactor protection system effectiveness will have to come from observations other than repeated actual reactor accidents. That is, most of these systems will remain in standby over the entire lives of the plants they serve, tested periodically but never to operate under their design accident conditions. Special measures, for example, severe equipment tests and penetrating inspections off-line, must therefore be devised to confirm both initial and sustained capabilities of protection systems to fulfill their functions.

The efforts by General Electric and the UKAEA point the way to some needed refinements of analysis, in particular, analysis of overall protection system response to specific accident-initiating conditions. Reliabilities of supporting functions or contributing systems are then of subordinate interest, and the main concern is the ultimate plant outcome. Expanded analyses of this type not only complement DBA investigations, but permit methodical examination of a wide range of situations with less severe accident potentials. In fact, this kind of broad approach seems the only feasible path to ultimate risk evaluation.

Returning to the detailed level, it is clear that the information input to system analyses needs to be greatly improved. Chapter 4 discusses

further how such information is being obtained and made available. But there remains the important question of how it shall be expressed in probability models, and here, it is the author's conviction, some serious errors are frequently introduced. Perhaps the worst misrepresentations arise in the use of "average service" life or failure data to characterize the probability that a device will survive an extreme stress; the data may be irrelevant, and the resulting error may easily be several orders of magnitude. Another important source of error is neglect of device operating mode in a particular application; for example, average failures of diesel engines per operating hour have little bearing on the vital probability of starting on first trial. The criticisms are partly by way of emphasizing earlier arguments that analyses must be conducted primarily by engineers familiar with the equipment. In addition, the common practice of expressing virtually all component reliabilities as exponential functions of time seems in need of overhaul. At least one simple expedient for adding realism appears to have been overlooked in this regard, that is, dividing the reliability of a device among discrete operating phases. Using the diesel engine for example again, one might consider "start," "assume load," and "extended operation" separately, with a simple probability expression for each phase.

To what extent the ultimate risk analyses of reactors will become convincing depends on how well the present problem uncertainties can be resolved. For the immediate future, however, the primary role of analysis is to enhance quality assurance. The developing interest in such applications is most evident in the area of system design. From the experience of the weapons and aerospace projects, we may see reliability analysis eventually assume an integral role in overall quality assurance. Its potential for providing detailed guidance will then be fully exploited, and resulting feedback of project realism should increase the objectivity of the analyses.

4. RELIABILITY OF COMPONENTS

The term "component" may refer to anything from a simple part to a complex device or system. Ordinarily it signifies an integral item of equipment which has one or a few contributing functions in a principal system of interest.

The earliest manufacturing and product application efforts relied on qualitative observations to evaluate serviceability; improvements then followed from investigations of failure or other unsatisfactory performance. Such procedures, both formal and informal, still provide important insights. But beginning with the work of the early industrial engineers, statistical methods have progressively been introduced to enhance, first, quality control and, later, product development; their use now ranges from materials through mass-produced assemblies and devices. Similar techniques were subsequently extended to problems of predicting and evaluating reliability of complex components on the basis of operating experience, and advanced applications concern the monitoring of equipment in service to assure continued satisfactory performance. Meanwhile, the knowledge of fundamental failure mechanisms has grown steadily in support of product development and is now being used effectively to complement the equipment experience data.

4.1 Failure Fundamentals

A brief review of the physical aspects of equipment failure will establish the basis for at least an intuitive understanding of the reliability objectives and methods at the component level.

The mechanisms that ultimately cause component failures act on the parts and materials of which the equipment is made. Typically, these include mechanical stresses, both random and cyclic; erosion or wear; corrosion; depletion of active or sacrifice materials; materials degradation caused or influenced by temperature, chemical action, or radiation; accumulation of foreign materials; etc. Many such effects are described in detail in Ref. 64. A single part may be subject to several degrading processes sequentially or concurrently, and these effects may be synergistic.

Occasionally a part failure is attributable to only one mechanism, but more generally failure is preceded by a gradual degradation involving several mechanisms, the final traumatic event then amounting to the arrival of a transient stress greater than the weakened part can withstand. Degradation rates can vary widely during the life of a part, sometimes appearing almost stepwise; many materials also have significant recovery properties following overstress.

With parts failures reduced to terms of degradation and overstress, the factors underlying failure distributions begin to emerge. The earliest failures in a population would be expected to include parts initially weak or defective and which may have been only moderately stressed. They will also include normal parts subjected to very severe early stresses. Later failures should involve some "average" parts that had so degraded that they could not withstand fairly severe stresses. The longest-lived parts are perhaps those that were initially the strongest, had the least lifetime deterioration, and were luckily spared the worst transient stresses.

Many common parts or simple components exhibit the properties just described. Ball bearings, for example, have service lives (defined in cycles rather than time) that can be predicted fairly accurately as functions of load for normal conditions; adverse conditions reduce the life expectancy greatly. The failures among good-quality lamp bulbs or electronic vacuum tubes of a particular model similarly tend to concentrate around the mean life value. While there is no known wear-out or depletion mechanism for transistor devices, there are degradation effects due to imperfect quality control; important among these is deterioration due to contaminants that are either introduced during manufacture or enter via poor seals. Such effects are generally unpredictable and often associated with manufacturing batches; they can result in what appear to be random scatterings of failures in time. Some organic electrical insulation materials at first improve with age and subsequently begin to lose mechanical strength. The deterioration is thought to follow the Arrhenius chemical rate law, doubling for each approximately 10°C increase in temperature. Insulation dielectric strength may appear virtually unaffected until the last stages of embrittlement; however, with loss of physical integrity,

any moisture present can quickly penetrate the insulation when cool and reduce the dielectric strength virtually to nil.

Elemental parts and materials are combined in as many different ways as there are component designs. However, intriguing though it may be as a design objective, only rarely is it practical to select or design elements which are at all consistent in reliability characteristics. As a rule we find that a few elements dominate the reliability of a device, and often these same elements are also intended to be overhauled or replaced routinely within the lifetime of the main device. At least this tends to simplify the task of component evaluation by allowing us to concentrate on the more probable routes to failure.

A regard for the basic failure mechanisms is perhaps the broadest unifying consideration throughout all the efforts to achieve reliability. In the development of materials and parts, the most obvious objectives are the practical definition of basic properties and their resolution with general application requirements; the development results gain expression in various ways, such as application limits, life data, and quality control requirements. The successful manufacture of devices which combine many parts and materials calls for a good understanding of the fundamental strengths and weaknesses of the individual elements, with the added knowledge of how these effects could interact over an anticipated range of equipment applications. Systems design may seem to entail simply the routine selection of qualified equipment; however, this frequently involves problems of defining or creating specific application conditions so as to assure that none of the basic limitations of the equipment will be violated. System construction quality control has similar aims. Major objectives in the operation of systems are to avoid conditions that stress elements known to be delicate, to replace elements having recognized deterioration mechanisms before incipient failure conditions threaten reliability, and to discover any weaknesses not originally anticipated during the design or initial tests. Finally, reliability prediction is largely a matter of assessing what basic failure modes will dominate and how great will be the effect of each.

4.2 Failure Statistics

In Chapter 3, the failure probability vs time was assumed to be known for each component. It was convenient to express the relationships generally as [P(t): component K is failed]. This section considers briefly the background and basis for these probability expressions. Additional material on this topic is presented in Refs. 1, 2, 4, 5, 6, 8, 9, and 10; Refs. 1 and 68 also provide indexed bibliographies.

4.2.1 Frequency Distribution of a Random Variable

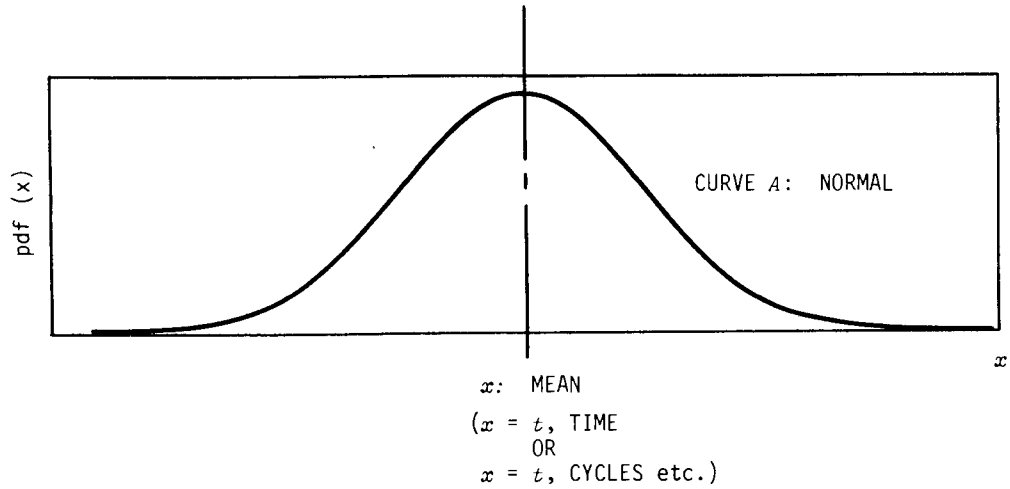
Early observations of human mortality were summarized in histograms, which showed the actual number of deaths out of some original population that occurred in each equal age increment. Such diagrams are crude frequency distributions of the random variable, age at death. Simply multiplying the ordinate scale of the mortality histogram by 1/(histogram area) transforms the diagram into a "probability density function" (pdf) plot, wherein the area corresponding to each age interval represents the population fraction that died in that interval. The pdf area from 0 to any given age t is then the population fraction dead at age t, or the probability that a member randomly selected from the original population will die before age t [P(t): member K has died]. With a large population and small age increments, the histogram approaches a smooth pdf curve which describes the rate of change of the deaths with respect to the original population, or pdf(t) = d/dt [P(t): member K has died]. By definition, the total area under the pdf curve equals unity or certainty.

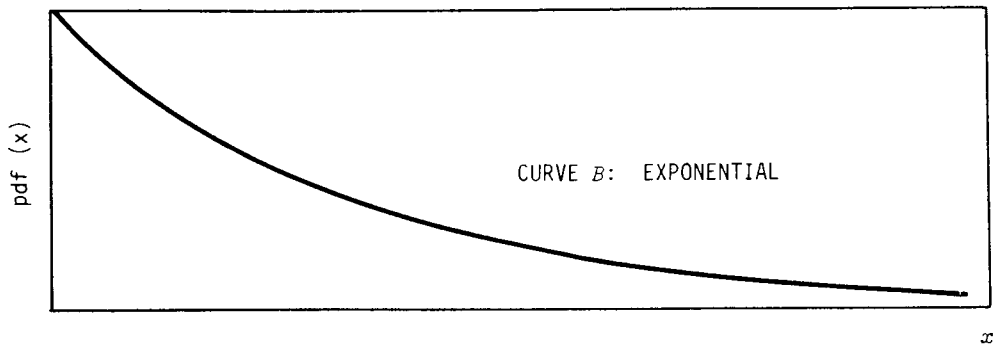
4.2.1.1 Normal Distribution. Eliminating or "censoring" infant deaths from the original populations, the mortality histograms for the remainder take on the familiar bell shape of the normal, or Gaussian distribution. This curve (see Fig. 4.1a) is described by

$$\mathrm{pdf}(t) = \frac{1}{\sqrt{2\pi}\,\sigma} \exp\left[-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2\right],$$

where μ is the mean value of t and σ is the standard deviation, a measure of the data resolution about μ. Applying some of the considerations from

ORNL-DWG 72-2250





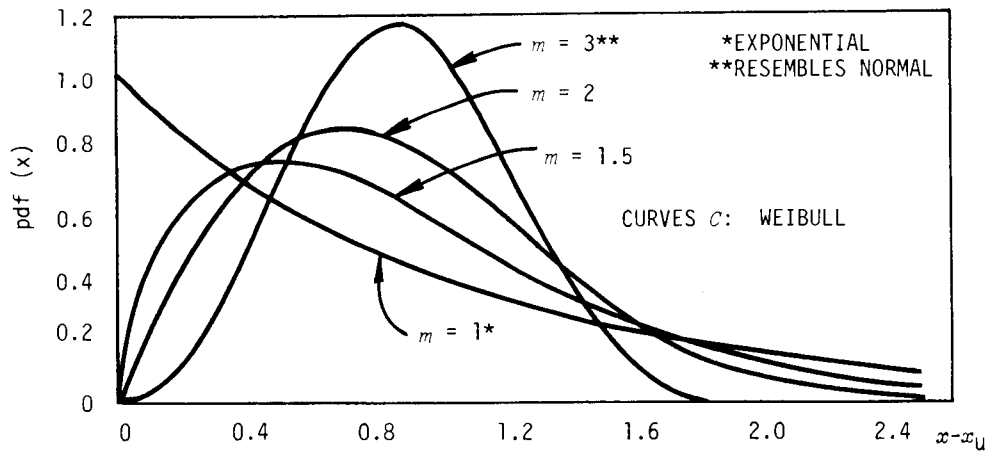


Fig. 4.1. Frequency distributions.

the preceding section, it would seem that if all people were identical and had identical life circumstances, they should all fail by "wear-out" at the same age. In fact, some form of general wear-out does dominate, but other factors blur the resolution. There now appear to be many concurrent wear-out mechanisms in the body; they are not independent, however, but together tend to produce a concentration of mortality around the average (mean) life-span.

4.2.1.2 General Empirical Distributions. The analogy between human and equipment mortality was found useful for depreciation accounting in the 1930's. In particular, regulated utilities had large investments in such items as telegraph poles, railroad ties, etc., whose depreciation was a significant business cost. Extensive records were kept, and empirical distribution formulas were developed[13] for convenient manipulation. These expressions describe mortality frequency distributions (i.e., pdf's) that are symmetrical or skewed, sharply peaked or widely spread.

4.2.1.3 Exponential Distribution. For many forms of equipment, it is easy to project the physical considerations of Section 4.1 to conceive a situation where there is no apparent resolution of failures about any particular age. Age at failure then seems to be as completely random as tossing coins. And in fact the pdf for failure vs time in this common situation can be developed (Ref. 1, pp. 43–49) from the limiting case of the binomial probability (see Sect. 4.2.4) for exactly r occurrences of a particular combination in n trials, that is, the Poisson distribution:

$C_r^n \, p^r \, q^{n-r}$ = [P: event of interest will occur exactly r times in n trials]; in this case, event is a component failure and trial is a particular time interval;

$$= \frac{n!}{r!\,(n-r)!} \, p^r \, q^{n-r} .$$

$p \equiv$ [P: event will occur during any random trial].

$q \equiv 1 - p$.

$C_r^n \equiv$ [Number of combinations of n things taken r at a time]; in this case, the number of possible different sequences by which r failures could occur in n trials.

$$\lim_{\substack{n \to \infty \\ p \to 0 \\ np \to m}} (C_r^n \, p^r \, q^{n-r}) = \frac{m^r \, e^{-m}}{r!} ,$$

where

m = average number of component failures found in n time intervals whose sum is time, t ,

$$= \frac{\text{total time of operation, } t}{\text{mean time to failure, } \theta} ,$$

$$\theta = \frac{1}{\text{failure rate, } \lambda} ,$$

$$m = \lambda t .$$

$$[P(t): \text{ component is not failed}] \equiv [P(t): \ r = 0]$$

$$= \frac{m^o e^{-m}}{0!}$$

$$= e^{-m}$$

$$= e^{-\lambda t} .$$

$$[\text{pdf}(t): \text{ component is failed}] = d/dt \, (1 - e^{-\lambda t})$$

$$= \lambda e^{-\lambda t} .$$

The pdf and the probability vs time that a random failure has occurred are the familiar exponential expressions. Figure 4.1b illustrates the exponential pdf.

A very simple analogy also can be drawn between exponential failure rate and the radioactive decay of materials. Thus

$$dN/dt = -\lambda N(t) ,$$

$$N(T) = N(0) \, e^{-\lambda t} ,$$

where $N(t)$ represents either survivors of an original species or of an original population and λ is the constant decay or failure rate.

4.2.1.4 Weibull Distribution. A more versatile distribution function was introduced by Weibull in 1951. In pdf form, the expression is

$$\mathrm{pdf}(t) = \frac{m(t - t_u)^{m-1}}{t_0} \exp\left[\frac{-(t - t_u)^m}{t_0}\right],$$

where t_u is the location parameter (usually 0), t_0 is the scale parameter, and m is the shape parameter.

If m = 1, and t_u and t_0 are fixed, the Weibull pdf becomes an exponential. As m increases, the pdf resembles increasingly that of the normal form. The Weibull distribution has been found to describe many sets of equipment failure data, notably electron tubes. Several Weibull curves are shown in Fig. 4.1c.

4.2.1.5 "Bathtub" Curve of Failure Rates. Of great practical significance is the composite "bathtub" curve, Fig. 4.2, of component failure rate vs time or cycles. This is not a pdf, since the failure rates are with respect to current rather than original population; however, the pdf could be derived from the curve information. The plot represents three life phases: (1) high initial failure rates due to defectives, diminishing to (2) a low constant failure rate corresponding to "chance" events during normal operating life, and (3) a rising rate with the advent of wear-out failures. It is important to note that system reliability predictions are usually based on the assumption that a deliberate effort will be made to assure that all vital components are operated only in the low-failure-rate phase.

4.2.1.6 Qualified Distributions. The data that determine the distributions may be rather casual (e.g., operating and maintenance records) or they may be from tests carefully conceived and executed. The latter sometimes produce sets of distributions corresponding to ranges of controlled variables; relationships within a set are often described by changes of the distribution parameters. Typically, effects of particular forms of stress are reported in this manner, as described in Section 4.4.1.1.

4.2.1.7 Other Distributions of a Random Variable. In attempting to evaluate relatively subtle effects, more elaborate statistical

ORNL-DWG 72-2251

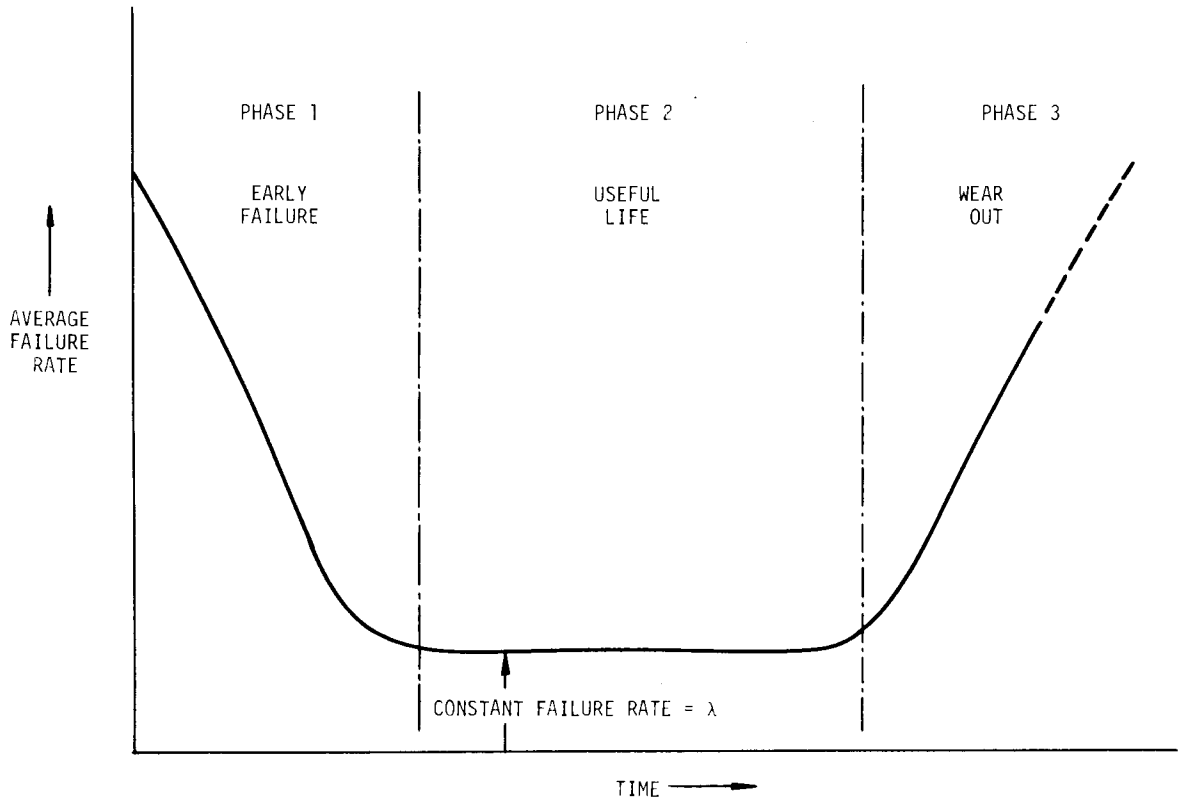


Fig. 4.2. Failure-rate characteristic.

techniques are often required. These could involve various distribution forms other than those described, such as log-normal, gamma, etc.

Two distribution forms, chi-square and Student t, are useful in confidence evaluation. This is covered in Section 3.8 and Example 1.4.

4.2.2 Reliability Function

In integrating a failure pdf, one obtains the corresponding function describing what portion of an original population has failed at any age (in time, cycles, etc.), that is, the failure characteristic of the item of interest or P(t): item is failed. The procedure reduces to practice the random selection analogy described in Section 3.1.2. The actual reliability function is the complement of the failure function, R(t) = 1 - [P(t): item is failed].

In most reliability work, circumstances justify the random failure assumption; hence, that reliability vs age is an exponential function, $R(t) = e^{-\lambda t}$. Accordingly, the pdf step is bypassed, and failure rate λ is estimated directly from time-to-failure observations,

$$\lambda = \frac{1}{\text{mean time to failure, } \theta} .$$

4.2.3 Use of Statistics for Reliability Prediction

The reliability function, which is derived from statistical data, concisely summarizes a discrete body of experience. That experience may be regarded either as a definitive indication of future component reliability or as merely one among various factors from which an estimate can be synthesized. Clearly, the more extensive the experience and the more closely it corresponds to a proposed device application, the greater weight it merits in the reliability estimate.

The principal sources of component reliability data are tests and service records, examples of which are described in Section 4.4. Information developed from these sources is customarily summarized and reported according to generic classes of types of equipment.

Some of the best quantitative information, but mainly for just a few types of relatively small equipment such as electronic parts, has resulted from substantial test programs. Such tests have carefully investigated the effects of life-determining variables over credible ranges and have been conducted on the scales necessary to assure statistically conclusive results. Components and complex devices may also be tested exhaustively, usually during development. The costs of large items and their test facilities, however, limit such activities to the extent that the results are essentially qualitative.

Enough service has been accumulated on many types of equipment found in reactor systems to provide excellent reliability insights. Unfortunately, most of this experience is thinly diffused over many industries, and relatively little has been recorded in ways that could easily yield reliability data. The information banks are attempting to overcome these problems. But the data they offer thus far tend to be fragmentary, hence, inconclusive statistically. Moreover, the data reduction done remotely by the banks may remove much of the information qualitative value by obscuring data origins or circumstances.

Not only is generic average reliability data scarce, but its use in some cases can be misleading. This caution was voiced earlier and bears repetition. In particular, it refers to cases where standby equipment may have to withstand severe stresses preceding or during emergency operation. Evaluation of failure probability under such unusual conditions must be treated as an engineering problem, of which "average" reliability is but one aspect.

4.2.4 Binomial Distribution

The basis for the binomial distribution is that an "infinite" population exists, each element of which has actually assumed one of only two possible states. Of interest are the probabilities that samples drawn from the population will exhibit various proportions of the two states. The laws governing these probabilities are essentially those used in Chapter 3 to describe possible states of system: $(p + q)^n = 1$. The values of p and q are the actual population fractions in each of the

states, and each term of the expansion represents the probability for one possible state combination in a sample of size n. The binomial distribution is useful in evaluating situations on the basis of sample observations, for example, number of defectives in a manufacturing batch.

4.2.5 Confidence

The concept and some applications of confidence were described in Section 3.8, where reference was made to further discussions in Example 1.4. It was pointed out that confidence can be used to express probable accuracy of a reliability estimate with respect to the amount of experience back of that estimate.

Example group 1.4.2 was contrived to suggest the amount of data obtainable from typical service records on a component class in a single system. That such data might not be conclusive for small samples is reflected in the rather broad intervals for 90% confidence about the "best" estimates for mean time to failure. Much better results could be expected for similar observations on the same component applied in many systems or life tested in large numbers.

As a cautionary note, favorable confidence figures (i.e., high confidence for a narrow interval about an estimate) are no guarantee of a good reliability estimate. That is, a set of data and an estimate could be badly biased for any number of reasons but still indicate high confidence via the formal calculations.

4.3 Practical Measures to Assure Component Reliability

A realistic effort to assure the reliability of a component begins with the determination that the component is basically qualified to perform its intended function and continues through quality control to the long-term monitoring of integrity in service.

4.3.1 Component Qualification

To determine that a component is qualified for a particular application may be as simple as checking to ensure that all service factors

for a standard item are within normal ranges and, of utmost importance, that the component is in fact basically matched to its task. However, some applications involve newly designed equipment and/or present possibilities of severe stress which a component may not have been demonstrated capable of withstanding. Problems of this nature are usually resolved by tests that simulate extremes of the anticipated operating conditions.

The question then arises: On what basis do we judge the test results to decide whether the component design is satisfactory? In a few cases of interest, for example, minor parts, tests may produce conclusive statistical results. More commonly it is practical to test only one or a few expensive prototypes, so that even the complete absence of failures in a reasonable test regime would then indicate high reliability only with rather low confidence. Some practical expedients for shoring up such inadequate statistical evidence are: (1) post-test physical inspection of the prototype(s) to determine the existence of degradation, wear, etc., that could reasonably be associated with the test conditions; (2) review of experience, if any, with similar components in similar applications; and (3) during early operation, presume the component to be of adequate reliability for intervals or duty cycles much shorter than actually expected and, accordingly, test or replace the item frequently until proved. Merely to increase redundancy of the component in question is usually not the answer, since like elements could share a common basic deficiency.

A short lifetime is not inconsistent with high reliability, provided this is recognized and arrangements are made for frequent device renewal. In reactors, however, the most severely stressed components are generally those in the core, for example, many of the sensors that initiate protective action and are inaccessible during operation. Qualification tests for these should be rigorous and should provide adequate physical evidence that the service life will at least exceed one fuel cycle by a generous margin.

Still in regard to component qualification, passing mention is made of a design technique currently attracting interest. This is the

"Stress/Strength Interference Theory," which seeks to represent deviations from nominal strength of and stress on a part as random variable distributions. The extent to which the high end of the stress curve and the low end of strength curve overlap, or "interfere," is then regarded as a design parameter and is related to the part reliability. While the technique could be useful in design of pressure vessels, piping, structures, etc., it does not seem immediately applicable to protective systems reliability work. References 14 and 52 introduce the concept.

4.3.2 Component Quality Control

Quality control has stirred a great deal of controversy in the reactor industry. The point at issue is whether components produced to manufacturers' or conventional industry standards are satisfactory for reactor applications. A recent marketing seminar sponsored by Power Engineering produced considerable opinion to the contrary. The situation was summarized by A. P. Perez, president of the Florida Power Corporation: "It is the general complaint throughout our industry that there is a deterioration in quality. This comes at a time when we are using very large units, and can ill afford the reliability risks and financial hardship imposed by unnecessary outages."[86] On the other hand, attempts to impose rigorous standards have resulted in severe cost increases, occasionally to several times the price of the same item off the shelf. The more dramatic cost increases are not necessarily unjustified; it is easily seen that custom tests, complex inspections, etc., on a small production batch could well exceed the costs of manufacture. Levine of the AEC Division of Reactor Licensing speculates that although the quality assurance effort for nuclear power plants will increase the total plant costs substantially, the additional expense should be more than returned in improved plant availability and load factors.[122]

The statistical methods so useful in monitoring quality of large production runs find only rare application in regard to nuclear systems components. The latter are mainly few-of-a-kind items, for which the most effective quality control includes such measures as close parts tolerances, extensive inspections during manufacture, and realistic tests of all completed equipment.

Quality control at the reactor plant construction site is certainly as important as that during components manufacture. The obvious reasons are that (1) equipment is often damaged between leaving the factory and final installation, (2) delicate devices may be inadvertently overstressed, for example, electronic equipment can be damaged by transients during circuit checkout, and (3) improper installation can cause early equipment failures, for example, machinery bearing failure due to misalignment.

4.3.3 Testing and Monitoring in Service

Extensive periodic test programs and some installed monitoring devices are employed to assure the continued integrity of reactor protective system components in service. These measures are designed primarily to discover gross failures and drifts off calibration.

The perennial question of optimum frequency or interval for periodic tests was covered in Chapter 3. Section 3.4.6 indicates a calculation method for the case where outage time for testing is a consideration, and Section 3.8.2 describes a way to update the test interval consistent with confidence in apparent failure rate.

The relationship between "random" failure rate (λ) and test frequency appears to have only limited usefulness, mainly for purposes of planning for test facilities and maintenance staff and for broad-scale monitoring of reactor operations. To assure reliability in an actual reactor plant, the physical circumstances of each equipment failure, malfunction, or evidence of degradation deserve a great deal more attention than the usual rather meager statistics in determining test frequencies as well as other maintenance and operating policies. This indicates the need for careful investigation of individual occurrences,

not only with regard to immediate correction requirements but also considering the following broader reliability implications:

1. Does the "failure" suggest poor manufacturing or construction quality control? Perhaps this can be identified with a fabrication batch or construction phase, which might be investigated further.
2. Does the "failure" indicate a design error or some design factor overlooked? A larger capacity component may be needed, or a relocation, or supplementary equipment, etc.
3. Is "normal" wear-out indicated? If so, a periodic replacement or overhaul program for similar components must be considered.
4. Is premature wear-out indicated? Perhaps the contributing conditions can be identified and corrected or frequent replacement planned.
5. Do individual or repeated "failures" suggest inadequate maintenance policy, for example, training or supervision?
6. Does a failure or malfunction result from idleness? For example, some steam valves are known to collect deposits on their stems, preventing operation; this condition can be relieved by periodic exercise.

Some practical answers to the central question of test frequency can be derived from the above considerations. First, as much operational testing as is feasible should be performed before a plant is placed in operation, that is, all vital systems and equipment must be thoroughly debugged. Second, test frequencies for steady-state operation may be established on the basis of expected "normal" failure rates, <u>except</u> where overriding physical reasons are evident or the statistics indicate difficulty. Third, evidence of wear-out or other cumulative effects must be sought deliberately and such conditions dealt with as individual problems.

4.3.4 Long-Term Effects

The matter of detecting wear-out, cumulative degradation, or other incipient failure conditions amounts to assuring that no vital component or set of redundant components will ever become so weakened as to jeopardize the protective functions. The problem is aggravated if the emergency conditions stress the components severely. Not only are in-core

components always suspect, but more conventional applications such as electrical equipment may actually become very unreliable with time. A prime example of unfailed but yet unreliable electrical equipment is the motor with degraded coil insulation; it is a likely candidate for failure due to the mechanical stresses of an ordinary startup or due to loss of insulation dielectric strength by absorption of moisture during idle periods in a wet location. If the motor were located within a reactor containment, it might well choose the occasion of a loss-of-coolant accident to fail, as the immediate consequence of wet steam.

Just how incipient failure conditions can be eliminated depends on the type of equipment. Perhaps the best guidance in this area is that obtained by interpreting the components' qualification engineering and test data.

4.4 Reliability Data Programs

The preceding discussions have indicated the wide variety of information that may contribute to an intelligent assessment of equipment reliability. To collect, store, and retrieve such information effectively for components of many types is an enormous task, requiring organization consistent with defined reliability objectives. Numerous programs have undertaken to develop parts and equipment reliability data methodically. The earlier ones were limited to special classes of equipment; more recent programs have been of increasingly broad scope, usually to meet the needs of the major military and aerospace projects. Similar comprehensive programs for reactor systems components are now emerging.

Reference 65 lists and summarizes about 120 information programs that handle data relevant to the reliability efforts of the U.S. military services, NASA, and their contractors. It further states that, altogether, "Over 1100 scientific and technical information centers currently exist in the United States." Relatively few of these, however, are more than incidentally concerned with either components or reliability. The remainder provide supporting and background material on diverse subjects, individually important to particular reliability studies. The information specialities of the programs listed range from basic materials properties

(e.g., the Plastic Technical Evaluation Center, PLASTEC) to phases of engineering technology (e.g., the Shock and Vibration Information Center, SVIC); some of the programs represent special library facilities (e.g., the University of Pennsylvania's Module Engineering Analysis Library, MEAL) or clearinghouses for technical reports. Another comprehensive summary of data sources is provided in Ref. 66.

Several of the programs just referred to have also been major sources of components information in reliability analysis of reactor systems to date. This has been true particularly for instruments and electronic gear, the equipment forms of main interest in the earlier studies of safety shutdown systems. In addition, the analyses have drawn on the few isolated reactor project data collections and the material provided by the equipment manufacturers.

4.4.1 Nonnuclear Component Data Programs

The reactor data programs, actual and proposed, emulate the military, aerospace, and commercial aviation information systems. Five of the latter are reviewed briefly in order to provide a background for further discussions of the reactor data programs and to emphasize certain features of potential value in reactor reliability work.

4.4.1.1 Rome Air Development Center (RADC) Program. The purpose of the RADC program is to develop U.S. Air Force ground support electronic equipment. It is one of several sponsored by the Department of Defense and tracing their origins back to the recommendations of the Advisory Group on Reliability in Electronic Equipment (AGREE).[22] In the early 1950's, it was sought to develop reliability in electronic systems on an objective basis, that is, through understanding and control of all factors. Extensive investigations of component life and failure characteristics constituted a major phase of the work; these were conducted partly in house and partly by contractors, notably RCA. Beyond the "average" characteristics, it was attempted to determine the effects of loading, environmental factors, and any other unusual stresses to which the equipment might be subjected. The results of the components work were expressed initially in terms appropriate to the particular types of equipment;

these included curves of failure rate vs application variables, recommended usage limits on application variables, derating factors, etc. Equipment application guides were then developed from the data, recognizing anticipated environment extremes and providing practical advice in equipment selection, configuration, and loading. In 1958–59, the RADC was responsible for one of the first attempts by the military to purchase equipment according to formal reliability specifications; this work is represented by the standard MIL-R-26474 (USAF).* Much of the RADC components reliability data was incorporated in MIL-HDBK-217.[70] References 23 and 24 describe the RADC program and present some of the early results. On a current basis, the RADC operates a reliability information service,[65] Reliability Analysis Central (RAC). It is appropriate to note here that a parallel DOD program under the U.S. Navy auspices produced another compilation of electronic equipment data for shipboard application, NAVSHIPS 93820.[72] There is now also an MIL-HDBK-217A,[71] which provides data on transistors.

4.4.1.2 Parts Reliability Information Center/Apollo Parts Information Center (PRINCE/APIC).[65] In view of the extraordinary emphasis on reliability for the space flights, it was expedient to establish a centralized project-oriented reliability program at the Marshall Space Flight Center. This program serves as a focal point for all Apollo information on parts and materials. Included in the store are drawings, test reports, specifications, and many other forms of information received from NASA centers, contractors, manufacturers, etc. The wide variety of parts and components has necessitated an elaborate indexing scheme to permit retrieval by parts classification or by system where applied. A major objective of the program is to coordinate project reliability activities, thereby reducing duplication of effort and generally improving project efficiency. PRINCE/APIC now incorporates two programs originated at Battelle Memorial Institute, the Electronic Component Reliability Center (ECRC) and the Transducer Information Center (TIC). Information output from the program is on a current basis, usually in response to inquiries.

---

*Superseded by MIL-STD-785 (see Ref. 25).

4.4.1.3 Federal Aviation Administration: Maintenance Data Analysis Program.[73,115] The FAA is largely concerned with the safety reliability of commercial aircraft. One major activity in this area is to monitor the maintenance programs of the air carriers via performance failure records and defects discovered during maintenance or inspection. Information is reported to the central data facility in Oklahoma City by about 220 field inspectors. Statistics such as moving average failure rates are derived from the information, and unusual incidents or findings are given special review. When a situation is discovered that suggests a design defect, maintenance deficiency, etc., with safety implications, the responsible organizations are alerted and the corrective actions subsequently monitored. The statistics are considered with regard to any proposals to relax periodic maintenance or inspection requirements, but generally they must be supported by physical evidence that the change will not affect the failure probabilities. For example, if it were thoroughly established that wear-out was the only degradation mode of a part, it might be acceptable to lengthen the inspection interval upon demonstration that the part invariably passed several of the current inspection cycles before wearing beyond tolerance. Reference 73 describes the FAA program in further detail, and Ref. 74 discusses similar programs carried on by the airlines.

4.4.1.4 Failure Rate Data Program (FARADA).[116] In 1960 the Bureau of Naval Weapons instigated a study to determine the availability of failure data for a wide range of components and the feasibility of a program to collect such data. The establishment of the FARADA program in 1961 followed from the results of the study. By 1969, it served about 300 participating agencies of and contractors to the U.S. armed services and NASA; each contractor is primarily a user of parts and components and must be generating failure rate data of interest via tests or operating experience. The program reviews, compiles, and stores reliability data voluntarily submitted by the participants. Figure 4.3 illustrates the input report forms, which cover both failure rates and supplementary information. Within the program the data are structured according to parts classifications and various factors pertaining to the failures, for example, application stress factors. The output is presented in several forms:

BACKGROUND INFORMATION ON FAILURE RATE DATA - FARADA PROGRAM
11ND FMSAEG-6800 9 (10-64)

TO SUPPORT "TABULAR FAILURE RATE DATA SUMMARY"

ACTIVITY	REPORT NUMBER OR IDENTIFICATION	DATE OF REPORT
ACME Company	ABC-123	4-21-68

I. DESCRIPTION OF EQUIPMENT(S) TESTED OR UNDER SURVEILLANCE

A. DESCRIPTION SYSTEM TYPE INTENDED FUNCTION

AN/FSQ-7- Large high speed digital computer for use in real-time air defense problems

B. PRODUCTION STATUS (Production, Prototype, breadboard)

Prototype

C. AGE OF EQUIPMENT (s) PRIOR TO COMMENCEMENT OF TEST OR SURVEILLANCE

2 years

D. VINTAGE OF EQUIPMENT (Year of operational status)

1967

II. CONDITION OF TEST (or surveillance)

A. DATE AND DURATION

15 October 1967 through 31 December 1967

B. ENVIRONMENT (ground, airborne, laboratory, normal field operations, accelerated life, etc. complete word description including geographical location)

Equipment housed in special environmentally controlled building at a classified location.

C. MAINTENANCE (routine replace and repair, preventative, etc.)

Some preventative maintenance in addition to routine replace and repair

III. SYSTEM STATISTICS

A. TOTAL SYSTEMS (number of equipments)

1 Computer

B. TOTAL OPERATING TIME AND TIME BASE (flight hours, heater hours, equipment hours)

8500 hours of equipment operation

C. SYSTEM MEAN TIME, TOTAL NUMBER OF FAILURES

842 Catastrophic failures
Approximately 10 hours MTBF

IV. FAILURE REPORTING SYSTEM

A. CONTROLLED OR UNCONTROLLED, METHOD OF REPORTING, PERSONNEL

Controlled; laboratory failure reports and equipment removal tags under the immediate surveillance of professional personnel

B. DEFINITION OF FAILURE

Significant removal rate - defined as the total removals minus accidental damage removals, removals due to failure of another component overload, and "no-defect-found" removals

C. ESTIMATED PERCENT OF TOTAL FAILURES REPORTED

95 to 100%

Fig. 4.3. Sample of completed "background information on failure rate data" form.

V. PART FAILURE MODES (for each part type, list failure modes and number of parts failing in each mode)

PART IDENTIFICATION	FAILURE MODE	NO. OF FAILURES
Semiconductor, Diodes	Open	141
" "	Shorted	87
" "	Back Resistance Under Lower Limit	22
" "	Unstable	5
" "	Total	255
Power Transistor, Silicon	Open	7

VI. PART FAILURE TIMES (list exact failure times for each failed part, where possible)

PART IDENTIFICATION	OPERATING TIME	NO. OF FAILURES
Capacitor, Ceramic	7255 hours	1
Semiconductor, Diode, Germanium	825 hours	1
Power Transistor, Silicon	2000-2500 hours	3
" " "	4500-6000 hours	2
Resistor, Carbon Composition	7500-8500 hours	1

VII. SPECIAL ENVIRONMENTAL CONDITIONS (list all environments not given on "Table for Failure Rate Data Summary")

Power surges to the AN/FSQ-7 occurred approximately 4 times per week because of the relative instability of the on-site power generators. These surges were as high as 130 percent of nominal.

VIII. ADDITIONAL INFORMATION (continue on additional sheets as required)

These data are a composite of two separate efforts of succeeding time periods (References a and b, respectively). The two groups of data were integrated into this single report since they describe the same equipment and the component failure rates were very similar.

IX. REFERENCES

(a) Doe, J.C., "A Preliminary Reliability Analysis of the AN/FSQ-7 Computer," Proceedings of the 12th National Symposium on Reliability and Quality Control, pp 372-380

(b) Mann, I.J., "The AN/FSQ-7, A Reliability Progress Report," Proceedings of the 17th RETMA Symposium of Applied Reliability, pp 75-82

11ND-FMSAEC 8300-9 (10-64) (BACK)

Fig. 4.3. (Cont.)

(1) permanent volumes summarizing earlier data, (2) loose-leaf handbooks of current data, frequently updated, and (3) computer magnetic tapes that are updated quarterly. Typical data output is shown in Figs. 4.4 and 4.5. Table A of Fig. 4.4 describes a series of statistical samplings, some evidently of adequate size and others not, and identifies a source report for each. The latter are kept available in original form to furnish detailed qualifying information. It is not attempted to develop generic failure rates for classes of equipment by combining data samples; however, some results of this nature developed by participants are available in the output. The FARADA program represents a significant departure from the earlier programs in several aspects: (1) it is comprehensive with regard to scope of equipment covered; (2) it addresses general rather than specific information needs, that is, there are no specific problem objectives; (3) it is "passive" in the sense that no information sources are sponsored or developed; and (4) it has no reliability service function, that is, the stored information is not combined or interpreted with regard to application problems. Reference 75 further outlines the program and provides details of its content.

4.4.1.5 Interservice Data Exchange Program (IDEP).[116] The principal purpose of the IDEP has been, since 1969, ". . . to provide automatic interchange of test data on parts, components, and materials among U.S. government contractors and agencies, thereby reducing duplicate expenditures for parts testing and improving system reliability."* Many of the FARADA participants also belong to the IDEP, and there is also support from the Canadian Military Electronics Standards Agency (CAMESA). Much of the management and headquarters facilities are shared with FARADA. The main program emphasis is on formal test, development, and technical analysis reports, which are distributed by microfilm on a current basis to the participants. Corresponding with the headquarters staff are program officers in each participating organization to whom material is sent to be distributed to interested individuals. Several important subsidiary activities have been incorporated, including arrangements to alert

*Foreword to Ref. 77.

TYPICAL PAGE OF FARADA COMPUTER PRINT-OUT, TABLE A

PAGE: 2.86

FMSAEG-CORONA,CALIF. TRI-SERVICE AND NASA FAILURE RATE DATA PROGRAM SEPTEMBER 1, 1968
TABLE-A-ELECTRICAL ELECTRONIC COMPONENT PART FAILURE RATE DATA

CROSS INDEX NO.	PARTS/COMPONENTS	SOURCE	OBSERVED ENVIRONMENT/INTENDED APPLICATION	REPORT DATE MO-YR	FAILURE RATE-FAILURES PER MILLION OPERATING HOURS	PARTS HOURS IN MILLIONS	NUMBER OF FAILURES	COMPONENT PART POPULATION
2290S	.AUXILIARY-COMPARTMENT	240	AIRCRAFT	06-66	153	.01306	2	86
2291M	.NOSE-28VDC	215	HELICOPTER	02-65	117	.06	7	240
	.RAMP-LOADING-INTERIOR	250	AIRCRAFT	06-66X	146	.08226	12	152
	.RAMP-LOADING-INTERIOR	227	AIRCRAFT	12-65X	283	.04944	14	96
	.REO-INTERIOR	228	AIRCRAFT	03-65X	28.4	1.3712	39	5676
	FREQUENCY-MULTIPLIERS							
2292S	.	231	SIM/AIRCRAFT	01-66	36.1	.0277	1	219
2293S	.	281	SHIPBOARD	07-66	20.63			
	FREQUENCY-SENSORS							
2294S	.	338B	LAB/AIRBORNE	04-68	2941(LT)	.00034	0	1
	FREQUENCY-TRACKERS							
	AN/APN-147.	227	AIRCRAFT	12-65X	4571	.02472	113	48
2295S	AN/APN-147.	250	AIRCRAFT	06-66X	5373	.04113	221	76
2296S	CV-1181/APN-147.DOPPLER-RADAR	292	AIRCRAFT	03-67	455	.12035	548	88
	FUSEHOLDERS							
	.	246A	SHIPBOARD(SUB)	08-65	5.1	.19608	1	1620
2297S	.	231	SIM/AIRCRAFT	01-66	18.05(LT)	.0554	0	438
	.ELECTRICAL-POWER-SYS	292	AIRCRAFT	03-67	8.31(LT)	.12035	0	88
	.ELECTRICAL-POWER-SYS	227	AIRCRAFT	12-65X	40.5(LT)	.02472	0	48
	.ELECTRICAL-POWER-SYS	250	AIRCRAFT	06-66X	24.3(LT)	.04113	0	76
2298	.PANEL-MOUNT-BAYONET-KNOB-3AG	288	LAB	05-67	15.2	.132	2	30
	.POST-TYPE	210	GROUND	08-64	.082	72	6	9446
2309S	.	302K	LAB	04-67	.21(LT)(8)	4.6752	0	
	.CLUTTER	295	SHIPBOARD	05-67	55.268	.2895	16	52
2310S	.CLUTTER-SEARCH-RADAR	256	AIRBORNE	07-66	2245	.00267	6	36
2311S	.DIODE-READ-MEMORY-COMPUTER	256	AIRBORNE	07-66	2619	.00267	7	36
	.PROGRAMMER	295	SHIPBOARD	05-67	177.32	.43425	77	78
	GENERATORS							
	.	339	AIRCRAFT	05-68	612	.02125	13	78
	.2-1/2KVA-EMERGENCY-POWER-SYS	292	AIRCRAFT	03-67	16.6	.12035	2	88
	.2-1/2KVA-EMERGENCY-POWER-SYS	250	AIRCRAFT	06-66X	48.6	.04113	2	76
	.2-1/2KVA-EMERGENCY-POWER-SYS	227	AIRCRAFT	12-65X	81	.02472	2	48
2312S	.40KVA-APU-DRIVEN-AC-POWER-SOURCE	292	AIRCRAFT	03-67	74.8	.12035	9	88
2313S	.40KVA-ENGINE-DRIVEN-AC-POWER-SOURCE	292	AIRCRAFT	03-67	260	.4814	125	352

TYPICAL PAGE OF FARADA COMPUTER PRINT-OUT, TABLE A1

PAGE: 2.252

FMSAEG-CORONA,CALIF. TRI-SERVICE AND NASA FAILURE RATE DATA PROGRAM SEPTEMBER 1, 1968
TABLE-A1-SUPPLEMENTARY PART IDENTIFICATION AND STRESS LEVEL INFORMATION FOR TABLE A

CROSS INDEX NO.	--VENDOR--	VENDOR PART NO. / MIL STD PART NO. / FEDERAL STOCK NO	--PERCENT OF RATED-- VOLTAGE	CURRENT	POWER	FREQUENCY	PRESSURE	TEMPERATURE CENTIGRADE TYPICAL	HIGH	LOW	VIBRATION--MECHANICAL--SINUSOIDAL-- FREQUENCY CPS	INTENSITY G/RMSG	RANDOM GXG/CPS	ACOUSTIC OM DB	ACOUSTIC L DB	MAX INTENSITY G	DURATION SEC	SHOCK--BLOWS PER MIN	TYPICAL PSI	PRESSURE-- TYPICAL PSIA	RANGE PSIA	RELATIVE-HUMIDITY PERCENT TYPICAL	RANGE	RADIATION ABS TYPE ORB RAD 10
2280								45											15			85		
2281								60																
2282	ERIE TECH							25											15					
2283	RF-INTER							25											15					
2284				70				40																
2285									35	-60	25	1.41												
2286								50																
2289		6111-3																						
2290	GRIMES-MFG																							
2292									55	-54	25	.7												
2293									40	18														
2294									35	-60	25	1.41												
2295		5841 859-3483																						
2296	CA-MARCONI	3323-800																						
2297									55	-54	25	.7												
2298	LITTELFUSE	342001A	50	100		98																50		
2299									55	-54	25	.7												
2300		F03G3R00A																						
2301		F03A250V3A																						
2302					10				55	50	20	2												
2303									35	-60	25	1.41												
2304		5920-235-8373																						
2305		5920-235-8373																						
2306	BUSSMAN	AGC-TYPE	50	75	36	98		24														50		
2307				10																				
2308	BUSSMAN	MDX-7	96	99	96	98		24														50		
2309								22	43	-7									15			90	20-100	
2310	HUGHES	464082																						
2311	HUGHES	464657																						
2312		A115-772-3552																						

Fig. 4.4. Typical page of farada computer print-out, table A.

TYPICAL PAGE OF FARADA COMPUTER PRINT-OUT, TABLE B

PAGE: 2.466

FMSAEG-CORONA,CALIF. TRI-SERVICE AND NASA FAILURE RATE DATA PROGRAM SEPTEMBER 1, 1968

TABLE-B-MECHANICAL HYDRAULIC PNEUMATIC PYROTECHNIC MISC. COMPONENT PART FAILURE RATE DATA

CROSS INDEX NO.	PARTS/COMPONENTS	SOURCE	OBSERVED ENVIRONMENT/INTENDED APPLICATION	REPORT DATE MO-YR	FAILURE RATE-FAILURES PER MILLION OPERATING HOURS	PARTS HOURS IN MILLIONS	NUMBER OF FAILURES	COMPONENT PART POPULATION
	TIMERS,STOP							
7656	.TIME-INTERVAL-120V-60CPS	288	LAB	05-67	45.4	.044	2	10
	TIMING-MOVEMENTS,MECHANICAL							
7657S	.655FC	220	MISS,SIM/MIS	05-65	5160(LT)	.00019	0	387
	TIPS							
	.6-SENSING-PRESSURE,AIR-FUEL-CONTROL	201	AIRCRAFT	08-65	10.6(N)	.37914	4	400
7658S	.NOSE-CAP-ELEVATOR-CONTROL-SYS	292	AIRCRAFT	03-67	4.15(LT)	.2407	0	176
	TIPS,AILERON							
	.	292	AIRCRAFT	03-67	4.15(LT)	.2407	0	176
	.	250	AIRCRAFT	06-66X	12.2(LT)	.08226	0	152
	.	227	AIRCRAFT	12-65X	20.2(LT)	.04944	0	96
	TIPS,ELEVATOR							
	.	227	AIRCRAFT	12-65X	20.2(LT)	.04944	0	96
7659S	.	250	AIRCRAFT	06-66X	12.2(LT)	.08226	0	152
7650S	.	292	AIRCRAFT	03-67	4.15(LT)	.2407	0	176
	.NOSE-CAP-ELEVATOR-CONTROL-SYS	227	AIRCRAFT	12-65X	20.2(LT)	.04944	0	96
7661S	.NOSE-CAP-ELEVATOR-CONTROL-SYS	250	AIRCRAFT	06-66X	12.2(LT)	.08226	0	152

	.MAIN-LANDING-GEAR	227	AIRCRAFT	12-65X	7767	.04944	384	96
	.MAIN-LANDING-GEAR	266B	AIRCRAFT	04-64	8796	1.677	9473	848
	.MAIN-LANDING-GEAR	226	AIRCRAFT	03-65X	36000	.22854	8223	946
7669M	.MAIN-LANDING-GEAR	225.	AIRCRAFT	03-66	15580	.017	260	64
7670S	.MAIN-LANDING-GEAR	250	AIRCRAFT	06-66X	3881	.329	1277	608
7671S	.MAIN-LANDING-GEAR	292	AIRCRAFT	03-67	3484.6	.9628	3355	704
	.NOSE-LANDING-GEAR	313	AIRCRAFT	06-67	4260	.298816	1273	724
7672S	.NOSE-LANDING-GEAR	292	AIRCRAFT	03-67	5006	.2407	1205	176
	.NOSE-LANDING-GEAR	22K	AIRCRAFT	03-65X	3730	.11427	426	473
7673M	.NOSE-LANDING-GEAR	225	AIRCRAFT	03-66	6112	.017	102	64
7674S	.NOSE-LANDING-GEAR	250	AIRCRAFT	06-66X	5458	.08226	449	152
	TORSION-BARS							
	.SUSPENSION-WHEEL	255	GROUND	04-66	4.86(MILES)	.6186M	3	150
	TORSION-BARS,HINGE							
7675	.HATCH-DRIVER	291	GROUND	07-66	5.543	1.804M	10	494
	TORUS-ASSYS							

TYPICAL PAGE OF FARADA COMPUTER PRINT-OUT, TABLE B1

PAGE: 2.528

FMSAEG-CORONA,CALIF. TRI-SERVICE AND NASA FAILURE RATE DATA PROGRAM SEPTEMBER 1, 1968

TABLE-B1-SUPPLEMENTARY PART IDENTIFICATION AND STRESS LEVEL INFORMATION FOR TABLE B

CROSS INDEX NO.	--VENDOR--	VENDOR PART NO. / MIL STD PART NO. / FEDERAL STOCK NO	--PERCENT OF RATED-- VOLTAGE	CURRENT	POWER	FREQUENCY	PRESSURE	TEMPERATURE CENTIGRADE TYPICAL	HIGH	LOW	VIBRATION MECHANICAL SINUSOIDAL FREQUENCY CPS	INTENSITY RMSG	RANDOM GXG/CPS	ACOUSTICAL DB	SHOCK MAX INTENSITY G	DURATION SEC	BLOWS PER HOUR	PRESSURE TYPICAL PSIA	RANGE PSIA	RELATIVE HUMIDITY PERCENT TYPICAL	RANGE	RADIATION ABSORBED TYPICAL RAD	TYPE
7649								22	27	16								15		60	55-65		
7650		1.20-760 0572																					
765.		6645-752-8185																					
7652								22	71	-54								15		60	5-100		
7653					90																		
7654								22	71	-54								15		60	5-100		
7655		6645-785 8834																					
7656	HAYDON-AW	F071.001	92			98		24												50			
7657								41	65	-37	10-2K	3.5	.05		100	6			.02-15		0-95		
7658		1560-011-1258																					
7659		1560-011-1257																					
7660		1560-011-1257																					
7661		.560-011-.256																					
7662	GOODRICH	VII																					
7663	GOODYEA																						
7664	GOODRICH																						

7718	M-HONEYWEL	FG56G14																					
7719		MS-24550																					
7720	COURTER-EL																						
7723	COURTER-EL																						
7730		6620-044-6034																					
7733		6230-676-.604																					
7734		6230-676-2604																					
7735	BENDIX																						
7736	MICRO-SYS	.004-0 29/3.	87	87			100	21	77	SRI	10-2K		.025	3						95	90-100		
7737		6685-781 .865																					
7738		6685-781-.865																					
7740	MICRO-SYS	.004-2031/3.	87	87			100	21	77	SRI	10-2K		.025	3						95	90-100		
7741		6620 044 6034																					
7742	AIRESEARCH	510962-2-1																					
7743	BENDIX	7609-37-M5-.																					

Fig. 4.4. (Cont.)

SAMPLE OF COMPLETED "TABULAR FAILURE RATE DATA SUMMARY" FORM

TABULAR FAILURE RATE DATA SUMMARY - FARADA PROGRAM

ACME Company — ABC-123 — 4-21-68

PART COMPONENT COMPLETE NOMENCLATURE	VENDOR AND VENDOR PART NO. MIL STD PART NO. OR FEDERAL STOCK NUMBER	OBSERVATION ENVIRONMENT	INTENDED INSTALLATION (FOR USE ENVIRONMENT)	PARTS X HOURS IN MILLIONS	NUMBER OF FAILURES	FAILURE RATE	PART COMPONENT POPULATION	VOLTAGE	CURRENT	POWER	FREQUENCY	PRESSURE	TEMPERATURE TYPICAL	TEMPERATURE MAX	TEMPERATURE MIN	VIBRATION MECHANICAL	VIBRATION ENVIRONMENT	VIBRATION ACOUSTIC	SHOCK	PRESSURE TYPICAL	PRESSURE RANGE	RELATIVE HUMIDITY TYPICAL	RELATIVE HUMIDITY RANGE	RADIATION	REFERENCE
COILS, TUBE-FOCUSING, VA828B/C KLYSTRON-BEAM	VARIAN 5950-473-5254	SHIPBOARD	SHIPBOARD	.00438	6	640	40						22	29	16					15		60	55-65		
TRANSISTORS, 2N2364 SILICON-NPN-LOW POWER-SWITCHING	PHILCO	LAB	MISSILE	10.57	3	.284	2700		10					86	60							50			
CYLINDER, ACTUATING, LINEAR, OIL-NOZZLE	NATIONAL WATERUPT 1125-0-7	AIRCRAFT	AIRCRAFT	1.896	14	10.03	325				60	21	41	4											

NOTE: (a) The following readings are used for radiation type

NUCLEAR: A Fast, B Slow, C Thermal

ELECTROMAGNETIC: D Gamma, E X Ray

CHARGED PARTICLES: F Proton, G Electron, H Miscellaneous

SAMPLE OF COMPLETED "FAILURE MODE DISTRIBUTIONS" FORM

TABULAR FAILURE MODE DATA SUMMARY - FARADA PROGRAM

ACME Company — ABC-123 — 4-21-68

PART COMPONENT COMPLETE NOMENCLATURE	VENDOR AND VENDOR PART NO. MIL STD PART NO. OR FEDERAL STOCK NUMBER	OBSERVATION ENVIRONMENT	INTENDED INSTALLATION (FOR USE ENVIRONMENT)	SHORTED	OPEN	INTERMITTENT	BURNED OUT	LEAKING	BENT	CRACKED	REGULATION IMPROPER	INOPERATIVE	BYPASSING	UNKNOWN
COILS, TUBE-FOCUSING, VA828B/C KLYSTRON-BEAM	VARIAN 5950-473-5254	SHIPBOARD	SHIPBOARD	4	1	1								
TRANSISTORS, 2N2364, SILICON-NPN-LOW-POWER-SWITCHING	PHILCO	LAB	MISSILE	2		1								
CYLINDER, ACTUATING, LINEAR, OIL-NOZZLE	NATIONAL WATERUPT 1125-0-7	AIRCRAFT	AIRCRAFT					6	4	2				2

Fig. 4.5. Sample of completed "tabular failure rate data summary" form.

the participants to difficulties experienced with specific items of equipment,[80] to apprise them of test programs in progress, and to standardize test equipment calibration procedures.[81] Some 20,000 reports covering 30,000 separate items are currently available on microfilm through simplified retrieval indexing procedures. There is no particular intent to evaluate or edit the data as received. Additional program details are described in Refs. 76 to 79.

4.4.2 Reactor Component Data Programs

Although the USAEC does not participate directly in the FARADA or IDEP programs, many of their contractors and the reactor equipment manufacturers do, by virtue of also being contractors to the armed services. The AEC has, however, recognized the need for components reliability data and has sponsored efforts aimed toward fulfilling these needs. On the project level is the Savannah River Probabilistic Analysis of Risk (PAR) Program, which collects data to monitor the plant operation and design adequacy.[117] Broader scope approaches are represented by the program at the Liquid Metals Engineering Center (LMEC) and by the Holmes and Narver, Inc., studies.

4.4.2.1 Liquid Metal Engineering Center.[118] The LMEC is operated for the USAEC by the Atomics International Division of North American Rockwell Corporation. In 1968, partly as an extension of their existing Maintenance and Malfunction Analysis Program, they were commissioned to develop a reliability information system to deal primarily with the mechanical equipment typical of liquid metals test facilities and reactors. The program was, however, intentionally organized for future expansion to cover general reactor components. Its main emphasis was on developing data sources and information handling methods to meet the needs of system reliability analysis; in addition, attempts were made to identify special application problems methodically. Initial program phases included a review of accumulated records for many liquid metals systems, from test loops up through the Fermi reactor, and the development of an in-house incident, malfunction, and problem report procedure. Program functions include storage of source material on microfilm; appropriate data are

extracted and evaluated by engineers, and the processed information is then classified and indexed as shown in Vol. II of Ref. 68.

Processed data is stored in computer memory, with which is associated an IBM 360 program for sorting, retrieval, and automatic plotting. Much of the collected material is essentially qualitative, reflecting the lack of quantitative experience with many of the component forms. Of the statistical data, most concerns the classification of failure modes. This information, along with a number of case history summaries, is presented in Vol. I of the principal program document.[68] Volume I also includes a great deal of well organized basic information on reliability theory and evaluation techniques, along with an extensive bibliography. Volume II details the identification categories used for storage and retrieval of information. Typical data summaries from the handbook are illustrated in Figs. 4.6 and 4.7. The program achieved the level of a well-advanced pilot effort before being mothballed in 1970. Reference 67 briefly reviews the program development and organization.

4.4.2.2 Holmes and Narver, Inc. Prominent among the studies that have given substance to the present concepts of reactor component reliability information systems is the series conducted for the USAEC by H&N. These efforts have addressed the broad question: What does operating experience tell us about the safety of nuclear reactors? Between 1961 and 1966 separate investigations were made of groups of test, research, and power reactors. All manner of design, test, operating, and maintenance records were reviewed, and from this material it was attempted to draw fairly broad conclusions. Most of the reliability data developed concerned the performance of vital systems and subsystems, since components were not the prime concern. It was acknowledged in the report on power reactors[96] that the data were insufficient to be of much statistical significance. References 94 and 95 describe the other investigations.

The experience gained in these studies led H&N in 1967 to propose a comprehensive program for monitoring the reliability of reactor safeguards. A key part of the program was to be an elaborate system for collecting and managing the reliability information. One specific aim of this system was to support the quantitative reliability analysis methods that were being proposed at the same time; these are described in

TABLE 1-114

FAILURE DATA FOR TRAPS (GENERAL)

(Sheet 11 of 12)

ITEM	1. COMPONENT/PART 2. SYSTEM/SUBSYSTEM 3. CODE: (Component) (System/Subsystem)	1. FACILITY 2. COMPONENT LOCATION 3. OPERATING CONDITIONS 4. SOURCE DOCUMENT	FAILURE INDEX CODE*			OPERATING HOURS	METHOD OF FAILURE DETECTION	1. FAILURE DESCRIPTION 2. CORRECTIVE ACTION 3. RECOMMENDATIONS
			CAUSE	MODE	EFFECT			
54	1. Traps/Wire Mesh 2. Heat Transfer/Driers and Traps 3. 33 224640	1. EBR-II 2. Primary/fission gas monitor 3. - 4. PMMR-57	MI 218	MI 51	MI 530	4400	Operational monitors	1. Vapor trap plugged with sodium. 2. Local repair; unit was heated and sodium drained. 3. If space permits, increase size of trap for longer service.
55	1. Traps/Wire Mesh 2. Heat Transfer/Driers and Traps 3. 33 224640	1. EBR-II 2. Primary/argon purification 3. - 4. PMMR-108	MI 218	MI 51	MI 530	11,320	Operational monitors	1. Wire mesh plugged. 2. Part replaced. 3. None.
56	1. Traps/Wire Mesh 2. Nuclear Fuel Handling and Storage Equipment /Cooling 3. 33 235140	1. EBR-II 2. Fuel handling machine 3. - 4. PMMR-102	MI 218	MI 51	MI 530	475	Operational monitors	1. Vapor trap plugged. 2. Part replaced. 3. None.
57	1. Traps/Wire Mesh 2. Nuclear Fuel Handling and Storage Equipment /Cooling 3. 33 235140	1. EBR-II 2. Fuel handling machine 3. - 4. Operation weekly report, 11/67	MI 500	MI BZ	MI 530	2156	Operational monitors	1. Vapor trap plugged. 2. Trap replaced. 3. None.
58	1. Traps/Adjusting Shaft 2. Steam, Condensate and Feedwater Piping and Equipment/Main Steam 3. 33 281000	1. EBR-II 2. Main steam (trap PVT-5) 3. - 4. PMMR-4	MI 500	MI 59	MI 530	1200	Repair of primary failure	1. Adjusting shaft broken. 2. Part replaced. 3. Determine cause of failure and confer with manufacturer before replacing part. Redesign of part may be necessary.
59	1. Traps/Gasket 2. Steam, Condensate and Feedwater Piping and Equipment/Main Steam 3. 33 281000	1. EBR-II 2. Main steam (trap PVT-5) 3. - 4. PMMR-4	MI 500	MI BZ	MI 530	1200	Direct observation	1. Gasket worn out. 2. Part replaced. 3. Determine cause of failure and confer with manufacturer before replacing part. Redesign of part may be necessary.

* I = INCIDENT MI = MINOR MALFUNCTION
MA = MAJOR MALFUNCTION P = PROBLEM

Fig. 4.6. LMEC failure data.

TABLE 1-115

FAILURE DISTRIBUTION FUNCTIONS

COMPONENT TRAPS (GENERAL)

COMPONENT SUBTYPE SODIUM FREEZE TRAPS

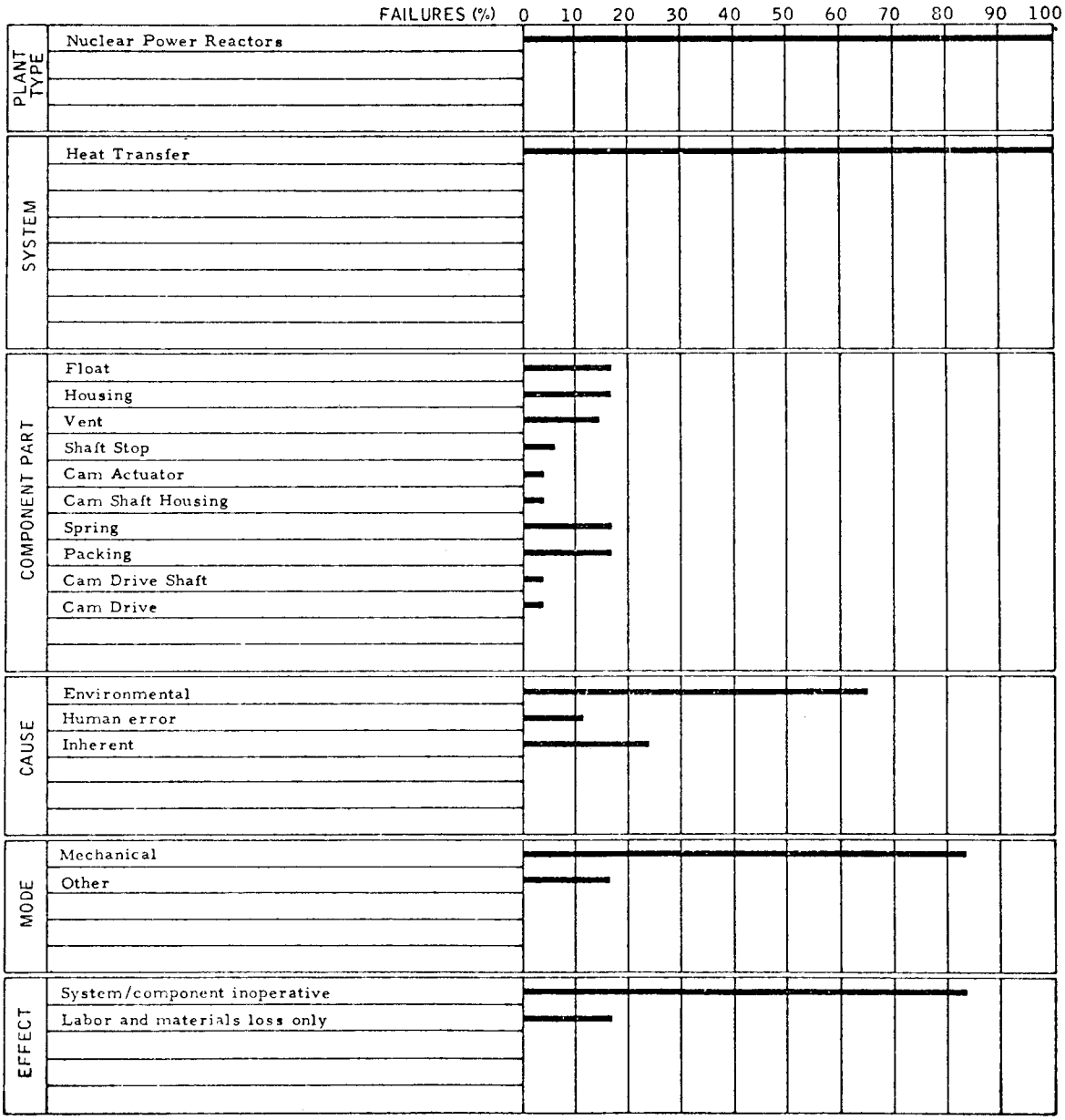


Fig. 4.7. LMEC failure data.

Chapter 3. Accordingly, desirable features from the IDEP, FARADA, and other programs were combined, with emphasis on ability to group information selectively for statistical studies of failure rates, repair intervals, etc. Reference 20 describes the overall proposal, and Ref. 21 expands on the methodology.

Pilot efforts to collect operating data according to the above proposed methods were initiated with AEC support by H&N for the Connecticut Yankee reactor power plant. The data collection has since been continued independently by the plant operator. In addition, a great deal of background engineering information was assembled for the components of interest; this work is summarized in Ref. 69.

4.4.2.3 Proposals for Cooperative Program. The USAEC has encouraged private industry, both manufacturers and operators of reactor power plants, to develop a cooperative arrangement for collecting and evaluating reliability data.[119] Such a program has recently been initiated[85] through the Edison Electric Institute (EEI). The EEI presently collects and publishes[84] statistics on major equipment outages of power utilities and has the necessary wide industry contacts.

4.4.2.4 General Electric Company. Prominent in the private sector is the data collection effort of the General Electric Company in support of their own analyses of reactor systems.[120] General Electric looked first to the established information programs, for example, FARADA, to obtain components data. Insufficient, inconsistent, or no data were found for many important classes of reactor equipment, particularly for new designs or novel applications. Alternative approaches were then explored. Within their own organization were found a great deal of relevant test, development, and field experience records from which could be derived good preliminary reliability estimates for many forms of equipment. Some of the specific device estimates were synthesized effectively from related or basic data by groups of specialists. The need to justify or confirm such estimates for certain critical applications is recognized, and in some cases special tests have been conducted. An example of these tests, essentially qualitative in nature, is a series on main steam line isolation valves.[82] General Electric has also carried out components

reliability test programs directly for the USAEC, notably investigations of piping stress effects.[83] Their efforts strongly emphasize the selection and interpretation of data by engineers, as opposed to uncritical direct use of it.

4.4.2.5 UKAEA. Probably the largest-scale data program on reactor components reliability presently operating is that of the United Kingdom Atomic Energy Authority (UKAEA); this program is an integral part of a unified plant reliability effort. Reference 103, in 1967, described the then proposed UKAEA data store to meet the requirements for reliability analysis of the British reactors. Both the analysis program and the data bank have since been established, as the "Systems Reliability Service"[102] and the "Syrel,"[106] respectively, and have recently begun to offer their services on a subscription basis to general industry as well as for the safety assessment of UKAEA reactors. The components information program employs an elaborate classification and coding scheme for elementary data patterned after the FARADA system; it also can store and index many forms of "engineering information," some of which corresponds to that handled by IDEP. Overall, the program appears better integrated with its data sources than FARADA or IDEP, resembling more the LMEC effort but on a larger scale. Equipment service data for reactors comes largely from the well-established Authority Health and Safety Branch (AHSB) fault and incident reporting system described in Ref. 104. The capabilities to review input data and to assemble and interpret information relevant to specific application problems have been incorporated in the system; Fig. 4.8 is a flowsheet describing how such information is developed. Reference 105 describes an approach to evaluating component reliability from parts and engineering information.

4.4.3 Status of Reliability Data Effort

The present consensus is that the established reliability data programs are still not meeting the current needs, either for analysis of reactor system designs or for monitoring operation of existing systems. Moreover, there is no clear agreement regarding the optimum scope of a data management effort nor, in the U.S., on how it should be undertaken. But

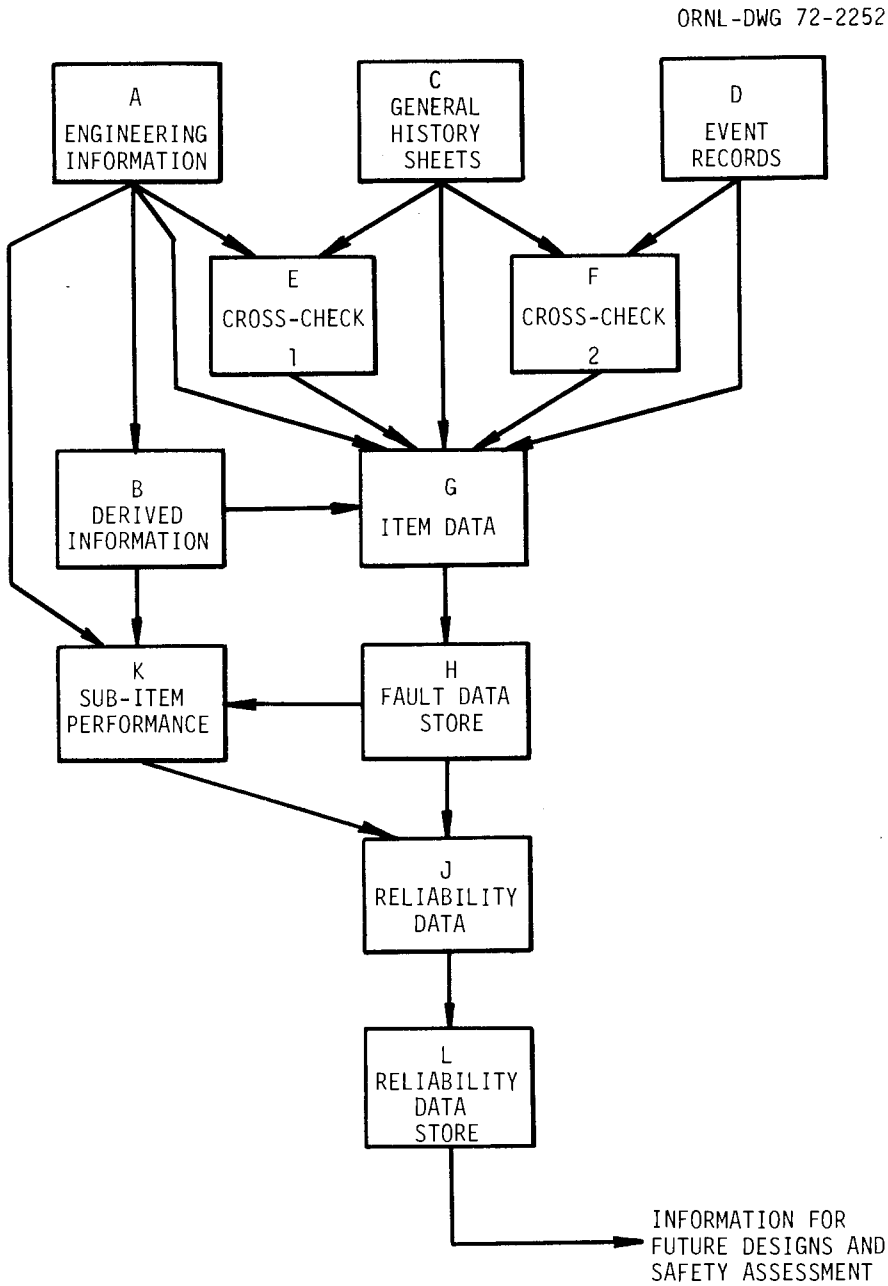


Fig. 4.8. Reliability data flow diagram — UKAEA.

experience and informed opinion have brought into focus at least the major objectives and functions of a reactor reliability data program. The salient aspects appear to be as follows:

1. The program should be sufficiently broad to cover the equipment comprising all systems of interest; the latter will include many important operating systems as well as those formally designated as protective systems.

2. There should be facilities for acquiring, storing, and making readily available a variety of information, for example, test and development reports, failure statistics, deficiency reports that convey significant information, quality control data, etc.

3. The program should provide the functions of a reliability service. These include rational efforts to overcome deficiencies in data as seen by the systems analysts, editing of input data and culling of irregularities, and assembly and interpretation of the stored information consistent with specific reliability problems. Griffin, of the LMEC, points out that event data must be analyzed by highly qualified engineers who are familiar with the application problems, noting that there is a tendency to relegate the task to technicians or reliability specialists.[118]

4. There should be central capability to monitor reactor industry (or segments thereof) operating effectiveness, providing rapid response to safety-reliability problems of more than immediate plant interest; this function might begin with the local plant operating records.

In the matter of organizing a comprehensive information system, one of the major problems is in classifying data for storage and retrieval. The complexities of this task are discussed at length in Ref. 8, and detailed recommendations for a reactor data program are presented in Refs. 20, 68, and 103. Reference 63 brings out some of the basic difficulties and limitations inherent to statistical summaries, in particular, the losses and distortions of information that are likely to occur. Other practical problems arise from data reporting practices.

Concern has been expressed over the thinness of the information base represented by the operating power reactors, which have not yet accumulated much experience. Reference 63 suggests that the base may readily be broadened by admitting the general industry or utility experience with

many common components, for which application in reactor plants is entirely conventional. The article cautions that there will still be data deficiencies due both to overall lack of experience with novel component applications and to the tendency for operating experience to represent obsolete equipment. Another area requiring special consideration is the definition of unusual stresses or environment to which certain components will be subjected, for example, components in the core or containment volumes.

Reference 19 addresses similar information problems in the aerospace industry. This source suggests a number of features that a "universal parts data bank" should have and estimates that such a program for aerospace might cost more than $20,000,000 per year.

5. RELIABILITY IMPLEMENTATION FOR REACTOR SYSTEMS

Reliability practice on a large scale involves such a wide range of technical considerations that formal organization of efforts becomes necessary to assure that all are dealt with effectively. Early attempts to create reliable safety systems, while proceeding from the same general concepts, were not at all consistent in method, emphasis, or results. The experience, however, did reveal common problem areas amenable to general solutions which could be expressed via criteria, guidance, and administrative procedures. These areas have since benefited from continual attention by various organizations concerned, notably the development and regulatory branches of the USAEC and the professional societies.

5.1 System Design for Reliability

It was recounted briefly in Chapter 1 how the present design principles for protection systems had evolved from practice, drawing liberally on reliability theory. These principles mainly express reliability requirements in terms of specific system arrangements and features. As the basis for current design acceptability, they are closely observed by the organizations developing reactor plants as well as by the USAEC licensing agencies.

5.1.1 System Design Criteria[92,93]

By 1965, considerable interest had developed in codifying the design principles. Substantial efforts were then under way by the USAEC, the Institute of Electrical and Electronics Engineers, and the International Electrotechnical Commission to reduce to criteria the design philosophy as well as desired system features.

The protection systems work, although but one phase of the overall AEC program for reactor safety, figured prominently in the 70 "General Design Criteria for Nuclear Power Plant Construction Permits" which were tentatively adopted in 1967 as an appendix to 10 CFR 50. A revised set of criteria was substituted in February 1971.[28] In 1968, the "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems"[88] was issued

as IEEE-279; while the document is limited in scope to the protection system instrumentation and controls, it treats that aspect in considerably greater detail than the AEC criteria. The international effort resulted in the 1967 publication of the IEC "General Principles of Nuclear Reactor Instrumentation,"[91] of which Clause 5 presents protection system criteria and Clause 8 treats general alarms, that is, visible and audible signal systems.

Each of the three sets of criteria cited states qualitatively a requirement for high reliability of the protection systems and then further specifies design features to enhance reliability. The language is intentionally broad so as to be applicable to the widest range of reactors and to foster innovative design. However, by being so general, the criteria are often difficult to interpret with regard to specific situations. Typical of such difficulties are those noted in Chapter 2 concerning reliability objectives. Consequently, the main attention is now focused on expanding the protection system criteria in detail and developing application guidelines.

The standards activities of the professional societies are presently being coordinated by the American National Standards Institute (ANSI; formerly USASI or ASA). Responsibility has been given to the American Nuclear Society (ANS) to prepare criteria on formulating the design basis for the individual protection systems; while primarily concerned with fundamental system requirements, these criteria should also include reliability goals. Various IEEE committees are engaged in the continual upgrading of IEEE-279 as well as developing related criteria and guidance material. Their work covers such areas as (1) interpretation of the single failure criterion, particularly with regard to common mode failures; (2) periodic testing; (3) application of reliability analysis methods in system design and operation; (4) operational compliance; and (5) reliable power supplies for vital systems. The last mentioned effort has resulted in the broad "IEEE Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations," IEEE-308.[89]

Supplementing the societies' work is the USAEC-DRDT Standards Program at Oak Ridge National Laboratory. The program seeks to provide a comprehensive set of systems and equipment standards for AEC-sponsored

reactors by adapting or augmenting existing standards where feasible and preparing new ones where none are available. In the matter of systems criteria, the Program has issued the tentative "Supplementary Criteria and Requirements for RDT Reactor Plant Protection Systems," C 16-1T,[90] based largely on IEEE-279 and extending the scope to include protection system final actuator devices. A similar set of criteria are currently in preparation for power supplies, adapting and expanding on IEEE-308.

The RDT protection system criteria acknowledge the probability aspect of reliability to the extent of requiring that quantitative goals for protection "subsystems" be established as a part of the design basis and then satisfied as a general functional requirement.

5.1.2 Literature on Design of Protection Systems

Further guidance in the design of protection systems is given by the SIFTOR report,[35] the LMEC "Failure Data Handbook for Nuclear Power Facilities,"[68] and numerous NSIC reports[36] devoted to specific types of systems. Two of the latter concern protection system instrumentation and control, emphasizing reliability features.[37,38] In addition, the Nuclear Safety Journal publishes timely articles on reliability topics, several of which are referenced in this report.

5.1.3 Design and Review Practice

A substantial portion of the design effort for each individual protection system is devoted to reliability aspects. As discussed in Section 3.9, the formal methods of reliability analysis have had only a limited role in the procedure. However, qualitative analysis techniques appear to be gaining acceptance in matters of demonstrating system single-failure and common-mode failure defense and defense in depth against postulated event sequences.

The practical reliability analysis applications in the design process have been mainly by the reactor manufacturers, AEC contractors, and a few consultant firms oriented to the reactor industry. Although the architect-engineering firms are currently assuming more of the responsibility for the design of reactor power plant safeguard systems, there is little

evidence that they are using the formal analysis methods to any significant extent.

The plant licensing procedure calls for design review by the Advisory Committee on Reactor Safeguards (ACRS) and the Division of Reactor Licensing (DRL). Both of these organizations are very much concerned with reliability of systems, but approach such questions in traditional ways. Their reviews stress design philosophy, conformance to the criteria, specific system features, and general quality of the overall design effort. Partly because of the confusion attending wide variations in analysis execution, introduction of quantitative results in support of license applications has not been encouraged by the regulatory.

5.2 Components Qualification and Quality Control

Chapter 4 described measures for assuring that components are essentially qualified for specific applications and satisfactorily free from defects. To apply such measures effectively for the wide range of elements in a complex system occupies perhaps the main administrative attention in a formal reliability program. Component quality assurance is primarily a responsibility of the reactor builders and operators but also is subject to extensive regulatory review. Moreover, substantial AEC development efforts are directed to quality assurance problems, particularly those concerning equipment qualifications. Components standards and criteria promote state-of-the-art technology to achieve consistent high quality and serviceability.

5.2.1 Quality Assurance in Private Plant Construction

Specific quality assurance requirements and procedures are developed along with the design of each plant and set forth in the technical specifications. The latter are required in support of license applications. In reviewing the applications, the DRL and/or the ACRS may highlight additional items requiring special attention during later phases of a reactor's construction and operation. Some of these will occasion the applicant to devise additional specifications or procedures, which are then also subject to review. All such formal quality assurance documentation

forms part of the basis on which the operating permits are granted and hence is a matter of public record.[39]

The Compliance Division of the AEC monitors manufacturing and construction activities to ensure that the proposed measures are properly executed. Their contribution typically amounts to rigorous quality control through directly supervised inspections and tests and audits of contractors' records.[124]

Unusual problems arising in the course of a reactor's construction or operation are subject to further review by the regulatory, as are the corrective measures proposed. The latter in some cases have involved substantial development programs to qualify a component, construction method, or inspection technique.

5.2.2 AEC "Quality Assurance" Program

Corresponding to the regulatory procedures for private plants is the AEC quality assurance (QA) program for government contractors. The program represents a highly organized administrative control over a broad range of activities, most of which affect reactor safety. Reference 87 describes the program scope and how it pertains to such measures as analysis, qualification, quality control, operating procedures, etc. In practice, each contractor establishes a permanent local quality assurance program and staff. The local QA officers then work with the project organizations to specify the requirements on every project, the procedures by which each shall be satisfied, and the responsibilities for all related activities. Careful documentation, subject to audit both by the local QA officers and by the AEC, is required at all stages.

5.2.3 Standards and Criteria for Components[92,93]

The standards programs of the professional societies and the USAEC-DRDT are actually more involved with reactor components than with the systems criteria described. Various efforts seek to establish the qualifications for critical equipment and to define appropriate quality control measures for components and plant construction. Existing industry and MIL standards are being adapted or upgraded where feasible, for example,

those for piping, pressure vessels, electrical insulation, etc. Entirely new standards are being developed for equipment or applications peculiar to reactors (radiation measuring instruments, containment penetrations, etc.).

An example of the more advanced reliability approach to standards is found in the IEEE effort on electric motors for service in containment enclosures, not yet published. Proposed is a qualification test regime that simulates age effects on electrical insulation and then superimposes the severe heat, moisture, and chemical contamination anticipated for the worst transient service conditions.

5.3 Safety Research

In the overall attempt to minimize performance uncertainties of equipment and systems, many of the problems encountered are not tractable to straightforward engineering and QA methods. Almost all these concern transient conditions under which the safeguard equipment must operate. Consequently, one of the principal safety research objectives is to provide insight regarding what mechanisms in reactor cores could prevent or degrade safeguard functions such as insertion of poison rods, core cooling by flood or spray, and the response of sensors monitoring core conditions. Additional work seeks to define structural stresses and other acceleration force effects resulting from earthquakes, wind loadings due to hurricanes, etc.

5.4 Organization and Training

Few would care either to question or to quantify the importance of attitudes, individual and corporate, in achieving reliability. But constructive attitudes can be cultivated in many ways, notably by education and by organization of responsibilities so that competing objectives do not degrade safety reliability.

The formal aspects of reliability are now being taught widely as a discipline in itself. In addition, the subject is stressed heavily in graduate and extension courses in reactor safety. Typical of the

extension courses directed toward practicing nuclear engineers are those which have been offered by MIT, UCLA, and the NUS Corporation.

The RDT Quality Assurance Program provides for reviews of contractor project activities by organizations independent of the projects themselves. Similarly the Division of Reactor Licensing is promoting the assignment of safety responsibilities for private power reactors to organizations separate from those concerned with production and reporting only to top utility management.

The specific measures used by individual reactor operators and builders to motivate their personnel is not discussed in the literature. But it is interesting to speculate on the extent that such incentives may have contributed to other complex endeavors, for example, to that ultimate exercise in reliability, the moon landings.

5.5 Reliability in Operation, Maintenance, and System Modifications

Chapters 3 and 4 cited various ways in which reliability depends on correct operating practices and on intelligent observations of the equipment performance or condition. To a large extent, the necessary actions can be reduced to formal procedures. Such procedures are included in the set of technical specifications for each reactor, referred to in Section 5.2.1, and are subject to review for initial reactor licensing. The Compliance Division monitors subsequent operation of private reactors to establish that the procedures are being observed, and branches of the Division of Reactor Licensing review the operating data continually in search of irregularities. Similarly, the Division of Operational Safety monitors the operation of AEC-sponsored reactors.

Either the plant operator or the AEC may initiate plant modifications, for reasons of revealed deficiencies as well as desired performance benefits. Such changes are accorded the same QA reviews as a new plant.

The protection system criteria, notably IEEE-279 (Ref. 88) and RDT C 16-1T (Ref. 90), acknowledge that a significant way to enhance reliability is by minimizing opportunities for procedural errors. Accordingly,

they call for special facilities to assure that portions of a system are properly restored to service after outages for testing or maintenance. Moreover, they specify that test facilities shall not compromise channel independence.

6. TOWARD A UNIFIED RELIABILITY EFFORT

The current reactor quality assurance efforts embody most features of a formal reliability program. That is, they assemble various technical and administrative measures in a coherent approach to satisfying particular system reliability goals. But there remains the opportunity, introduced in Chapter 2, for substantial improvement in the present apportioning of resources in this endeavor. Advanced work, therefore, has both sought objective bases for quantitative reliability goals and promoted more effective integration of the support activities. By stressing broad problem approaches, such studies have added perspective to the safety reliability efforts.

6.1 Defining the Safety Reliability Requirement

The basic question of "How much safety is enough?" precedes the rational organization of reliability efforts. Siddall, of Canada, addressed this question in 1959 with some ideas on the balance between social risks and benefits.[30] He viewed the benefits partly in terms of greater affluence of society, with consequent better life quality and reduced general mortality; more specifically, he also anticipated a reduction in the mortality of hazardous occupations, such as coal mining, which would be displaced by nuclear power. Acceptable risk levels were inferred from those associated with other human activities, noting that our willingness to incur risk increases with the personal benefits. Acknowledging also the economic consequences of accidents, it was suggested how the acceptable risks could be expressed quantitatively in terms of frequencies for the principal classes of accidents. Several of Siddall's views today still seem speculative by U.S.A. standards, but reflect attitudes abroad. In particular, he hoped that experience gained from minor mishaps and from accidents successfully mitigated would result in improvements to prevent the most serious accidents. Moreover, he argued that money spent for containment shells might produce better results if spent to reduce accident probabilities, not just in reactors but in other industry as well.

Other authorities have since considered the risk vs benefit question in greater depth. Notable is Starr's correlation[31] between fatality rates and personal benefits for activities grouped according to whether personal exposure is voluntary or involuntary. The results suggest we are willing to accept involuntary risks in the range of one to three orders of magnitude lower per unit of exposure time than the overall disease mortality rate of one death per million persons per hour. Activities with high real or imagined benefits may induce us to incur risks two or more orders higher than average; private flying, for example, has about 20 times the disease mortality rate. Starr concludes that where the public might be willing to sustain risks equivalent to those arising from fossil fuel plants, estimated at 4×10^{-10} fatality per person per hour of exposure, the economic consequences of major accidents in nuclear plants would enforce a much lower risk limit, perhaps in the order of 10^{-11}.

Wall, of General Electric, approaches the same problem[32] through comparisons with the public risks from other major engineering works such as dams, bridges, buildings, etc. These installations are designed to withstand high stresses from natural catastrophes but with an awareness of the finite probabilities that even greater stresses can occur. Wall's article also cites studies indicating that, for constant personal risk, public risk aversion increases with the magnitude of the initiating hazardous events.

In 1967 Farmer, of the UKAEA, proposed[29] a reactor siting criterion that reflects three main accident probability considerations: risk to any individual, number of casualties, and public reaction. These are factored into a plot of allowable accident frequence vs curies of ^{131}I released in one accident. The criterion does not purport to represent the total risk from all accidents; the method was chosen for simplicity and the allowed frequencies were set conservatively low. Farmer further proposed that the criterion serve as a design basis for the protective systems and suggested methods whereby accident outcome probabilities could be estimated with regard to system reliability factors. Subsequent work by Beattie, Bell, and Edwards[97] has expanded on the UKAEA risk

evaluation approach, expressing it in general mathematical statements and obtaining solutions for particular proposed reactor sites. Overall, the method estimates average personal fatality risk with regard to accident initiation and protection system response probabilities, population distribution, meteorological conditions, and general exposure consequences.

The USAEC sponsored the development of a mathematical model to describe the probability distribution of radiation dose level from accidents as a function of time and location with respect to a reactor. It takes into account, by means of subsidiary models, such factors as reactor kinetics, heat transfer, fission product transport within the containment, and atmospheric transport beyond the containment, along with various aspects of system reliability. As might be expected, the overall program is quite complex. Informal criticisms of the results reflect perhaps more the great difficulty of the problem than the innovative work done to create the program. Mainly they concern the large number of elemental assumptions that are cascaded; some of the assumptions are introduced as input information and others are inherent in the calculation methods. A description was given[33] by Mulvihill in 1966.

6.2 Efforts to Establish Uniform Reliability Monitoring Program

Additional work sponsored by the USAEC was to develop a uniform reliability monitoring program for reactor safeguard systems. The first of the two major program phases concerned techniques to evaluate reliability of systems. This required initially the definition of system objectives and characteristics. Appropriate computer methods were then developed to facilitate the detailed analyses; these methods followed principles demonstrated in earlier aerospace programs, but were better adapted to the present needs. Two of the analysis procedures, ARMM and SAFTE, are described in Chapter 3 and in Example 1.3.2 of the Appendix. The other program phase, discussed in detail in Section 4.4.2.2, consisted in developing and demonstrating methods for collecting and analyzing data on the operation, maintenance, inspection, and testing of the safeguard systems components.

Largely in conjunction with the project just described, Garrick has proposed[21] a "Unified Systems Safety Analysis" approach to the overall problem. An interesting key feature of the approach is the "Activity Network," which represents a guiding pattern for all the diverse activities intended to produce reliable systems. Some 50 separate activities are identified and diagrammed according to their interrelationships, indicating the complexity of the overall problem.

In practice, the UKAEA has perhaps come closest to the ideal of a unified and rational approach to safety-reliability. This is partly by virtue of their advantage in having centralized control over their entire nuclear power effort. Although we may debate the overall merits both of this arrangement and the conclusions it has produced, the competence and dedication of the individuals responsible for the safety program command respect. To summarize, they have developed practical and rational safety reliability objectives, devised effective analysis procedures, and established an extensive system for collecting and processing the data necessary to support the analyses. References 97 through 106 describe various aspects of the UKAEA program.

7. CONCLUDING REMARKS

Interest in adapting reliability engineering methods for applications to reactor systems was highest in the United States between 1964 and 1969, stimulated by AEC support of several pilot programs to explore the reliability aspects of reactor safety. The benefits from the development effort of this period were mainly in terms of revealed opportunities to apply analytical techniques in evaluating or optimizing system designs and ways to introduce reliability considerations into quality assurance. Less successful were the initial attempts to extend the probabalistic approach to broad questions of safety, these evoking some opinion that highly complex analyses exaggerated rather than resolved the actual problem uncertainties. Continuing efforts have sought both to strengthen the credibility of analysis and to expand its role in providing guidance to other safety activities.

7.1 Emerging Analysis Roles

Reliability analysis is now firmly established as an effective and practical means for improving system designs, as evidenced by its steadily mounting application for review and optimization purposes. Attempts to extend the probabilistic approach to reactor risk and safety evaluation, however, continue to face rigorous challenges on grounds of credibility. The complex credibility question covers all phases of analysis, gaining expression commonly in the following areas of concern:

1. Does the analysis account for all factors significant to the conclusion, that is, will the probability of a common-mode failure be high enough to invalidate a reliability estimate based on random component failures?

2. Has the mathematical model distorted or biased the results, for example, by uneven level of detail or oversimplified component characteristics?

3. Are the analysis input data valid, for example, are component failure rates based on conclusive experience?

Advances in analytical capabilities have done a great deal to overcome the first two concerns, while accruing experience and innovations in data management promise to make available better information on components reliabilities. Moreover, in some studies the standpoint is now taken that their conclusions need represent no more than reliability which is reasonably attainable; hence the credibility burden is deferred or shifted to quality assurance.

Reactor protection systems, by virtue of being both standby facilities and arranged to provide multiple defenses, stress yet another aspect of analysis credibility: the requirement for relevance to reactor safety. The question of relevance becomes critical whenever it is attempted to place the reliability of one system in perspective with that of other systems sharing a functional responsibility, or with the probabilities of other events which affect a conclusion of interest. Obviously, the analytical model used for risk analysis must reflect accurately all the determining factors if the study is to be credible.

Relevance considerations have stimulated what is perhaps the most significant current trend in analysis of protection systems, toward studies which are situation oriented. The trend in some ways departs from the traditional reliability studies and in other ways builds upon them. Thus event arrays in the familar tree models of individual systems are beginning to emphasize system operating modes and conditions. Broader situation problems now are being attempted, often modeled as decision trees. These may incorporate the conclusions from studies of discrete ("hardware") systems of the scope ordinarily treated in a reliability analyses; such effects then appear in the main problem structure along with other events, special conditions, or specific equipment actions that affect the situation outcome probabilities. Moreover, numerical evaluations of the broader problems are increasingly distinguishing between two classes of system contribution: (1) those which can be adequately represented by general reliability factors of the sort determined by the traditional system-oriented analyses and (2) others so influenced by the special problem conditions as to require separate evaluation of specific response probabilities.

The case studies marking the current trend vary widely in depth and immediate objectives. In the United States a number of investigations are being patterned according to the Design Basis Accident (DBA) approach; that is, their initial conditions are those of the DBA's. The objectives, then, are to examine defense in depth and identify protection system weaknesses. Few of these studies are being carried out to probability evaluations, and what numerical conclusions have been reached are generally too tentative to warrant publication. References 59 through 62 describe a series of such studies by the domestic manufacturers of large water-cooled reactors. The UKAEA is routinely conducting full-scale risk analyses, which progress from initiating events through alternative situation outcomes. Probabilities are estimated for all outcome determining factors, and consequences are expressed as release magnitude vs frequency, in accordance with the Farmer risk criterion (Sect. 6.1). A comprehensive set of such risk studies constitutes the main safety assessment of a reactor plant.

Questions of risk-forecast credibility have unfortunately obscured the merits of the direct situation approach to system analysis, delaying its acceptance. The real advantages are in regard to improvement of system designs. Thus, the situation perspective contributes most by focusing on those reliability requirements pertinent to each plant contingency. Such requirements may be identified at the conceptual design level in terms of function responsibilities to be allocated among systems; at succeeding detailed levels, emphasis shifts to system operating modes and conditions, from which special equipment qualifications may be derived. Within the situation context appears, in addition, the main prospect of developing meaningful reliability criteria for protection systems — criteria which will reflect the importance of each system contribution to safety.

Given the present state of the art in reliability analysis, the immediate benefits from situation studies will be primarily the insights obtainable from the event or decision tree diagrams. Some probability evaluations of the trees are also desirable, but for the present these will be mostly incidental to comparing alternative designs, expressing

estimates, or formulating objectives. Quantitative statements of risk or situation outcome will gradually become less speculative as supporting experience accrues. Some factors that will determine the future acceptability of quantitative risk and safety evaluations are summarized in the next section.

The ultimate safety evaluation is, in effect, a summation of all risks. However, there is no general agreement on how best to combine the individual risk factors and set limits, for example, whether as integrated average population dose, maximum dose to individuals, mortality dose frequency, etc. Moreover, any "total risk" figure can be challenged with regard to accuracy or possible omissions. The UKAEA justification for advancing safety claims based on risk summation is that the levels are so low as to allow for substantial error and still remain within acceptable limits.

7.2 Aims in Analysis Development

More penetrating investigations of reliability and broader evaluations of risk clearly increase the demands on analysis. Current efforts with regard to (1) problem formulation, (2) support information gathering, (3) model evaluation techniques, and (4) resolution of uncertainties promote the development of analysis capability to its full potential.

7.2.1 Problem Formulation

The tree diagram in various forms is coming into general use as the basic model to express reliability or risk evaluation problems. Particularly, the fault tree has become popular with engineers due to its directness and ability to represent all manner of considerations. Little if any training is needed to prepare fault tree diagrams, and the results generally require no special interpretation to or by analysts. Moreover, a detailed problem can be managed via expansion of a main-event fault tree into subsidiary trees.

Advanced problems in risk analysis favor the decision tree form, which branches from an initiating event or condition through alternative

situation outcomes. This method, too, can be applied by the engineer independently, but with difficulty that mounts rapidly with increasing problem detail. By means of the coarse-structure decision tree, however, it will often be practical to identify subsidiary problems for separate evaluation.

Other procedures serve to organize and screen material for input to analysis models, as well as aiding in the search for design weaknesses. Very effective in this regard are the failure-mode-and-effect (FMEA) and the common-mode-failure (CMF) analysis approaches. The FMEA is generally quite detailed and time consuming but is nevertheless an important part of a thorough design review.

7.2.2 Support Information

The data requirements for reactor protection system reliability analyses and for the broader risk studies are only beginning to be met. The information problem is twofold: (1) there is insufficient experience with many important components to establish average failure rates conclusively and, (2) the more sophisticated current studies consider equipment response probabilities by specific operating modes and conditions, which may not correspond at all to the "averages."

How future data banks may cope with the problems is indicated by the UKAEA Syrel approach. Key activities there are the intensive, highly organized data collection effort and facilities for interpreting information according to problem needs. The Syrel system utilizes qualitative information and subjective engineering judgment along with statistical data.

In other significant efforts, qualitative observations from prototype tests are being organized into rational reliability conclusions. More general experience is also being exploited by synthesizing component reliability estimates out of parts and materials considerations, again utilizing qualified engineering judgment.

Increasingly, quality assurance is being called upon to guarantee minimum reliability levels. Where confidence can be placed in meeting the component specifications, the requirement levels themselves may be used in the system analysis.

7.2.3 Model Evaluation

The most satisfying progress in reliability analysis has been with regard to problem solution capabilities. Digital computers have dominated the scene since about 1965, the developments there having produced a wide range of programs.

Within the scope of each of the several major analytical programs exists a number of variations which either expand the program capability or improve efficiency; efficiency is generally achieved at the sacrifice of capabilities that may be of no advantage in particular problems. Systems of several hundred components are modeled routinely, often in problems involving mission sequences and other complex dependencies.

The existence of programs with great analytical power or special capabilities does not imply that all these programs are immediately available. In general the programs are proprietary, the analyst having access to the one main program (with variants) which has been developed, or bought and adapted, by his organization. Several organizations offer program availability as a part of reliability consulting services.

7.2.4 Analysis Uncertainties

Section 3.8.3 touched on the matter of analysis uncertainties with regard to input information. Almost all numerical analyses are built of point values, representing "best estimates" of component failure rates. The probable range of each value could be very wide in the case of poor data or close for good data. Evidently it would be desirable as a future objective for analysis conclusions to express the degree of overall data resolution in a manner analogous to the confidence levels and intervals of statistics.

7.3 Reliability Implementation

It should be understood that the bulk of the actual reactor reliability effort has been devoted to prosaic support tasks — the exhaustive design reviews, myriad quality control details, etc. — and to development projects which provide reliability information perhaps incidental to

other goals. The extent and effectiveness of such activities represent solid accomplishment to date in reliability implementation. In summary, the progress is evident in the rapidly developing standards and criteria, thorough administration of quality assurance tasks, guidance literature, and improvements in organizing staff responsibilities. The reactor quality assurance programs have taken on essentially all the features of formal reliability programs in other areas; however, the influence of quantitative analysis is still rather weak.

7.4 The Safety-Reliability Record

Since there have been no major releases of radioactivity from power reactors in the United States, the safety record must be rated as excellent. Enough incidents have occurred in power, test, and research reactors, however, to preclude a complacent attitude toward reliability factors in safety. Studies of these incidents by Epler[40] suggest that many would not have been predictable by the simpler analysis techniques. Some fundamental protective system failure causes he enumerates are: (1) change in characteristics of the system being protected, (2) unrecognized dependence on a common element, (3) equipment disabled by the accident, and (4) communication (human) error. Noting that it is virtually impossible to assign probabilities to these factors, the experience tends to discredit analysis-based claims for extremely high system reliability. The material of his studies is presented by way of argument for greater efforts to avoid such conditions as the potential for common-mode failures and human error and to assure that the systems are thoroughly qualified to perform their intended functions.

7.5 Viewpoints Abroad

The views expressed during three meetings sponsored by the European Nuclear Energy Agency (ENEA) Committee on Reactor Safety (CREST) and during a symposium of German specialists on nuclear safety reflect roughly the same status and problems regarding reliability as exist in the United States. The CREST meetings in 1967 were devoted to "Reliability of

Electronic Equipment and Systems for Nuclear Reactor Safety,"[109] in 1968 to "Reliability of Electric Supply Systems and Related Electromechanical Components for Nuclear Reactor Safety,"[110] and in 1969 to "Reliability of Mechanical Components and Systems for Nuclear Reactor Safety."[111] The German meeting in 1969 was more general.[112] There appeared to be overall agreement that quantitative reliability analysis, particularly via the fault tree, was a desirable aid in improving system designs, but concern was expressed over the lack of supporting data, the difficulties in obtaining and interpreting such data, and the likelihood of not being able to envision a substantial portion of the ultimate system failure causes or sequences. Considerable skepticism of quantitative analysis was voiced at the German meeting, and it was generally concluded that the MCA concept would not soon be entirely replaced as a basis for safety assessment of reactors.

REFERENCES

Reliability and Statistics Texts, etc.

1. N. H. Roberts, Mathematical Methods in Reliability Engineering, McGraw-Hill, New York, 1964.

2. I. Bazovsky, Reliability Theory and Practice, Prentice-Hall, Englewood Cliffs, N. J., 1961.

3. G. H. Sandler, System Reliability Engineering, Prentice-Hall, Englewood Cliffs, N. J., 1963.

4. S. R. Calabro, Reliability Principles and Practices, McGraw-Hill, New York, 1962.

5. M. L. Shooman, Probabilistic Reliability: An Engineering Approach, McGraw-Hill, New York, 1968.

6. W. H. Von Alven (ed.), ARINC Research Corporation, Reliability Engineering, Prentice-Hall, Englewood Cliffs, N. J., 1964.

7. B. Beizer and S. W. Leibholz, Engineering Applications of Boolean Algebra, Gage, New York, 1958.

8. W. G. Ireson (ed.), Reliability Handbook, McGraw-Hill, New York, 1966.

9. A. Hald, Statistical Theory with Engineering Applications, Wiley, New York, 1952.

10. A. H. Bowker and G. J. Lieberman, Handbook of Industrial Statistics, Prentice-Hall, Englewood Cliffs, N. J., 1955.

11. A. Hald, Statistical Tables and Formulas, Wiley, New York, 1952.

12. National Bureau of Standards, Tables of the Binomial Probability Distribution, Applied Mathematics Series No. 6.

13. R. Winfrey, Statistical Analyses of Industrial Property Retirements, Bulletin 125, Iowa Engineering Experiment Station, 1931.

14. E. B. Haugen, Probabilistic Approach to Design, Wiley, New York, 1968.

Topical or Comprehensive Reports on Reliability

15. Research Triangle Institute, Practical Reliability, vol. I, Parameter Variations Analysis, NASA-CR-1126 (July 1968).

16. Research Triangle Institute, Practical Reliability, vol. II, Computation, NASA-CR-1127 (August 1968).

17. Research Triangle Institute, Practical Reliability, vol. III, Testing, NASA-CR-1128 (August 1968).

18. Research Triangle Institute, Practical Reliability, vol. IV, Prediction, NASA-CR-1129 (August 1968).

19. Research Triangle Institute, Practical Reliability, vol. V, Parts, NASA-CR-1130 (July 1968).

20. B. J. Garrick et al., Reliability Analysis of Nuclear Power Plant Protective Systems, HN-190 (May 1967).

21. B. J. Garrick, "Unified Systems Safety Analysis for Nuclear Power Plants," dissertation submitted to the University of California, Los Angeles, 1968.

22. Advisory Group on Reliability of Electronic Equipment (AGREE), Reliability of Military Electronic Equipment, 1957.

23. Rome Air Development Center, RADC Reliability Notebook, RADC-TR-58-111, U.S. Air Force (Oct. 30, 1959) (published also by U.S. Department of Commerce as Report PB 161894).

24. Rome Air Development Center, RADC Reliability Notebook Supplement 1, RADC-TR-58-111 (suppl.), U.S. Air Force (Sept. 1, 1960) (published also by U.S. Department of Commerce as Report PB 161894-1).

25. MIL-STD-785, Requirements for Reliability Program for Systems and Equipment, effective June 30, 1955.

26. M. A. Schultz and G. C. Geisler, Study of New Protective System Design Techniques for Application in Nuclear Reactor Plants, NYO-3986-1 (Mar. 31, 1969).

27. E. A. Saltarelli and D. G. Fitzgerald, "Reliability Techniques as Applied to Operating Systems and to Design Optimization," Reactor Fuel Process. Technol. 12(1), 55–65 (Winter 1968–69).

(See also Ref. 98 and Subject Classified Bibliography of Ref. 68.)

Basis for Reliability Requirements

28. Code of Federal Regulations, Title 10, Part 50, General Design Criteria for Nuclear Power Plant Construction Permits; see also Federal Register 32(132), 10213–18 (July 11, 1967) and 36(35), 3255–60 (Feb. 20, 1971).

29. F. R. Farmer, Siting Criteria – A New Approach, UKAEA/AHSB Report SM 89/34 (1967). (Paper presented to IAEA Symposium on the Containment and Siting of Nuclear Power Reactors, Vienna, April 3–7, 1967.)

30. E. Siddall, "Statistical Analysis of Reactor Safety Standards," Nucleonics 17(2), 64–69 (February 1959).

31. C. Starr, "Social Benefit Versus Technological Risk," paper presented at the Symposium on Human Ecology, Warrenton, Virginia, November 24–27, 1968.

32. I. B. Wall, Application of Decision Analysis to Reactor Design and Siting Policy, Lecture Notes for Short Course on Nuclear Reactor Safety, UCLA, Sept. 8–12, 1969.

33. R. J. Mulvihill, A Probabilistic Methodology for the Safety Analysis of Nuclear Power Reactors, PRC-R-657, Planning Research Corp. (February 1966).

Systems Design

34. W. H. Jordan, A Philosophy of Reactor Control, ORNL-CF-53-3-241 (1953) (internal report).

35. T. J. Thompson and J. G. Beckerley (eds.), The Technology of Nuclear Reactor Safety, vol. 1, Reactor Physics and Control, MIT Press, Cambridge, Mass., 1964.

36. Nuclear Safety Information Center, Oak Ridge National Laboratory, Series of USAEC-ORNL-NSIC reports on reactor safety technology.

37. S. H. Hanauer and C. S. Walker, Design Principles of Reactor Protection Systems, ORNL-NSIC-51 (September 1968).

38. H. G. O'Brien and C. S. Walker, Protection Instrumentation Systems in Light-Water-Cooled Power Reactor Plants, ORNL-NSIC-29 (October 1969).

39. USAEC Public Document Room, Records of Application Proceedings for Licensing of All Private Reactors in the U.S.A.

40. E. P. Epler, "Common Mode Failure Considerations in the Design of Systems for Protection and Control," Nucl. Safety 10(1), 38–45 (January–February 1969).

(See also Refs. 14, 26, 28, 52, 88, 89, 90, and 91.)

Reliability Analysis Methods and Computer Programs

41. C. W. McKnight, L. J. Modiest, and N. E. Schmidt, "An Automatic Reliability Mathematical Model," pp. 518–32 in Proceedings of the Eleventh National Symposium on Reliability and Quality Control, 1965, Miami Beach, Fla.

42. A. B. Mearns, "Fault Tree Analysis: The Study of Unlikely Events in Complex Systems," paper presented at the System Safety Symposium sponsored by the University of Washington and the Boeing Co., Seattle, Wash., June 1965.

43. D. F. Haasl, "Advanced Concepts in Fault Tree Analysis," paper presented at the System Safety Symposium sponsored by the University of Washington and the Boeing Co., Seattle, Wash., June 1965.

44. P. M. Nagel, "A Monte Carlo Method to Compute Fault Tree Probabilities," paper presented at the System Safety Symposium sponsored by the University of Washington and the Boeing Co., Seattle, Wash., June 1965.

45. S. Orbach, "The Generalized Effectiveness Methodology (GEM) Analysis Program, Lab. Project 920-72-1," Progress Report 1, U.S. Naval Applied Science Laboratory, Brooklyn, N.Y. (May 8, 1968).

46. O. C. Baldonado, "On Some Computer Methods for System Reliability Evaluation," paper presented at the International Conference on Quality Control, Tokyo, Japan, Oct. 21–24, 1969.

47. W. E. Vesely, Analysis of Fault Trees by Kinetic Tree Method, IN-1330 (October 1969).

48. P. M. Nagel, "Importance Sampling in Systems Simulation," The Boeing Company Annals of Reliability and Maintainability, vol. 5, Achieving System Effectiveness, pp. 330–37, July 1966.

49. I. M. Jacobs, The Common Mode Failure Discipline, IEEE Trans. Nucl. Sci. NS 17(1), 594–97 (February 1970).

50. I. M. Jacobs and P. W. Marriott, Guidelines for Determining Safe Test Intervals and Repair Times for Engineered Safeguards, APED-5736, General Electric Co. (April 1969).

51. I. M. Jacobs, "Reliability of Engineered Safety Features as a Function of Testing Frequency," Nucl. Safety 9(4), 303–12 (July–August 1968).

52. D. Kececioglu and E. B. Haugen, "A Unified Look at Design Safety Factors, Safety Margins and Measures of Reliability," Annals of Assurance Sciences 1968, Seventh Reliability and Maintainability Conference, San Francisco, Calif., July 14–17, 1968, pp. 520–30.

53. W. E. Vesely, "Reliability and Fault Tree Applications at the NRTS," IEEE Trans. Nucl. Sci. NS 18, 472–80 (February 1971).

(See also Refs. 14, 20, 21, 27, 33, 63, 68, 98, 99, 100, 101, and 105.)

Analyses of Specific Systems

54. Atomics International and Combustion Engineering Corporations, Heavy Water Organic Cooled Reactor: 500 Mwe Nuclear Demonstration Plant Conceptual Design, Section G, Fault Tree Studies, AI-CE-MEMO-25 (Mar. 29, 1966).

55. I. M. Jacobs, Reactor Protection System: A Reliability Analysis, APED 5179, General Electric Co. (June 1966).

56. W. L. Headington, W. E. Stewart, and J. O. Zane, Fault Tree Analysis of the PBF Transient Rod Drive System, IDO-17274 (November 1968).

57. O. B. Monteith, Reliability Analysis of the FFTF Conceptual Plant Protection System, BNWL-1201 (October 1969).

58. M. E. Stewart, J. F. White, and J. O. Zane, Reliability Analysis of the Power Burst Facility Reactor Protection System, IN-ITR-200 (December 1969).

59. T. W. T. Burnett et al., Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors, WCAP-7306 (April 1969).

60. L. G. Frederick et al., An Analysis of Functional Common-Mode Failures in GE BWR Protection and Control Instrumentation, NEDO-10189 (July 1970).

61. W. C. Coppersmith et al., Reactor Protection System Diversity, CENPD-11 (February 1971).

62. Systematic Failure Study of Reactor Protection Systems, BAW-10019 (September 1970).

Components Reliability Information

63. P. Rubel, "Reliability of Reactor Components," Nucl. Safety 9(6), 481–86 (November–December 1968).

64. D. R. Earles and M. F. Eddins, Reliability Engineering Data Series – Failure Mechanisms, AVCO Corp., April 1962.

65. Interagency Data Exchange Program (IDEP), Information Systems Handbook, IDEP Sixth Annual Workshop Conference, Los Angeles, Calif., May 1–3, 1968.

66. Reliability and Maintainability Data – Source Guide, System Effectiveness Branch, Electronics Division, U.S. Naval Applied Science Laboratory, Brooklyn, N.Y., January 1967.

67. Liquid Metal Engineering Center, Failure and Problem Reporting for Nuclear Reactors (brochure), LMEC-Memo-69-6 (1969).

68. Liquid Metal Engineering Center, Failure Data Handbook for Nuclear Power Facilities, LMEC-Memo-69-7 (Aug. 15, 1969).

69. B. J. Garrick et al., Collection of Reliability Data at Nuclear Power Plants, HN-199 (December 1968).

70. MIL-HDBK-217, Military Standardization Handbook – Reliability, Stress and Failure Rate Data for Electronic Equipment, Defense Documentation Center, Washington, D.C., 1962.

71. MIL-HDBK-217A, Military Standardization Handbook – Reliability, Stress and Failure Rate Data for Electronic Equipment, Defense Documentation Center, Washington, D.C.

72. NAVSHIP-93820, Handbook for the Prediction of Shipboard and Shore Electronic Equipment Reliability, 1961.

73. Federal Aviation Administration, Maintenance Data Analysis Program, FAA Handbook 8300.2A, Rev. Apr. 16, 1970.

74. Federal Aviation Administration, Handbook for Maintenance Control by Reliability Methods, FAA Advisory Circular 120.17, Dec. 31, 1964.

75. Failure Rate Data (FARADA) Program, Naval Fleet Missile Systems Analysis and Evaluation Group, Corona, Calif. (descriptive brochure), Rev. April 1969.

76. Interagency Data Exchange Program (IDEP): Scope, Objectives, Operation, IDEP-IV, Program Summary (descriptive brochure) (July 1967).

77. Interagency Data Exchange Program (IDEP): Requirements for Participation, IDEP-I (descriptive brochure) (March 1968).

78. Interagency Data Exchange Program (IDEP): Information Storage and Retrieval System, IDEP-V, Operational Procedures (descriptive brochure) (July 1967).

79. Interagency Data Exchange Program (IDEP): Codes for Establishing Index Number, IDEP-II (descriptive brochure) (January 1969).

80. Interagency Data Exchange Program: The IDEP Alert Dissemination Procedure (descriptive brochure) (August 1968).

81. Interagency Data Exchange Program (IDEP): Test Equipment Calibration Procedures, IDEP-VII, Participation Requirements (descriptive brochure) (August 1969).

82. I. M. Jacobs, "Demonstration of the Performance and Reliability of the General Electric Company Boiling Water Reactor Main Steamline Isolation Valves," presented at the CREST meeting on Reliability of Mechanical Systems and Components, Risø, Denmark, September 1969.

83. S. A. Wilson, "Pipe Reliability Estimating by the Time to Damage Method," presented at the 15th Annual Meeting of the American Nuclear Society, Seattle, Wash., June 15–19, 1969.

84. Edison Electric Institute, Report on Equipment Availability for the Nine Year Period, 1960–68, EEI Publication 69-33 (September 1969).

85. H. M. Johaningsmeir, "Status of EEI Nuclear Plant Reliability Data Collection System," paper presented at the 1971 IEEE Nuclear Power Systems Symposium, San Francisco, Calif., November 4, 1971.

(See also Refs. 94, 96, 102, 103, 104, 105, and 106.)

Quality Assurance

86. R. Schuster, "Utility Heads Cite Quality Gap," Power Eng. 74(6), 43–44 (June 1970).

87. RDT Standard: Quality Assurance Program Requirements, RDT F 2-2T, USAEC Division of Reactor Development and Technology, June 1969.

88. Institute of Electrical and Electronics Engineers, Proposed IEEE Criteria for Nuclear Power Plant Protection Systems, IEEE Publication No. 279, August 1968.

89. Institute of Electrical and Electronics Engineers, IEEE Criteria for Class IE Electric Systems for Nuclear Power Generating Stations, IEEE Publication No. 308, September 1969.

90. RDT Standard: Supplementary Criteria and Requirements for RDT Reactor Plant Protection Systems, RDT C 16-1T, USAEC Division of Reactor Development and Technology, December 1969.

91. International Electrotechnical Commission, Principles of Nuclear Reactor Instrumentation, IEC Publication 231, Geneva, 1967.

92. Nuclear Safety Information Center, Compilation of United States Nuclear Standards, 5th ed., ORNL-NSIC-57 (1968).

93. Nuclear Safety Information Center, Compilation of National and International Nuclear Standards — Excluding U.S. Activities, 5th ed., ORNL-NSIC-63 (1969).

(See also Ref. 74.)

Reviews of Reactor Plant Reliability Experience

94. B. J. Garrick, W. J. Costley, and W. C. Gekler, A Study of Test Reactor Operating and Safety Experience, HN-172 (May 1963).

95. B. J. Garrick et al., A Study of Research Reactor Operating and Safety Experience, HN-180 (June 1964).

96. B. J. Garrick, W. C. Gekler, and H. P. Pomrehn, An Analysis of Nuclear Power Plant Operating and Safety Experience, HN-185 (1966).

(See also Ref. 69.)

UKAEA* Safety-Reliability Program

97. J. R. Beattie, G. D. Bell, and J. E. Edwards, Methods for the Evaluation of Risk, AHSB (S) R 159 (1969).

98. A. E. Green and A. J. Bourne, Safety Assessment with Reference to Automatic Protective Systems for Nuclear Reactors, AHSB (S) R 117 (1966).

99. A. R. Eames, Reliability Assessment of Protective Equipment for Nuclear Installations, AHSB (S) R 99 (1965).

100. A. E. Green, Assessment of Sensing Channels for High Integrity Protective Systems, AHSB (S) R 113 (1965).

101. E. R. Woodcock, The Calculation of Reliability of Systems: The Program Noted, AHSB (S) R 153 (1968).

102. Systems Reliability Service, descriptive brochure by the UKAEA Reactor Group, 1970.

103. A. R. Eames, Data Store Requirements Arising out of Reliability Analyses, AHSB (S) R 138 (1967).

---

*United Kingdom Atomic Energy Authority; Authority Health and Safety Branch (AHSB).

104. E. Parker and R. Roughley, AHSB Reporting System for Plant Faults — Plant Fault Code, AHSB (S) R 127 (1967).

105. G. Hensley, The Reliability Prediction of Mechanical Instrumentation Equipment for Process Control, AHSB (S) R 178 (1969).

106. SYREL Reliability Data Bank, descriptive brochure, 1970.

(See also Ref. 29.)

Reactor Safety Research and Development

107. Water Reactor Safety Program Plan, WASH-1146 (February 1970).

108. "Progress Summary of Nuclear Safety Research and Development Project," Nuclear Safety (included as a regular feature in every issue).

ENEA/CREST and German Meetings

109. ENEA/CREST, Colloquium of Specialists on the Reliability of Electronic Equipment and Systems for Nuclear Reactor Safety, Docket EUR/C/3747/67, Brussels, Belgium, Apr. 11–12, 1967.

110. ENEA/CREST, Meeting of Specialists on the Reliability of Electrical Supply Systems and Related Electromechanical Components for Nuclear Reactor Safety, Docket 19452/111/68, Ispra, Italy, June 27–28, 1968.

111. L. Leonardini, "The Third Reliability Meeting at Risø, ENEA/CREST Docket 19338/111/69," Nucl. Safety 11(4), 309–14 (July–August 1970).

112. E. A. Nephew, "Fifth German Symposium on Progress in Safety Evaluation of Nuclear Power Plants," Nucl. Safety 11(6), 463–67 (November–December 1970).

Personal Communications

113. N. E. Schmidt, North American Rockwell Corporation.

114. B. J. Garrick, W. C. Gekler, O. C. Baldinado, and R. J. Mulvihill, Holmes and Narver, Inc.

115. R. T. Burke, Federal Aviation Administration, Maintenance Analysis Center, Oklahoma City, Okla.

116. E. T. Richards and R. R. Moore, U.S. Navy Fleet Missile Systems Analysis and Evaluation Group (FARADA and IDEP programs).

117. R. Smith and R. Impara, USAEC Division of Reactor Standards.

118. C. W. Griffin, Liquid Metals Engineering Center.

119. E. Davidson, USAEC Division of Reactor Development and Technology.

120. I. M. Jacobs and L. Frederick, General Electric Company.

121. D. G. Fitzgerald, E. A. Saltarelli, J. R. Lennon, and J. Johnson, NUS Corporation and Consultech.

122. S. Levine, USAEC Division of Reactor Licensing (lecture at UCLA short course on Reactor Safety).

123. V. A. Moore, USAEC Division of Reactor Licensing.

124. J. P. O'Reilly, USAEC Division of Compliance.

125. W. E. Vesely, Idaho Nuclear Corporation.

APPENDIX

Part 1: Analysis Basic Examples

1.1 Notations

K, $\overline{K}$	Element (e.g., component) "K" is good (K), or failed ($\overline{K}$); represents status and not probability*
S, $\overline{S}$	System is good (S), or failed ($\overline{S}$); represents status and not probability*
S_K, F_K, A_K	Immediate probability that element "K" is good (S), or failed (F), or available (A)
S_S, F_S, A_S	Immediate probability that system is good (S), or failed (F), or available (A)
$S_K(t)$, $S_S(t)$, etc.	Above probabilities as functions of time
[P: (descriptor)]	Immediate probability of condition described
[P(t): (descriptor)]	Probability, as a function of time, of condition described
[S_S, F_S, S_A, F_A, etc. | (descriptor)]	Immediate probability that system or subsystem (e.g., "A") is good (S) or failed (F), <u>given</u> conditions described
[$S_S(t)$, etc. | (descriptor)]	Above <u>conditional</u> probabilities as functions of time
P_i (t)	Probability that system is in state "i" at time t
F-K, R-K	Events: Failure or repair of element "K"

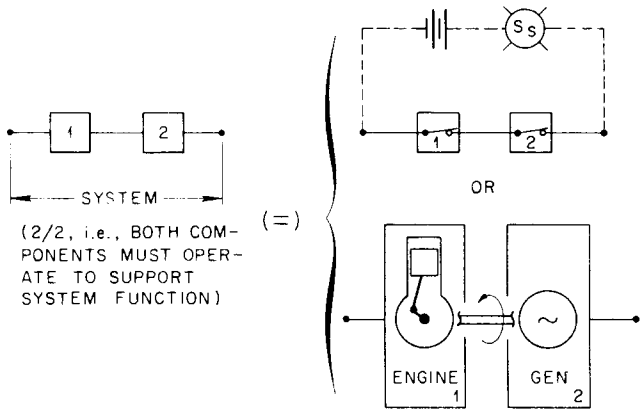
*In some literature, notation shown does signify probability.

1.2 Basic Examples

1.2.1 Direct ("Immediate") Probability Combinations

1.2.1.1 Series Elements

(a)



Element state probabilities:

$S_1 + F_1 \equiv 1$ (i.e., it is certain that element 1 is either good or failed)

$S_2 + F_2 \equiv 1$

System state probabilities:

$$S_1S_2 + S_1F_2 + F_1S_2 + F_1F_2 \equiv 1$$

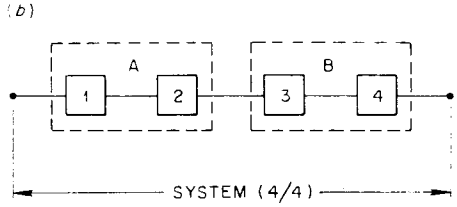
$$S_1S_2 = S_S$$

$$S_1F_2 + F_1S_2 + F_1F_2 = F_S$$

Restate F_S in more conventional terms of elemental failure probabilities only:

$$F_S = (1 - F_1)F_2 + F_1\ (1 - F_2) + F_1F_2$$
$$= F_1 + F_2 - F_1F_2$$

(b)



By analogy to (a):

$$F_S = F_A + F_B - F_A F_B$$
$$F_A = F_1 + F_2 - F_1 F_2$$
$$F_B = F_3 + F_4 - F_3 F_4$$
$$F_S = F_1 + F_2 + F_3 + F_4 - F_1F_2 - F_1F_3 - F_1F_4 - F_2F_3 - F_2F_4 - F_3F_4 + F_1F_2F_3 + F_1F_2F_4 + F_1F_3F_4 + F_2F_3F_4 - F_1F_2F_3F_4$$
$$S_S = S_A S_B$$
$$S_A = S_1 S_2$$
$$S_B = S_3 S_4$$
$$S_S = S_1S_2S_3S_4$$

By system states:

$$F_S + S_S = 1$$
$$S_S = S_1S_2S_3S_4$$
$$F_S = F_1S_2S_3S_4 + S_1F_2S_3S_4 + S_1S_2F_3S_4 + S_1S_2S_3F_4 + F_1F_2S_3S_4 + F_1S_2F_3S_4 + F_1S_2S_3F_4 + S_1F_2F_3S_4 + S_1F_2S_3F_4 + S_1S_2F_3F_4 + F_1F_2F_3S_4 + F_1F_2S_3F_4 + F_1S_2F_3F_4 + S_1F_2F_3F_4 + F_1F_2F_3F_4$$

Simplest expressions:

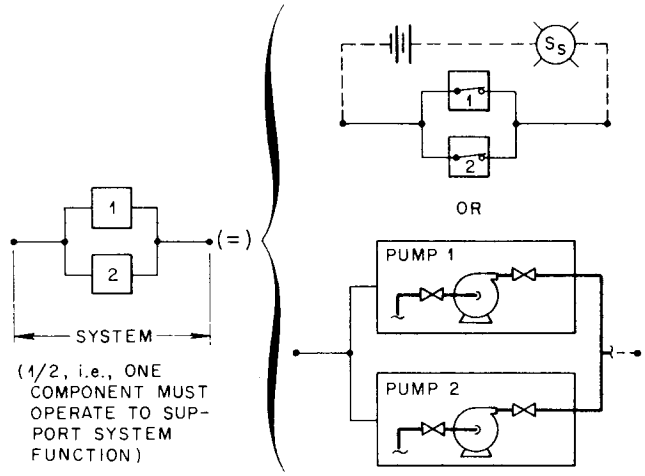
$$S_S = S_1S_2S_3S_4$$
$$F_S = 1 - S_S = 1 - S_1S_2S_3S_4$$

Note: All above expressions for F_S are equivalent.

Numerical example: Assume $F_1 = F_2 = F_3 = F_4 = S_1 = S_2 = S_3 = S_4 = 0.5$; then

$$S_S = (0.5)^4 = 0.0625$$
$$F_S = 1 - S_S = 0.9375$$

1.2.1.2 Parallel Elements (i.e., Independent-Redundant)



System state probabilities:

$$S_1S_2 + S_1F_2 + F_1S_2 + F_1F_2 \equiv 1$$

(i.e., same as "a" in Ex. 1.2.1.1, and general for any two-element system)

$$F_1F_2 = F_S$$

$$S_1S_2 + S_1F_2 + F_1S_2 = S_S$$

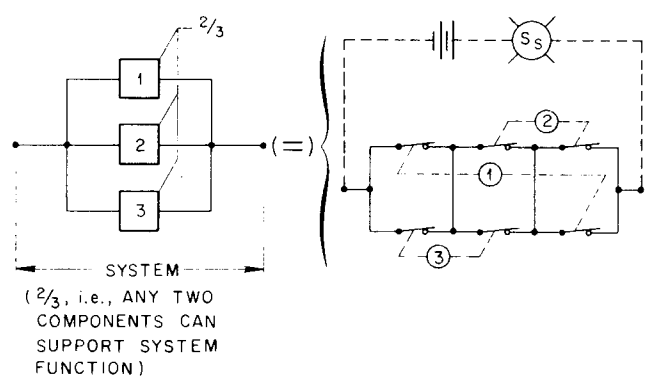
Restate S_S in more conventional terms of elemental success probabilities only:

$$S_S = S_1S_2 + S_1(1 - S_2) + (1 - S_1)S_2$$
$$= S_1 + S_2 - S_1S_2$$

Restate S_S in simplest form:

$$S_S = 1 - F_S$$
$$= 1 - F_1F_2$$

1.2.1.3 Any M-of-N Elements



Problem statement: If any two elements are failed, system is failed. (Note: This corresponds to a situation of three half-capacity pumps or electric generators.)

System state probabilities:

$$S_1S_2S_3 + F_1S_2S_3 + S_1F_2S_3 + S_1S_2F_3 + F_1F_2S_3 + F_1S_2F_3 + S_1F_2F_3 + F_1F_2F_3 = 1$$

$$F_S = F_1F_2S_3 + F_1S_2F_3 + S_1F_2F_3 + F_1F_2F_3$$

$$S_S = S_1S_2S_3 + F_1S_2S_3 + S_1F_2S_3 + S_1S_2F_3$$

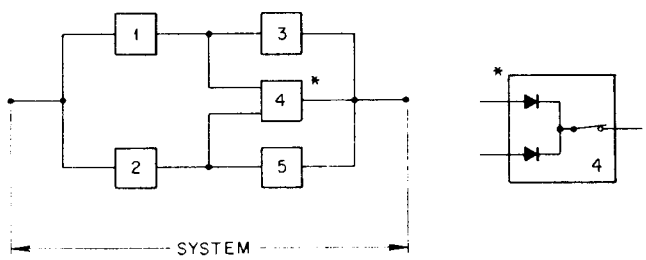
Simplify statements:

$$F_S = (S_1 + F_1 = 1)\ F_2F_3 + F_1F_2S_3 + F_1S_2F_3$$

$$= F_2F_3 + F_1F_2S_3 + F_1S_2F_3$$

$$S_S = S_2S_3 + S_1F_2S_3 + S_1S_2F_3$$

1.2.1.4 Restricted Redundance



Problem statement: If element 1 <u>and</u> either element 3 or element 4 are good, <u>or</u> element 2 <u>and</u> either element 5 or element 4 are good, the system is good. (Note: This corresponds to a situation where one emergency generator is assigned to one reactor unit in a plant, a second generator is assigned to the other reactor unit, and the third generator is a spare that can serve either reactor unit; elements 1 and 2 then represent the distribution systems, and elements 3, 4, and 5 are the generators.)

This is a convenient point to introduce conditional probability as a means to develop the system overall probability statement:

a) $S_S = [S_S \mid 1]{*}S_1 + [S_S \mid \overline{1}]F_1$

($*S_S$, given that element 1 is good, etc.)

b) $[S_S \mid 1] = [S_S \mid 1 \,\&\, 3]S_3 + [S_S \mid 1 \,\&\, \overline{3}]F_3$

c) $[S_S \mid 1 \,\&\, 3] = (1)$ (i.e., certainty)

d) $[S_S \mid 1 \,\&\, \overline{3}] = [S_S \mid 1 \,\&\, \overline{3} \,\&\, 4]S_4 + [S_S \mid 1 \,\&\, \overline{3} \,\&\, \overline{4}]F_4$

e) $[S_S \mid 1 \,\&\, \overline{3} \,\&\, 4] = (1)$

f) $[S_S \mid 1 \,\&\, \overline{3} \,\&\, \overline{4}] = [S_S \mid 1 \,\&\, \overline{3} \,\&\, \overline{4} \,\&\, 2]S_2 + [S_S \mid 1 \,\&\, \overline{3} \,\&\, \overline{4} \,\&\, \overline{2}]F_2$

g) $[S_S \mid 1 \,\&\, \overline{3} \,\&\, \overline{4} \,\&\, 2] = S_5$

h) $[S_S \mid 1 \,\&\, \overline{3} \,\&\, \overline{4} \,\&\, \overline{2}] = (0)$

f′) $[S_S \mid 1 \,\&\, \overline{3} \,\&\, \overline{4}] = S_5S_2$

d′) $[S_S \mid 1 \,\&\, \overline{3}] = S_4 + S_2S_5F_4$

b′) $[S_S \mid 1] = S_3 + S_4F_3 + S_2S_5F_4F_3$

i) $[S_S \mid \overline{1}] = [S_S \mid \overline{1} \,\&\, 2]S_2 + [S_S \mid \overline{1} \,\&\, \overline{2}]F_2$

j) $[S_S \mid \overline{1} \,\&\, 2] = [S_S \mid \overline{1} \,\&\, 2 \,\&\, 4]S_4 + [S_S \mid \overline{1} \,\&\, 2 \,\&\, \overline{4}]F_4$

k) $[S_S \mid \overline{1} \,\&\, 2 \,\&\, 4] = (1)$

l) $[S_S \mid \overline{1} \,\&\, 2 \,\&\, \overline{4}] = S_5$

j′) $[S_S \mid \overline{1} \,\&\, 2] = S_4 + S_5F_4$

m) $[S_S \mid \overline{1} \,\&\, \overline{2}] = (0)$

i′) $[S_S \mid \overline{1}] = S_4S_2 + S_5F_4S_2$

a′) $S_S = S_3S_1 + S_4F_3S_1 + S_2S_5F_4F_3S_1 + S_4S_2F_1 + S_5F_4S_2F_1$

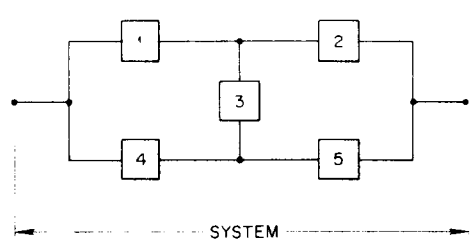
$= S_1S_3 + S_1F_3S_4 + S_1S_2F_3F_4S_5 + F_1S_2S_4 + F_1S_2F_4S_5$

a″) $F_S = (1) - S_S$

Note: Different, but equivalent, expressions will result from starting the conditional probability problem from different points. Also, the above expression can be expanded to obtain all of the "Success State" terms by recognizing that, for example:

$$S_1S_3 \equiv S_1S_3\,(1) \equiv S_1S_3\,[S_2S_4S_5 + F_2S_4S_5 + S_2F_4S_5 + S_2S_4F_5 + F_2F_4S_5 + F_2S_4F_5 + S_2F_4F_5 + F_2F_4F_5],\ \text{etc.}$$

1.2.1.5 Cross-Link or Bridge



Problem statement: Any of the following minimum combinations of good elements will result in the system being good: (1 and 2) or (4 and 5) or (1 and 3 and 5) or (4 and 3 and 2). (Note: This corresponds to a situation where redundant load elements are fed from redundant power networks, with a tie breaker.)

By conditional probability:

$$S_S = [S_S \mid 3]S_3 + [S_S \mid \overline{3}]F_3$$

$$[S_S \mid 3] = \text{(intermediate steps not shown)}$$

$$= S_1S_2 + S_1F_2S_5 + F_1S_2S_4 + F_1F_2S_4S_5$$

$$[S_S \mid \overline{3}] \equiv S_S \text{ for simple parallel system with elements } 1, 2, 4, 5$$

$$= S_1S_2 + S_4S_5 - S_1S_2S_4S_5$$

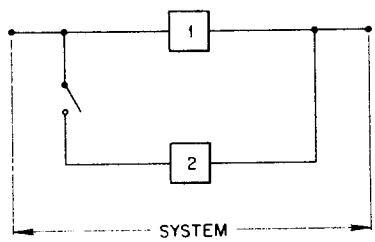
$$S_S = S_1S_2S_3 + S_1F_2S_3S_5 + F_1S_2S_3S_4 + F_1F_2S_3S_4S_5 + S_1S_2F_3 + F_3S_4S_5 - S_1S_2F_3S_4S_5$$

Noting that $S_1S_2S_3 + S_1S_2F_3 = S_1S_2\ (1)$,

$$S_S = S_1S_2 + S_1F_2S_3S_5 + F_1S_2S_3S_4 + F_1F_2S_3S_4S_5 + F_3S_4S_5 - S_1S_2F_3S_4S_5$$

$$= \text{(other equivalent expressions)}$$

1.2.1.6 Standby – Parallel



Problem statement: If element 1 does not fail, <u>or</u> if element 2 does not fail and the switch operates one time, the system is good.

By conditional probability:

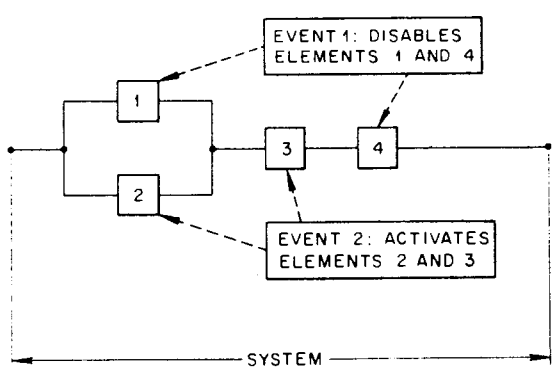
$$S_S = [S_S \mid 1]S_1 + [S_S \mid \overline{1}]F_1$$

$$[S_S \mid 1] = (1)$$

$$[S_S \mid \overline{1}] = [\text{P: switch operates}]S_2$$

$$S_S = S_1 + F_1S_2\ [\text{P: switch operates}]$$

1.2.1.7 A Generalized Event-Dependent (or "Contingent") Probability



Problem statement: Elements 1, 2, 3, and 4 form a simple series-parallel system. All elements are subject to random failure. Event 1 disables elements 1 and 4. Elements 2 and 3 cannot function unless activated by event 2.

By conditional probability:

a) $S_S = [S_S \mid \text{event } 1]\cdot[P\text{: event } 1] + [S_S \mid \text{no event } 1]\cdot[P\text{: no event } 1]$

b) $[S_S \mid \text{event } 1] = (0)$

c) $[S_S \mid \text{no event } 1] = [S_S \mid (\text{no event } 1)\ \&\ (\text{event } 2)]\cdot[P\text{: event } 2] + [S_S \mid (\text{no event } 1)\ \&\ (\text{no event } 2)]\cdot[P\text{: no event } 2]$

d) $[S_S \mid (\text{no event } 1)\ \&\ (\text{event } 2)] \equiv [S_S\text{: as determined by element failures alone}] = [S_1 + S_2 - S_1S_2]S_3S_4 = S_1S_3S_4 + S_2S_3S_4 - S_1S_2S_3S_4$

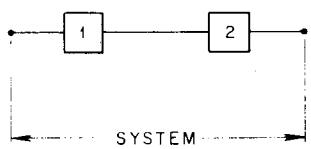
e) $[S_S \mid (\text{no event } 1)\ \&\ (\text{no event } 2)] = (0)$

c′) $[S_S \mid \text{no event } 1] = [S_1S_3S_4 + S_2S_3S_4 - S_1S_2S_3S_4]\cdot[P\text{: event } 2]$

a′) $S_S = [P\text{: no event } 1]\cdot[P\text{: event } 2]\cdot[S_1S_3S_4 + S_2S_3S_4 - S_1S_2S_3S_4]$

1.2.2 Combinations of Probability vs Time Functions

1.2.2.1 Series Elements — Continuous, No Repair



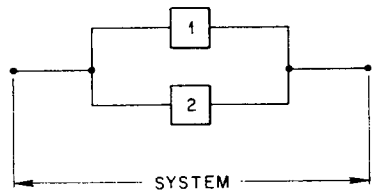
a) General:

$$F_S(t) = F_1(t) + F_2(t) - F_1(t)F_2(t)$$
$$S_S(t) = S_1(t)S_2(t)$$

b) For constant failure rates, λ_1 and λ_2 (i.e., "exponential" failure distribution):

$$S_1(t) = e^{-\lambda_1 t};\ F_1(t) = 1 - e^{-\lambda_1 t}$$
$$S_2(t) = e^{-\lambda_2 t};\ F_2(t) = 1 - e^{-\lambda_2 t}$$
$$S_S(t) = e^{-\lambda_1 t}e^{-\lambda_2 t} = e^{-(\lambda_1 + \lambda_2)t}$$
$$F_S(t) = 1 - e^{-(\lambda_1 + \lambda_2)t}$$

1.2.2.2 Parallel Elements — Continuous, No Repair



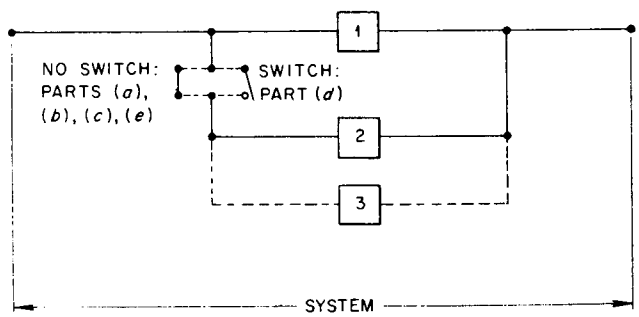
a) General:

$$F_S(t) = F_1(t)F_2(t)$$
$$S_S(t) = S_1(t) + S_2(t) - S_1(t)S_2(t)$$

b) For constant failure rates, λ_1 and λ_2:

$$F_S(t) = (1 - e^{-\lambda_1 t})\,(1 - e^{-\lambda_2 t})$$
$$= 1 - e^{-\lambda_1 t} - e^{-\lambda_2 t} + e^{-(\lambda_1 + \lambda_2)t}$$
$$S_S(t) = e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1 + \lambda_2)t}$$

1.2.2.3 Parallel Elements – Standby, No Repair



a) Problem statement: If element 1 fails and then element 2 fails, the system fails. Element 2 is not subject to failure while in standby

By conditional probability:

$$S_S(t) = [S_S(t)|\,1]\; S_1(t) + [S_S(t)|\,\bar{1}]\; F_1(t)$$
$$[S_S(t)|\,1] = (1)$$
$$[S_S(t)|\,\bar{1}] = [S_2(t)|\,\bar{1} \text{ at time } t]$$

Note qualification of $S_2(t)$, namely that $\bar{1}$ is regarded as certainty at time t. Accordingly, the probability of $\bar{1}$ at $t_1 < t$ is:

$$[F_1(t_1)|\,\bar{1} \text{ at time } t] = \frac{F_1(t_1)}{1 - e^{-\lambda_1 t}} = \frac{1 - e^{-\lambda_1 t_1}}{1 - e^{-\lambda_1 t}}$$

Then the probability of $\bar{1}$ occurring during dt_1 at t_1 (i.e., given $\bar{1}$ at t)

$$= \frac{d}{dt_1} [F_1(t_1) | \bar{1} \text{ at time } t] \, dt_1$$

$$= \underbrace{\frac{\lambda_1}{1 - e^{-\lambda_1 t}} e^{-\lambda_1 t_1} \, dt_1}$$

$$[S_2(t)|\bar{1}] = \int_{t_1=0}^{t_1=t} \left| \overbrace{\frac{\lambda_1}{1 - e^{-\lambda_1 t}} e^{-\lambda_1 t_1} \, dt_1} \right| \quad 1 \quad \left| e^{-\lambda_2 (t - t_1)} \right|$$

= [P: given that element 2 is called upon, call occurs during dt_1 at t_1]

= [P: an element 2 called upon at t_1 has survived to t_1]

= [P: an element 2 called upon and surviving at t_1 will then survive to t]

$$= \left(\frac{1}{1 - e^{-\lambda_1 t}}\right) \left(\frac{\lambda_1}{\lambda_2 - \lambda_1}\right) \left(e^{-\lambda_1 t} - e^{-\lambda_2 t}\right)$$

$$S_S(t) = S_1(t) + [S_2(t)|\bar{1}] \, F_1(t)$$

$$= e^{-\lambda_1 t} + \left[\left(\frac{1}{1 - e^{-\lambda_1 t}}\right) \left(\frac{\lambda_1}{\lambda_2 - \lambda_1}\right) \left(e^{-\lambda_1 t} - e^{-\lambda_2 t}\right)\right] \left[1 - e^{-\lambda_1 t}\right]$$

$$= e^{-\lambda_1 t} + \left[\left(\frac{\lambda_1}{\lambda_2 - \lambda_1}\right) \left(e^{-\lambda_1 t} - e^{-\lambda_2 t}\right)\right]$$

b) Problem statement: Same as (a), but by more concise "probability density function" method.

The probability density function (pdf) for a system describes the *rate* at which the failure probability for the system is increasing. Usually, this function consists of several terms, each one describing the contribution of one component to the total rate of increase of the system failure probability. For a single-component system, exponential failure distribution, the function is just:

$$[\text{Rate of Increase of Failure Probability}] = \frac{d}{dt} [F_1(t)] = \frac{d}{dt} \left[1 - e^{-\lambda_1 t}\right] = \lambda_1 e^{-\lambda_1 t}$$

For a system of several components, all in continuous service, the corresponding expression is a set of partial differentials of $F_S(t)$ with respect to t and, respectively, each contributing component.

The "standby" case – without the switch – is special because of its discontinuity. This system can fail *only* when the last standby element fails. Consequently, the probability density function can be expressed in just one term, if that term also includes the contributions of preceding elements. For the two-element system, with exponential distributions, this is developed as follows:

[Failure pdf] ≡ [Rate of Increase of System Failure Probability]

$$= \int_{t_1=0}^{t_1=t} \lambda_1 e^{-\lambda_1 t_1}\, dt_1 \; \cdot \; 1 \; \cdot \; e^{-\lambda_2 (t-t_1)} \; \cdot \; \lambda_2$$

- $\lambda_1 e^{-\lambda_1 t_1}\, dt_1$ = [P: standby element 2 is called upon in dt_1 at $t_1 < 1$]
- 1 = [P: element 2 survives to t_1]
- $e^{-\lambda_2 (t-t_1)}$ = [P: an element 2 placed in service at t_1 will survive to t]
- λ_2 = rate of increase of failure probability of a surviving element 2

= [P: an element 2 will be placed in service in dt_1 at t_1 and will survive to t]

$$= \lambda_1 \lambda_2 \left(\frac{e^{-\lambda_1 t}}{\lambda_2 - \lambda_1} + \frac{e^{-\lambda_2 t}}{\lambda_1 - \lambda_2} \right)$$

$$F_S(t) = \int_0^t [\text{pdf}]\, dt$$

$$= 1 - \left[e^{-\lambda_1 t} + \frac{\lambda_1}{\lambda_2 - \lambda_1} \left(e^{-\lambda_1 t} - e^{-\lambda_2 t} \right) \right]$$

$= [1 - S_S(t)]$, as obtained in part (a)

c) Problem statement: Same as (b), but with third standby element added. Element 3 is not subject to failure until placed in service.

$$[\text{Failure pdf}] \equiv \left[\frac{d\, F_S(t)}{dt} : \text{3-element system} \right]$$

$$= \int_{t_2=0}^{t_2=t} \left[\lambda_1 \lambda_2 \left(\frac{e^{-\lambda_1 t_2}}{\lambda_2 - \lambda_1} + \frac{e^{-\lambda_2 t_2}}{\lambda_1 - \lambda_2} \right) \right] dt_2 \; \cdot \; 1 \; \cdot \; e^{-\lambda_3 (t-t_2)} \; \cdot \; \lambda_3$$

- $\left[\lambda_1 \lambda_2 \left(\frac{e^{-\lambda_1 t_2}}{\lambda_2 - \lambda_1} + \frac{e^{-\lambda_2 t_2}}{\lambda_1 - \lambda_2} \right) \right]$ = pdf for 2-element system (see previous example)
- dt_2
- 1 = [P: element 3 survives to t_2]
- $e^{-\lambda_3 (t-t_2)}$ = [P: element 3 placed in service at t_2 survives to t]
- λ_3 = rate of increase of failure probability of a surviving element 3

= [P: 2-element system fails in dt_2 at t_2
= [P: element 3 is called upon in dt_2 at t_2

= pdf for element 3

An equivalent but more concise statement is:

$$[\text{Failure pdf of 3-element system}] = \int_{t_2=0}^{t_2=t} \int_{t_1=0}^{t_1=t_2} \begin{bmatrix} \text{pdf of} \\ \text{element 1} \end{bmatrix} \begin{bmatrix} \text{pdf of} \\ \text{element 2} \end{bmatrix} \begin{bmatrix} \text{pdf of} \\ \text{element 3} \end{bmatrix} dt_1\, dt_2$$

$$= \int_{t_2=0}^{t_2=t} \int_{t_1=0}^{t_1=t_2} \left[\lambda_1 e^{-\lambda_1 t_1} \right] \left[\lambda_2 e^{-\lambda_2 (t_2 - t_1)} \right] \left[\lambda_3 e^{-\lambda_3 (t-t_2)} \right] dt_1\, dt_2$$

$$F_S(t) = \int_{t=0}^{t=t} \text{[pdf of 3-element system]}\ dt$$

$$= 1 - \left[\frac{\lambda_2 \lambda_3 e^{-\lambda_1 t}}{(\lambda_2 - \lambda_1)(\lambda_3 - \lambda_1)} + \frac{\lambda_1 \lambda_3 e^{-\lambda_2 t}}{(\lambda_1 - \lambda_2)(\lambda_3 - \lambda_2)} + \frac{\lambda_1 \lambda_2 e^{-\lambda_3 t}}{(\lambda_1 - \lambda_3)(\lambda_2 - \lambda_3)} \right]$$

d) Problem statement: Same as (a), but with the switch added. The system can now fail in two ways: either by element 1 and the switch failing, *or* by element 2 failing. Because there are these two modes, the single pdf used in (b) must be replaced by a more complex function. It is just as convenient in this case to use a conditional probability statement like in (a):

$$S_S(t) = [S_S(t) | 1]\ S_1(t) + [S_S(t) | \bar{1}]\ F_1(t)$$

$$[S_S(t) | 1] = (1)$$

$$[S_S(t) | \bar{1}] = [S_S(t) | \bar{1} \text{ \& switch fails}] \cdot [\text{P: switch fails}]$$
$$+ [S_S(t) | \bar{1} \text{ \& switch operates}] \cdot [\text{P: switch operates}]$$

$$[S_S(t) | \bar{1} \text{ and switch fails}] = (0)$$

$$[S_S(t) | \bar{1} \text{ \& switch operates}] = [S_2(t) | \bar{1} \text{ at time t}]$$

$$S_S(t) = e^{-\lambda t} + \left[\left(\frac{\lambda_1}{\lambda_2 - \lambda_1} \right) \left(e^{-\lambda_1 t} - e^{-\lambda_2 t} \right) \right] \cdot [\text{P: switch operates}]$$

e) Problem statement: Same as (a), but element 2 subject to random failure rate λ_{2A} while in standby and λ_{2B} in service. The system can now fail in two ways: by element 1 failing after element 2, or element 2 after element 1; again the single pdf in (b) must be replaced by a more complex function,* and it is more convenient to use a conditional probability statement:

$$S_S(t) = [S_S(t) | 1]\ S_1(t) + [S_S(t) | \bar{1}]\ F_1(t)$$

$$[S_S(t) | 1] = (1)$$

$$[S_S(t) | \bar{1}] = [S_2(t) | \bar{1} \text{ at time t}]$$

$$\text{*pdf (failure)} = \underbrace{\left[\int_{t_1=0}^{t_1=t} \lambda_1 e^{-\lambda_1 t} dt_1\ e^{-\lambda_{2A} t_1} e^{-\lambda_{2B}(t-t_1)} \lambda_2 \right]}_{\text{= rate of increase of system failure probability due to element 2 failures } \textit{after} \text{ element 1 failures}} + \underbrace{\left[\lambda_1 e^{-\lambda_1 t} (1 - e^{-\lambda_{2A} t}) \right]}_{\text{= rate of increase of system failure probability due to element 2 failures } \textit{before} \text{ element 1 failures}}$$

$$[S_2(t)\,|\,\bar{1} \text{ at time } t]^{\dagger} = \int_{t_1=0}^{t_1=t} \left(\frac{\lambda_1}{1-e^{-\lambda_1 t}}\right) e^{-\lambda_1 t_1}\, dt_1 \;\Bigg|\; \underbrace{e^{-\lambda_{2A} t_1}}_{\substack{= [\text{P: an element 2 that is called upon at } t_1 \text{ has survived to } t_1]}} \;\Bigg|\; e^{-\lambda_{2B}(t-t_1)}$$

$$= \left(\frac{1}{1-e^{-\lambda_1 t}}\right)\left(\frac{\lambda_1}{\lambda_{2B}-\lambda_1-\lambda_{2A}}\right)\left(e^{-(\lambda_1+\lambda_{2A})t} - e^{-\lambda_{2B} t}\right)$$

$$S_S(t) = S_1(t) + [S_2(t)\,|\,\bar{1} \text{ at time } t]\; F_1(t)$$

$$= e^{-\lambda_1 t} + \left[\left(\frac{\lambda_1}{\lambda_{2B}-\lambda_1-\lambda_{2A}}\right)\left(e^{-(\lambda_1+\lambda_{2A})t} - e^{-\lambda_{2B} t}\right)\right]$$

1.2.3 Probability vs Time Functions for Repairable Systems: "Markov Chain" Problems
(Note: See discussion in Sect. 3.4.3.)

1.2.3.1 Repairable Single-Element System: Element has exponential failure distribution with rate λ and exponential repair distribution with rate μ

System state a $\equiv$ Element 1 is good
System state b $\equiv$ Element 1 is failed

[P: System is in state a at time $(t + \Delta t)$] $\equiv P_a(t + \Delta t)$

= [P: system is in state a at time t]

+ [P: system is in state b at time t] $\times$
[P: system is repaired during interval Δt and does not fail again in Δt]

- [P: system is in state a at time t] $\times$
[P: system fails during interval Δt and is not repaired again in Δt]

$\pm$ [P: multiple failures and repairs within single Δt; this P $\to$ 0]

$$P_a(t + \Delta t) = P_a(t) + P_b(t)\,\mu\,\Delta t - P_a(t)\,\lambda\,\Delta t \pm (0)$$

$$\underset{\Delta t \to 0}{\text{Limit}} \frac{P_a(t + \Delta t) - P_a(t)}{\Delta t} = \frac{d\,P_a(t)}{dt} = P_b(t)\,\mu - P_a(t)\,\lambda$$

---

†Expression analogous to that in part (a).

Similarly:

$$P_b(t + \Delta t) = P_b(t) + P_b(t)\,\lambda\,\Delta t - P_b(t)\,\mu\,\Delta t \pm (0)$$

$$\underset{\Delta t \to 0}{\text{Limit}} \frac{P_b(t + \Delta t) - P_b(t)}{\Delta t} = \frac{d\,P_b(t)}{dt} = P_a(t)\,\lambda - P_b(t)\,\mu$$

$$\frac{d\,P_a(t)}{dt} = -\,P_a(t)\,\lambda + P_b(t)\,\mu$$

$$\frac{d\,P_b(t)}{dt} = P_a(t)\,\lambda - P_b(t)\,\mu$$

$$P_a(t) = 1 - P_b(t), \text{ i.e., } P_a(t) + P_b(t) \equiv 1$$

$$\frac{d\,P_a(t)}{dt} = -P_a(t)\,\lambda + \mu - P_a(t)\,\mu$$

With the initial condition that the element was good at t = 0:

$$P_a(0) = 1$$

$$P_a(t) = \frac{\lambda e^{-(\lambda+\mu)t} + \mu}{\lambda + \mu}$$

With the initial condition that the element was failed at t = 0,

$$P_a(0) = 0$$

$$P_a(t) = \frac{\mu\left(1 - e^{-(\lambda+\mu)t}\right)}{\lambda + \mu}$$

With the initial condition that the probability of element failed at t = 0 is 50%:

$$P_a(0) = 0.5$$

$$P_a(t) = \frac{\mu - \left(\frac{\mu - \lambda}{2}\; e^{-(\lambda+\mu)t}\right)}{\lambda + \mu}$$

1.2.3.2 Two-Element System: Elements 1 and 2 have exponential failure rates λ_1 and λ_2, respectively, and exponential repair rates μ_1 and μ_2

This problem is solved first as a "generalized" two-element system; i.e., it is of no interest at first which states represent

system failure or success. After obtaining a solution for every state, we then combine them according to the element configuration to determine the system success/failure probabilities.

The system has four possible states:

State a ≡ element 1 — good; element 2 — good
State b ≡ element 1 — good; element 2 — failed
State c ≡ element 1 — failed; element 2 — good
State d ≡ element 1 — failed; element 2 — failed

For state a:

[P: system is in state a at time $(t + \Delta t)$] $\equiv P_a(t + \Delta t)$

$= P_a(t)$

$- [P_a(t)] \times$ [P: failure of element 1 during Δt causes system to leave state a]

$- [P_a(t)] \times$ [P: failure of element 2 during Δt causes system to leave state a]

$+ [P_b(t)] \times$ [P: element 2 is repaired during Δt, causing system to enter state a]

$+ [P_c(t)] \times$ [P: element 1 is repaired during Δt, causing system to enter state a]

$\pm \sum$ [P: multiple events during Δt, such as repair of both elements if state d existed at time t, or failure and repair of one element, etc.; this $P \to 0$]

$$P_a(t + \Delta t) = P_a(t) - [P_a(t)][(\lambda_1 + \lambda_2)\,\Delta t] + [P_b(t)][\mu_2\,\Delta t] + [P_c(t)][\mu_1\,\Delta t] \pm (0)$$

$$\lim_{\Delta t \to 0} \frac{P_a(t + \Delta t) - P_a(t)}{\Delta t} = \frac{d\,P_a(t)}{dt} =$$

$$-(\lambda_1 + \lambda_2)\,P_a(t) + \mu_2\,P_b(t) + \mu_1\,P_c(t) + (0)\,P_d(t)$$

Similar development yields differential expressions for the other three states. They can be represented altogether and solved as the following matrix:

$$\begin{bmatrix} \dot{P}_a(t) \\ \dot{P}_b(t) \\ \dot{P}_c(t) \\ \dot{P}_d(t) \end{bmatrix} = \begin{bmatrix} (-\lambda_1 - \lambda_2) & \mu_2 & \mu_1 & 0 \\ \lambda_2 & (-\lambda_1 - \mu_2) & 0 & \mu_1 \\ \lambda_1 & 0 & (-\lambda_2 - \mu_1) & \mu_2 \\ 0 & \lambda_1 & \lambda_2 & (-\mu_1 - \mu_2) \end{bmatrix} \begin{bmatrix} P_a(t) \\ P_b(t) \\ P_c(t) \\ P_d(t) \end{bmatrix}$$

Typically, the initial conditions for solving the equations represent an "all-new" system:

$$P_a(t = 0) = 1$$

$$\left.\begin{aligned} P_b(0) &= 0 \\ P_c(0) &= 0 \\ P_d(0) &= 0 \end{aligned}\right\}$$ i.e., there is no possibility of any failures allowed at t = 0

Solving the differential equations for all the $P_i(t)$ yields a set of individual expressions, each describing the probability vs time that a particular combination of failed and unfailed elements exists. System expressions corresponding to Example groups 1.2.1 and 1.2.2 are obtained simply by adding the $P_i(t)$ expressions for the system state of interest. Thus, if the original two elements formed a parallel redundant system:

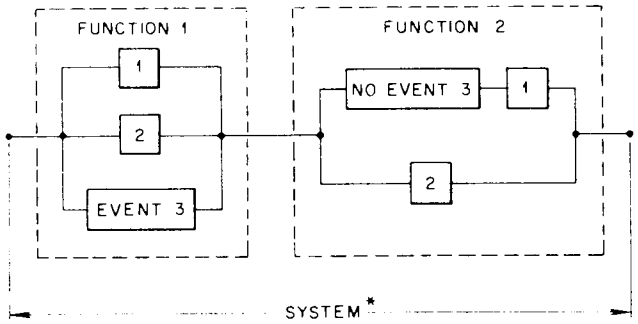
$$S_S(t) = P_a(t) + P_b(t) + P_c(t)$$
$$F_S(t) = P_d(t)$$

Special constraints may be added in the matrix solution to yield modified conclusions. For example, one form of reliability interest is where we wish to know the [P(t): System has <u>never</u> failed]. This is expressed in the equations by prohibiting any transfers out of states corresponding to system failure (e.g., for the 2-element parallel system, transfers out of state d).

Differential equations like the example, but with more complicated terms, can be written to represent element failure and repair distributions other than exponential, to represent events, and to represent interdependencies among elements (e.g., standby redundance).

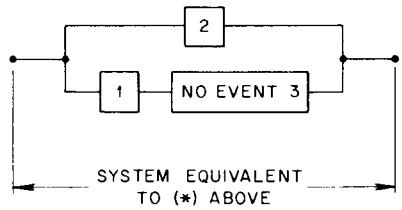
1.2.4 Other Aspects of System Problems

1.2.4.1 Block or Logic Diagram Representation of Components or Events That Have Multiple Effects in System

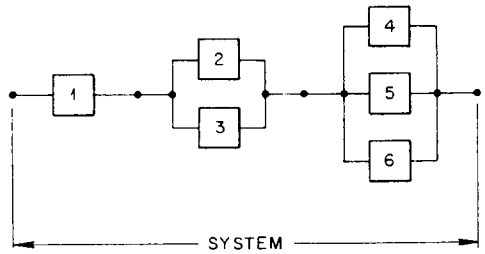


$$S_S = S_1S_2[P\text{: event } 3] + F_1S_2[P\text{: event } 3] + S_1S_2[P\text{: no event } 3]$$
$$+ F_1S_2[P\text{: no event } 3] + S_1F_2[P\text{: no event } 3]$$
$$= S_2 + S_1F_2[P\text{: no event } 3]$$
$$F_S = S_1F_2[P\text{: event } 3] + F_1F_2[P\text{: event } 3] + F_1F_2[P\text{: no event } 3]$$
$$= F_1F_2 + S_1F_2[P\text{: event } 3]$$

*Note: For a complex system it would require formal methods (e.g., Boolean) to make a network simplification like:



1.2.4.2 Approximation to System Failure Probability: Restricted Number of Failures in System (i.e., larger number of independent failures is considered too improbable to be worthwhile considering)



a) Complete statement of system failure probability, by conditional probability method:

$$F_S = F_1 + S_1F_2F_3 + S_1S_3F_4F_5F_6 + S_1S_2F_3F_4F_5F_6$$

b) By conditional probability, allowing no more than two failures to exist in the system:

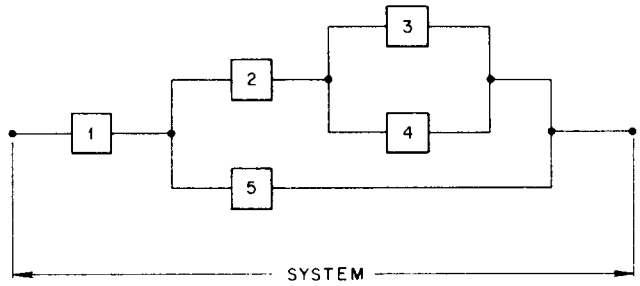
$$F_S = [F_S \mid \bar{1}]F_1 + [F_S \mid 1]S_1$$
$$[F_S \mid \bar{1}] = (1)$$
$$[F_S \mid 1] = [F_S \mid 1 \,\&\, \bar{2}]F_2 + [F_S \mid 1 \,\&\, 2]S_2$$
$$[F_S \mid 1 \,\&\, \bar{2}] = F_3$$
$$[F_S \mid 1 \,\&\, 2] = (0)$$

since there is no other way in which just <u>two</u> failures can disable system.

$$[F_S \mid 1] = F_2F_3$$

$$F_S = F_1 + S_1F_2F_3$$

1.2.4.3 Approximation to System Failure Probability: "Minimum Cut Set"



The minimum cut sets are:

$$\overline{1},\ \overline{2}\ \overline{5},\ \overline{3}\ \overline{4}\ \overline{5}$$

System failure probability — rigorous:

$$F_S = F_1 + S_1F_2F_5 + S_1S_2F_3F_4F_5$$

System failure probability — by minimum cut set:

$$F_S = F_1 + F_2F_5 + F_3F_4F_5$$

1.2.4.4 Sensitivity of System Probabilities to Changes in Elemental Probabilities: Sensitivity Analysis

a) Simple change in component parameter:

$$\text{Sensitivity*} = [F_S \mid \text{New value of component parameter}] - [F_S \mid \text{Old value of component parameter}]$$

(*Can be expressed as a fraction or percent change, or can be with respect to S_S, $S_S(t)$, $F_S(t)$, etc.)

b) Rate of variation of system probability with change in component parameter:

$$\frac{dS_S}{d\ (\text{component parameter})}\ ;\ \left[\frac{\partial S_S}{\partial\ (\text{parameter 1})} + \frac{\partial S_S}{\partial\ (\text{parameter 2})}\right]\ ;$$

$$\frac{\Delta S_S}{\Delta\ (\text{component parameter})}\ ;\ \text{etc.}$$

For a two-element series system, exponential distributions of component failures:

$$S_S(t) = e^{-\lambda_1 t}\ e^{-\lambda_2 t}$$

$$\frac{d\ S_S(t)}{d\lambda_1} = -t\ S_S(t) = -\ te^{-\lambda_1 t}\ e^{-\lambda_2 t}$$

$$\frac{\Delta\ S_S(t)}{\Delta\lambda_1} \approx -\ t\ S_S(t)$$

$$\frac{\partial\ S_S(t)}{\partial\lambda_1} + \frac{\partial\ S_S(t)}{\partial\lambda_2} = -2t\ S_S(t)$$

1.2.4.5 Testing

a) Average availability of a three-element series system over interval T, where the component test intervals are, respectively, t_1, t_2, and t_3; also, assume $t_1 < t_2 < t_3$ and $t_3 < T < (t_3 + t_1)$

$$A_S \text{ average over } T = \frac{1}{T}\left[\int_0^{t_1} A_S(t)\ dt + \int_{t_1}^{t_2} A_S(t)\ dt + \int_{t_2}^{t_3} A_S(t)\ dt + \int_{t_3}^{T} A_S(t)\ dt\right]$$

b) Average availability of a three-element series system, each element having exponential failure distribution, ALL ELEMENTS TESTED SIMULTANEOUSLY and at regular intervals of t_1; rigorous method:

$$A_S(t) = e^{-(\lambda_1+\lambda_2+\lambda_3)t}$$

$$A_S \text{ average over } t_1 = \frac{1}{t_1}\int_0^{t_1} e^{-(\lambda_1+\lambda_2+\lambda_3)t}\ dt$$

$$= \frac{1 - e^{-(\lambda_1+\lambda_2+\lambda_3)t}}{t_1\ (\lambda_1 + \lambda_2 + \lambda_3)}$$

c) Same as (b), but using midpoint approximations for individual component availabilities:

$$A_S \text{ average over } t_1 \approx e^{-\lambda_1 t_1/2}\ e^{-\lambda_2 t_1/2}\ e^{-\lambda_3 t_1/2}$$

d) Same as (c), but further approximating the component averages:

$$A_S \text{ average over } t_1 \approx \left(1 - \frac{\lambda_1 t_1}{2}\right)\left(1 - \frac{\lambda_2 t_1}{2}\right)\left(1 - \frac{\lambda_3 t_1}{2}\right)$$

e) Same as (d), but with different test intervals for each component and for a T >> (any test interval):

$$A_S \text{ average over } T \approx \left(1 - \frac{\lambda_1 t_1}{2}\right)\left(1 - \frac{\lambda_2 t_2}{2}\right)\left(1 - \frac{\lambda_3 t_3}{2}\right)$$

1.3 Examples of Analysis by Computer Programs

1.3.1 "Analytical" Approach: by "Automatic Reliability Mathematical Model" (ARMM)

1.3.1.1 Organization of Analysis Program

a) Define reliability problem for each time interval in a sequential series: changes from one interval to the next may include problem objective (e.g., from "Availability" to "Mission Reliability," etc.), system configuration, events considered, component or event probability parameters, etc. In effect, each interval is a separate problem. Group problem system elements by "Functions."

b) For each interval, determine significant failure combinations by conditional probability in "general" form.

c) For each interval, calculate by numerical integration (Simpson's rule) the probability that each individual component will fail during that interval, assuming it was "new" at the beginning. Store values for future retrieval, either directly or as complementary values (i.e., nonfailure probabilities). Similarly, determine and store interval event probabilities.

d) Select from (c) and combine according (b) the required factors to determine system failure probability over one interval.

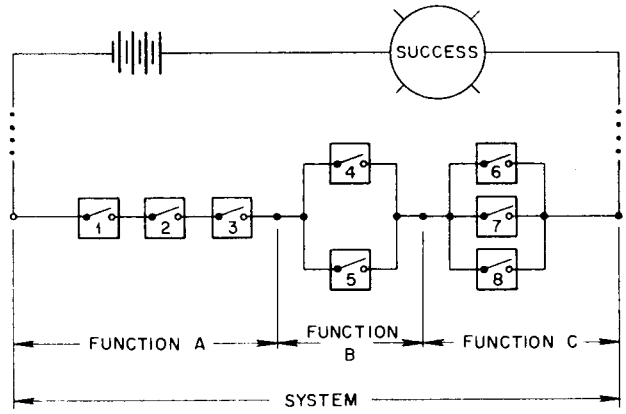
e) Multiply together the complements of the values obtained by (d) for all intervals to obtain overall "Mission Success" probability.

f) If desired, steps analogous to (b), (c), and (d) may be used to determine failure probabilities of individual functions for any interval or overall; however, like the main problem, every sequence assumes that a function is "renewed" (i.e., no carry-over of accumulated probability) at the beginning of each interval.

g) Similar to (f), but function contributions to overall system failure probability.

h) Similar to (f) and (g), but for individual components.

1.3.1.2 Computer Approach to Determining Significant Failure Combinations for One Interval:



In following arrays, "4" means component 4 is not failed, and is represented by "switch" closed or logic gate open, etc. "$\overline{4}$" means component 4 is failed. An array like $123\overline{4}\overline{5}$ --- F signifies a defined set of failure combinations wherein 1, 2, and 3 must be good; 4 and 5 must be failed.

a) Unrestricted number of failures:

Step	Combination		Failure?
1	$\overline{1}2345678$	---	F
2	$1\overline{2}345678$	---	F
3	$12\overline{3}45678$	---	F
4	$123\overline{4}5678$		
5	$123\overline{4}\overline{5}678$	---	F
6	$123\overline{4}5\overline{6}78$		
7	$123\overline{4}5\overline{6}\overline{7}8$		
8	$123\overline{4}5\overline{6}\overline{7}\overline{8}$	---	F
9	$123\overline{4}5\overline{6}7\overline{8}$		
10	$123\overline{4}56\overline{7}\overline{8}$		
11	$1234\overline{5}678$		
12	$1234\overline{5}\overline{6}78$		
13	$1234\overline{5}\overline{6}\overline{7}8$		
14	$1234\overline{5}\overline{6}\overline{7}\overline{8}$	---	F
15	$1234\overline{5}\overline{6}7\overline{8}$		
16	$1234\overline{5}6\overline{7}\overline{8}$		
17	$12345\overline{6}78$		
18	$12345\overline{6}\overline{7}8$		

Step	Combination		Failure?
19	$1234\overline{5678}$	---	F
20	$1234\overline{5}\overline{678}$		
21	$1234\overline{567}\overline{8}$		
22	$1234\overline{5}\overline{6}\overline{78}$		

Most efficient statement of system failure probability, obtained by conditional probability methods (see Ex. 1.2.1.4, etc.) is:

$$F_S = F_1 + S_1F_2 + S_1S_2F_3 + S_1S_2S_3F_4F_5 + S_1S_2S_3S_4F_6F_7F_8 + S_1S_2S_3F_4S_5F_6F_7F_8;$$

corresponding element combinations are

$$\overline{S} = \overline{1} + 1\overline{2} + 12\overline{3} + 123\overline{45} + 1234\overline{678} + 12\overline{3}4\overline{5}\overline{678}.$$

From computer-identified combinations:

$$\overline{S} = \overline{1} + 1\overline{2} + 12\overline{3} + 123\overline{45} + 12\overline{3}4\overline{5}\overline{678} + 1234\overline{5}\overline{678} + 12345\overline{678}.$$

Noting that $1234\overline{678} = 12345\overline{678} + 1234\overline{5}\overline{678}$, the two expressions for $\overline{S}$ are equivalent.

b) Number of failures restricted to two; i.e., "Depth Controlled" to two:

Step	Combination		Failure?
1	$\overline{1}2345678$	---	F
2	$1\overline{2}345678$	---	F
3	$12\overline{3}45678$	---	F
4	$123\overline{4}5678$		
5	$123\overline{45}678$	---	F
6	$123\overline{4}\overline{5}\overline{6}78$		
7	$123\overline{4}\overline{5}6\overline{7}8$		
8	$123\overline{4}\overline{5}67\overline{8}$		
9	$1234\overline{5}678$		
10	$1234\overline{56}78$		
11	$1234\overline{5}\overline{6}\overline{7}8$		
12	$1234\overline{5}\overline{6}7\overline{8}$		
13	$12345\overline{6}78$		
14	$12345\overline{678}$		

Step	Combination	Failure?
15	$1234\overline{567}\overline{8}$	
16	$1234\overline{567}8$	
17	$1234\overline{567}\overline{8}$	

$[\overline{S}$: by computer$] \equiv [\overline{S}$: conditional probability$]$

$$= \overline{1} + 1\overline{2} + 12\overline{3} + 12\overline{345}$$

1.3.1.3 Typical Failure Probability Expressions for Individual Components:

a) Independent component, exponential failure distribution:

$$[F_2\text{: at end of interval 5}] = 1 - \int_0^{t=t_5-t_4} e^{-\lambda_2(t-t_4)}\ \lambda_2\ dt$$

b) Standby redundance, exponential distribution (see Ex. 1.2.2.3.b):

$$[F_4F_5\text{: at end of interval 7}] = \int_0^{t=t_7-t_6} \lambda_4\ \lambda_5 \left(\frac{e^{-\lambda_4(t-t_6)}}{\lambda_5 - \lambda_4} + \frac{e^{-\lambda_5(t-t_6)}}{\lambda_4 - \lambda_5}\right) dt$$

c) General, any distribution (e.g., Weibull in 1965 program version):

$$[F_K\text{: at end of interval } (i + 1)] = \int_0^{t=t_{i+1}-t_i} [\text{failure probability density function for component K}]\ dt.$$

1.3.1.4 Probability of System Failure in One Interval:

Assume number of component failures restricted to two during interval 8, and that the following values had been calculated for component state probabilities over interval 8, by methods of preceding example: $F_1 = 0.1$, $S_1 = 0.9$; $F_2 = 0.01$, $S_2 = 0.99$; $F_3 = 0.01$, $S_3 = 0.99$; $F_4 = 0.1$, $S_4 = 0.9$; $F_5 = 0.1$, $S_5 = 0.9$.

$$[F_{S:8}] \equiv [F_S\text{: over interval 8}] = 0.1 + (0.9 \times 0.01) + (0.9 \times 0.99 \times 0.01) + (0.9 \times 0.99 \times 0.99 \times 0.1 \times 0.1) = 0.1257$$

1.3.1.5 Probability of Mission Failure over N Intervals

$$P = [1 - F_{S:1}] \times [1 - F_{S:2}] \times \ldots \times [1 - F_{S:N}]$$

1.3.1.6 Contribution of Function A to System Failure Probability During Interval 1:

[contribution of function A during interval 1] = ($F_{S:1}$: no qualifications] − [$F_{S:1}$: F_A prohibited]

$= [F_1 + S_1F_2 + S_1S_2F_3 + S_1S_2S_3F_4F_5 + S_1S_2S_3S_4F_6F_7F_8 + S_1S_2S_3F_4S_5F_6F_7F_8$: interval 1] − [$F_4F_5 + S_4F_6F_7F_8 + F_4S_5F_6F_7F_8$: interval 1]

1.3.2. Monte-Carlo Simulation: SAFTE Program Concept

1.3.2.1 Organization of Program

A) Define reliability problem for one interval of interest: during this interval the system logical model does not change, i.e., the reliability objectives and component parameters do not change. All elements are "good as new" at the beginning of the interval, and any repairable element is restored to this condition by repair.

B) For each component or event, a sequence of random occurrences is determined by "Monte-Carlo," up to the end of the interval. A repairable component (or reversible event) may by chance fail and be repaired several times within one interval, or may not sustain the first failure.

C) From (B), develop a cumulative list of system events in proper sequence according to calculated time of occurrence. At each event, log all of the individual conditions (e.g., component failures) remaining at that time to contribute to system failure.

D) For the system conditions effective following each occurrence listed in (C), test the system logic model to determine whether the system is failed or not.

E) Log and analyze the results of many iterations of (B—C—D). The results of interest are: (1) number of runs in which system failure occurred and (2) time-to-failure, averaged over all runs.

The above steps are illustrated in Fig. A.1-1.

1.3.2.2 Conduct of Runs and Interpretation of Results

A) Direct results as programmed (Ref. 20, p. 2.41)

1. Probability of system first failure within interval of run (i.e., at $t < T_0$, Fig. A.1-1).

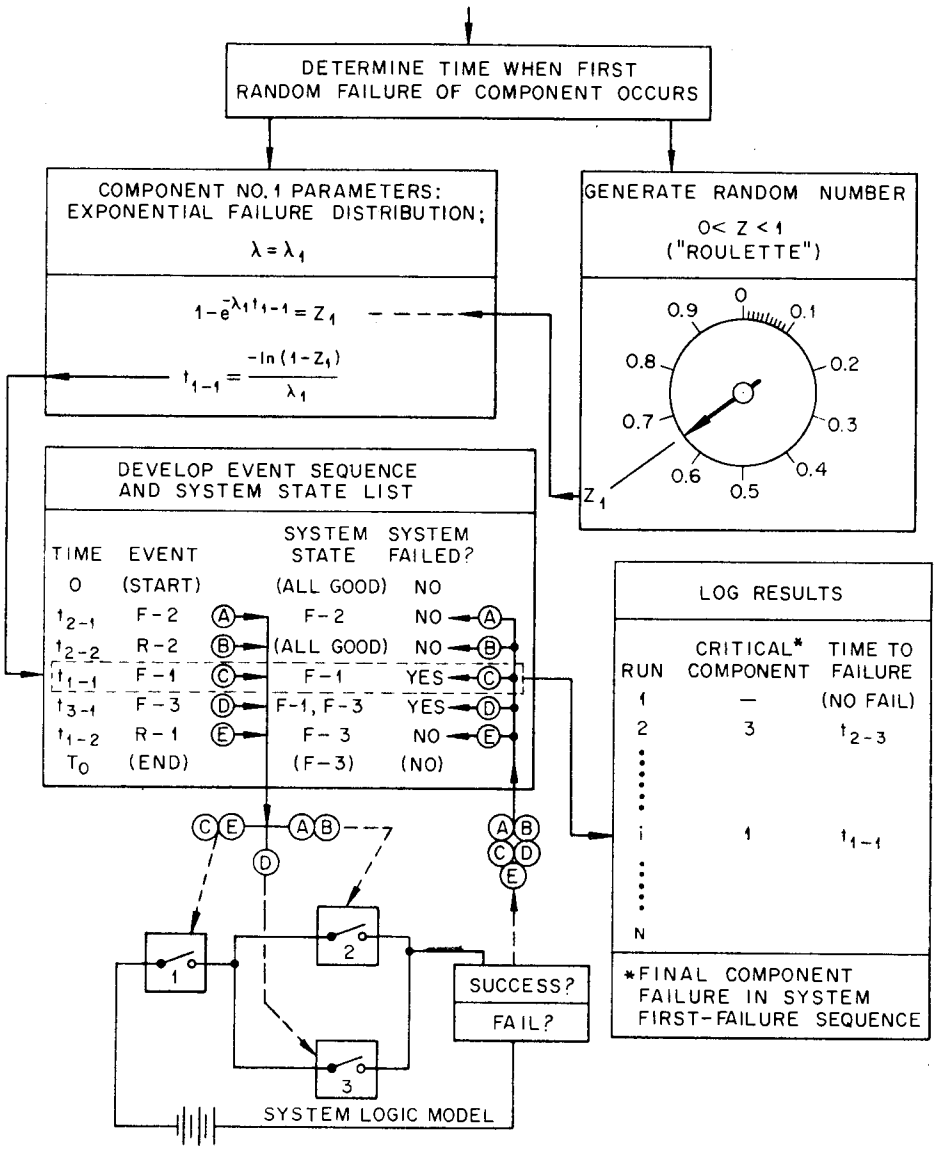


Fig. A1-1. Monte Carlo simulation.

2. Failure density function for system; i.e.,

$$\frac{d\,F_S(t)}{dt} = \left[\text{P: system is unfailed at t}\right] \left[\frac{d\,F_S(t)}{dt} : \text{for surviving systems}\right]$$

3. Cumulative probability that system has failed before $t < T_0$; i.e.,

$$F_S(T_0) \approx \frac{\left[\sum_{N\ \text{runs}} \text{number of runs in which failure occurred}\right]}{N}$$

4. Probability for each component that it is the final failure in the sequence leading to first failure of the system.

B) Potential Further Interpretations of Results:

1. From (A-1) and assuming random distribution of system failures, it is possible to calculate a system λ_S and a system MTFF by the simple relationships:

a) $F_S(T_0) = 1 - e^{-\lambda_S T_0}$

b) $(\text{MTFF})_S = \frac{1}{\lambda_S}$

However, the values thus obtained are subject to serious errors for the system with repairable components, since the system does not reach steady state. In theory, the program could be modified to approximate steady state by making $T_0 >>$ (longest MTFF for any component) and then logging only failures that occur after some initial interval.

2. From (A-3), an Average Availability (or Average Reliability) without repair over the run interval T_0 could be determined by:

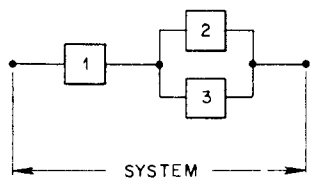
$$A \equiv \text{Average Availability} = \frac{1}{T_0} \int_{t=0}^{t=T_0} F_S(t)\,dt$$

$$\approx \frac{1}{T_0} \times \sum \frac{\left[\text{runs in which } \overline{S} \text{ occurs } \times t_{\text{system failure}}\right]}{N}$$

Note: This method, although very general and conceptually easy to follow, may require long computing runs. In situations where it is considered applicable, information for all time is obtained. The need to obtain statistically significant results means the generation of many system first times to failure, as discussed in Sect. 3.5.3.1; this difficulty is increased by the repair consideration.

1.3.2.3 Use of "Importance Sampling" to Reduce the Number of Runs Required to Obtain Statistically Significant Results from Simulations

The term "Importance Sampling" refers to the greater statistical significance of runs in which failure occurs, as compared to runs in which no failure occurs. In very reliable systems, few failures are expected; in order to improve the simulations of such systems — i.e., to reduce the number of runs required to obtain useful failure statistics — the input data are biased and the output results are suitably corrected. This is illustrated below for a simple three-component system in which all components have exponential failure distributions and none are repairable within the run interval; component 1 is assumed to be very reliable and, therefore, rarely the cause of a system failure:



The system failure state probability expression is

$$F_S(t) = F_1(t) + S_1(t)\, F_2(t)\, F_3(t) \ ,$$

which expands to

$$F_S(t) = F_1(t)\, [S_2(t)\, S_3(t) + F_2(t)\, S_3(t) + S_2(t)\, F_3(t) + F_2(t)\, F_3(t) = 1] + S_1(t)\, F_2(t)\, F_3(t)$$

Accordingly, we "expect" to observe the following system state occurrences over N runs of duration T_0 at the <u>ends</u> of the run intervals:

$$N\, \frac{F_1(T_0)\, S_2(T_0)\, S_3(T_0)}{1} = N\, (1 - e^{-\lambda_1 T_0})(e^{-\lambda_2 T_0})(e^{-\lambda_3 T_0})$$

$\approx$ number of runs ending with system in state $\overline{1}23$
(a very <u>small</u> number because λ_1 is very small)

$$N\ F_1(T_0)\ F_2(T_0)\ S_3(T_0) = N\ (1 - e^{-\lambda_1 T_0})(1 - e^{-\lambda_2 T_0})(e^{-\lambda_3 T_0})$$

$\approx$ number of runs ending with system in state $\overline{123}$ (also probably small)

$\vdots$

(other cases of $\overline{1}$, etc.)

$\vdots$

$$N\ S_1(T_0)\ F_2(T_0)\ F_3(T_0) = N(e^{-\lambda_1 T_0})(1 - e^{-\lambda_2 T_0})(1 - e^{-\lambda_3 T_0})$$

$\approx$ number of runs ending with system in state $1\overline{23}$ (statistically significant because λ_2 and λ_3 are large)

In order to increase the "Importance" of component 1 in the statistics, its failure rate is exaggerated: e.g., choose $\lambda_1' = 10\lambda_1$. Then, one representative "expected" observation is

$$N\ F_1'(T_0)\ S_2(T_0)\ S_3(T_0) = N(1 - e^{-\lambda_1' T_0})(e^{-\lambda_2 T_0})(e^{-\lambda_3 T_0})$$

$$= N(1 - e^{-10\lambda_1 T_0})(e^{-\lambda_2 T_0})(e^{-\lambda_3 T_0})$$

$\approx$ number of biased runs ending with system in state $\overline{1}23$

To "unbias" the end results, correction factors are applied wherever needed. In this case, they are simply:

$$\frac{\left[\sum_{N\ \text{runs}} \begin{array}{l}\text{observations of } \overline{1}23,\ \overline{123},\ \overline{1}\overline{23}, \text{ and } \overline{123} \text{ at the} \\ \underline{\text{ends}} \text{ of the biased runs}\end{array}\right]}{N} \times$$

$$\left[\frac{1 - e^{-\lambda_1 T_0}}{1 - e^{-10\lambda_1 T_0}}\right] \approx F_1(T_0)\ ,$$

and

$$\frac{\left[\sum_{N\ \text{runs}} \begin{array}{l}\text{observations of } 1\overline{23} \text{ at the ends of} \\ \text{the biased runs}\end{array}\right]}{N} \times$$

$$\left[\frac{e^{-\lambda_1 T_0}}{e^{-10\lambda_1 T_0}}\right] \approx S_1(T_0)\ F_2(T_0)\ F_3(T_0)\ ,$$

and similar corrections for every state expression involving component 1.

Notes:

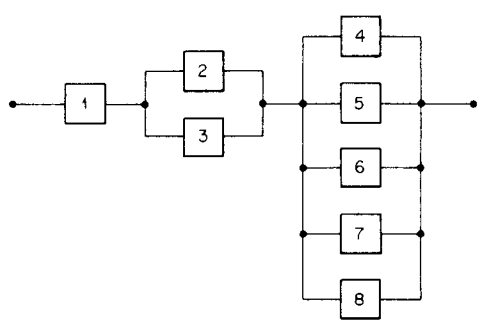
1. The above biasing-and-correction scheme is valid for observations of system states made any time after system failure, i.e., $t_{fail} < T_0$; provided the corrections are made to groups of system states, as shown. For individual states, the "premature" observations are incomplete; e.g., if component 1 fails first, it is not known what the final state of the system would be at T_0 ($\overline{1}23$, $\overline{1}\overline{2}3$, etc.).

2. It is generally impractical to use Importance Sampling in simulations whose statistical results are to form the basis for further calculated conclusions (e.g., for Average Availability) or for conclusions that depend upon event sequences (e.g., probability of System failing in one mode vs another, or System MTFF, etc.).

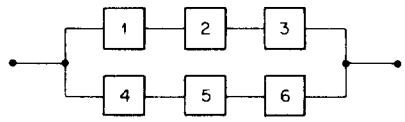
1.3.3 Monte Carlo Simulation to Identify System Failure Modes, Combined With Analytical Evaluation of Failure Mode Probabilities

Referring to Ex. 1.2.4.3, a conservative estimate of system failure probability can be obtained by summing all of the minimum cut set probabilities. Biased Monte Carlo simulations will identify the cut sets efficiently, and the remaining analytical evaluations of set probabilities are simple and straightforward. This is the basis of several recent programs, including MINCUT and "Kinetic Tree Theory."

One difficulty encountered is that the simulation does not directly identify the minimum cut sets. For example, in the following diagram one such set is $\overline{1}$. However, the simulation would identify failure sets like $\overline{6}\overline{5}1$, $\overline{7}\overline{4}\overline{2}1$, $\overline{8}\overline{3}1$, etc.:



The procedure in MINCUT to identify the critical sets is to "unfail" in succession each element of each actual failure set found by Monte Carlo. Thus, for the $\overline{7}\overline{4}\overline{2}1$ case above, the program would proceed to check whether system failure still existed with $7\overline{4}\overline{2}1$, $7\overline{4}2\overline{1}$, and $7\overline{4}\overline{2}\overline{1}$, noting $\overline{1}$ as the critical set. The following diagram shows that the elimination method determines only one critical set in situations where there may be several:



If failure was reached in progression $\overline{1} \rightarrow \overline{2} \rightarrow \overline{3} \rightarrow \overline{5}$, yielding set $\overline{1235}$, the elimination process might yield only set $\overline{35}$. Actually, sets $\overline{15}$ and $\overline{25}$ may be just as important. However, with a large number of simulations, we can generally depend on the randomness to identify all sets, even though their occurrence frequency may not be consistent with the real probabilities. It should also be apparent that other methods could be devised to identify sets by first order of arrival, but there seems no reason to do so when the sets are to be evaluated analytically.

1.4 Confidence

A brief introduction to statistical confidence was given in Section 3.8.1. Example group 1.4.1 explains some of the methods in elementary terms, and group 1.4.2 illustrates several common applications. This material is included primarily because engineers are called upon to assign significance to confidence evaluations, often without adequate understanding.

Distributions of a random variable, for example, component age at failure, are discussed in Sections 4.2.1 and 4.2.4. The mathematical expressions describing certain forms of distribution could represent ideal populations of infinite size. The existence of such a population is moot. However, a set of data, perhaps related to other prior experience or expectations, may suggest that one of the principal distributions is a good approximation, and that distribution form may then be assumed. The set of data is thus regarded as a sample from a population that has the assumed distribution form.

Each sample has statistical properties corresponding to the population properties, for example, a mean and a standard deviation, or a binomial proportion. The sample statistics can be viewed as estimates of the population properties. However, the statistics vary among samples from the same population, the amount of variation for those of interest here tending to decrease with increasing sample size. Such variations have their own frequency distributions, some of which have been described mathematically. It can be proved, for example, that the means of uniform-sized samples from a known normal population will also have a normal distribution and that the standard deviations of such samples are related to chi-squared distributions.

When the values of some characteristic of samples from a known population distribute predictably, then it can also be predicted what proportion of a large number of samples will have their statistics within any arbitrary pair of limits. The same holds for unknown populations whose

distribution form is known, except now the limits are predictable only relative to the (unknown) value of the characteristic for the population. In either case, the proportion of samples whose statistics are between limits equals the probability that the value for one random sample will be within the limit interval. This is the basis for confidence evaluations.

The practical confidence calculation concerns a sample of particular size, say n trials or data values, presumed to be from a population whose distribution form is known but whose distribution parameter value(s) are unknown. The latter are estimated by the corresponding sample statistics. A confidence level is then chosen, and the associated confidence limits, or interval, are found by methods shown in this example group. These methods exploit what is known, a priori, of the distributions of statistical properties among samples from populations whose random variable distributions are of known form. Confidence level and confidence limits then have the following significance: Repeated sampling and confidence interval (limits) calculations, all for the same sample size and same confidence level as the actual sample, will yield a percentage of the intervals that bracket the true distribution parameter value of the unknown population; that percentage equals the confidence level percent. Hence the confidence level is the probability that the confidence interval for any one random sample includes the true distribution parameter value of the population.

The remainder of the example group describes the confidence calculations. It should be emphasized that the results are largely determined by the distribution form assumed for the population. By comparing the results of examples 1.4.2.2 and 1.4.2.3 given in Table A1-2, it can be seen that different assumptions in this regard may lead to large variations in the confidence interval.

Reference is made to tabulations of areas under distribution curves, corresponding to intervals of the distributed variable and of binomial probability distribution. Condensed versions of such tables appear in many reliability texts, and expanded versions are found in Refs. 11 and 12. Use of the tables is sometimes confusing due to the different ways of expressing and arranging the data. Thus the values sometimes correspond to intervals within the stated limits, and in other tables to portions of the distribution outside the limits (e.g., area under the curve tails); the values may be expressed as percentages or fractiles of a population, or again as probabilities that a random point will or will not fall inside an interval.

1.4.1 Basis of Confidence Calculations

1.4.1.1 Confidence with Respect to the Mean of a Normally Distributed Random Variable

The discussion is introduced with some elementary considerations in probability concerning the distribution curve shown in Fig. A1-2a. In addition to being of normal form, the curve is also "normalized," that is,

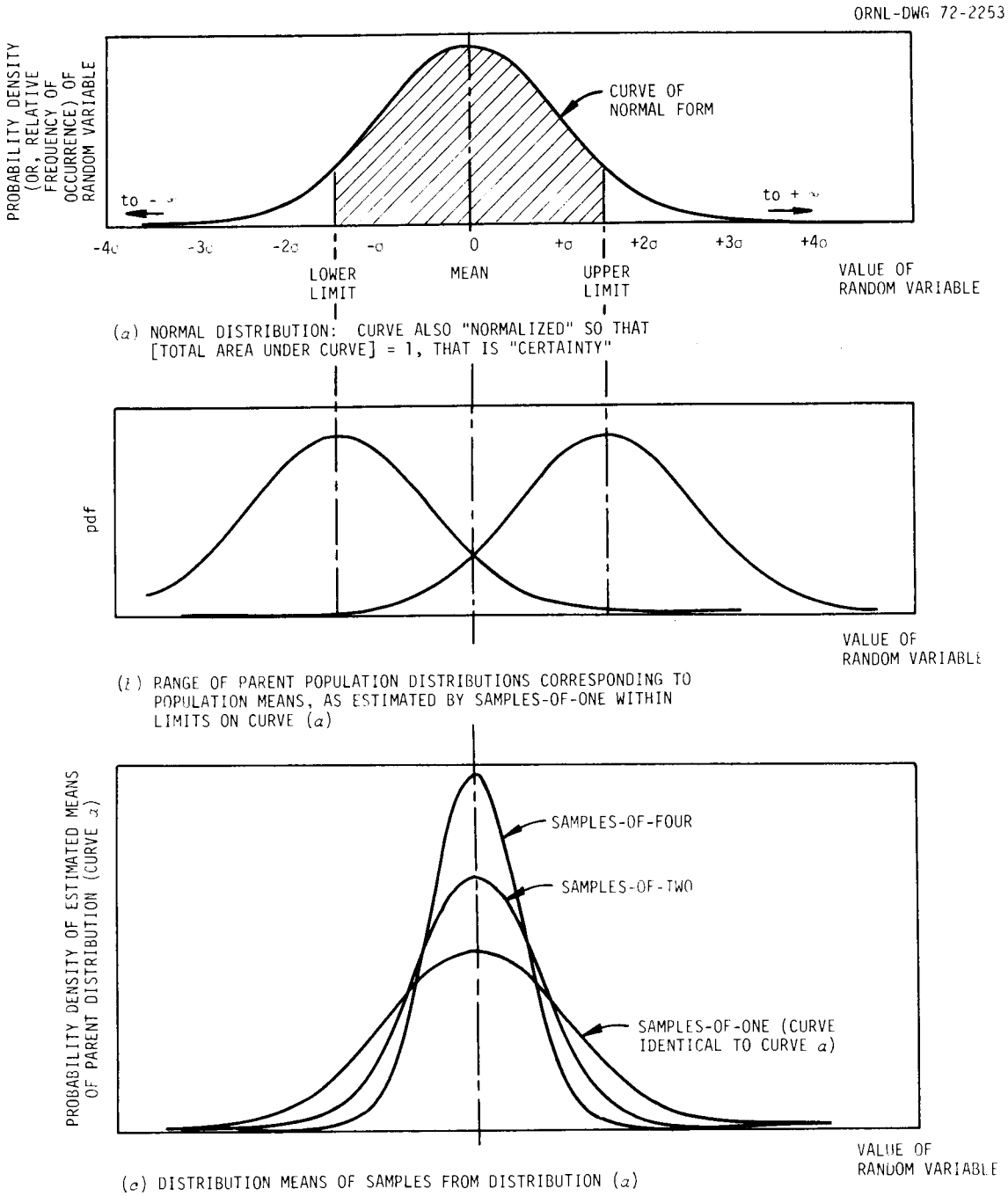


Fig. A1-2. Distribution of sample means from a normally distributed parent population.

it is a probability density plot and the total area under the curve is unity, which signifies certainty. Between any pair of limits, like those shown, the curve area then represents the portion of the total population having values of the distributed random variable in the range defined by the limits. Perhaps this variable might be a dimension deviation and the range of interest like −0.040 to −0.045 in. The probability that any one element randomly chosen from the population would have a value of the variable within the range of a pair of limits is precisely the area of the normalized curve between the limits.

Suppose next that we knew a certain population to be distributed normally, as in Fig. A1-2a, but did not know the distribution mean; that is, the curve shape and scale are known and the location in unknown. Given a sample of just one element, the best guess we could make about the location is that the observed characteristic value of the sample element is the same as the parent distribution mean value. Now we wish to establish objectively how good the guess is. In this very special case, the answer is almost obvious: If we were to take samples of one repeatedly, calling the value of each an estimate of the population mean, then the estimated means would distribute out identically as the parent distribution. And like the parent distribution, a definite proportion of these "means" would fall between any pair of arbitrary limits. Our "confidence," then, that the actual unit sample is within an arbitrary pair of "confidence limits" is analogous to the general probability that any randomly chosen element is within a corresponding interval of the parent population true distribution. As it pertains to the normal distribution, confidence is ordinarily expressed as a percentage of the total curve area that occurs between symmetrical limits about the estimated mean, but the evaluation could be made for any other interval desired.

The limits, while actually representing the distributed variable x, are usually expressed in multiples of the distribution standard deviation σ:

$$s = \sqrt{\frac{\sum_{i=1}^{i=n} (x_i - x_{mean})^2}{n-1}} \xrightarrow[n \to \infty]{} \sigma .$$

This adds greatly to the convenience in numerical evaluation of curve areas, since the area between a given pair of limits expressed in multiples of σ is the same for all normal distribution curves.

The customary interpretations of confidence have only been suggested thus far. Proceeding, we now briefly consider samples of two elements each from the same parent normally distributed population. The mean of each sample is the average of two values, and if a large number of samples of two were taken, we could expect the means to distribute out in some fashion. Evidently, this distribution should peak more sharply than the corresponding distribution for samples of one, because the individual estimates of a parent population mean are better. And it turns out that

this distribution, shown in Fig. A1-2c, is also of normal form. Intuition tells us that progressively larger samples will have increasingly sharper distribution peaks, and the mean of a very large sample should be very close to the parent population mean. The property just described qualitatively is defined precisely in the following relationship:

$$\sigma_{\substack{\text{sample means}\\ \text{distribution}}} = \frac{\sigma_{\text{parent distribution}}}{\sqrt{(n = \text{sample size})}} .$$

Since the distribution of means for samples of a particular size is normal, the confidence that any one sample of that size is within a pair of arbitrary limits is equivalent to the probability that any random point from the "population of means" is within the same limits; the numerical value again equals the area of the appropriate normal curve between the limits, in this case the means distribution curve. The virtue of large samples now becomes apparent: The proportional curve areas between pairs of limits having identical σ values is the same for all of the means curves, but the numerical values of σ in terms of the parent distribution random variable decrease with sample size as shown above. Hence, a given level of confidence is attributed to successively smaller intervals about a sample mean as the sample size increases.

All of the above arguments are qualified by the early statement that the curve scale is known. If the scale parameter, that is the σ value, is not known, any estimate of the curve location from sample data is subject to greater uncertainty. The amount of the uncertainty depends on sample size; for samples of 20 or more, the s estimate of σ is generally good enough that the error in the confidence interval about the estimated distribution mean is negligible, using the normal distribution of means just described. The latter method is illustrated in Example 1.4.2.3, including use of the tabulated areas of intervals under the normal distribution curve.

For samples smaller than 20, where it is known only that the parent distribution is normal, the confidence intervals about the sample means are determined by the Student's t distribution. Student's t is the quantity

$$t = \frac{x_{\text{sample mean}} - \mu}{s/\sqrt{n}} ,$$

in which μ is the population mean and n the sample size. Thus, many repeated samplings of size n from the same normal population would yield a particular percentage (the confidence level) of t values within any pair of limits (confidence interval) of the t distribution for that size of sample; the percentage corresponds now to that portion of the area under the t curve and between the limits. The intervals and percentages are tabulated. A simple calculation then converts the confidence interval in t to the desired interval in μ. The procedure is shown in Example 1.4.2.4.

1.4.1.2 Confidence with Respect to Standard Deviation for a Normal Population: The Chi-Square Distribution

If a normal distribution is to be described completely, its standard deviation σ must be known in addition to the mean. Estimates of σ are denoted by s and are obtained from samples as indicated earlier; again it is desirable to establish confidence in such estimates. Invoking intuition once more, it seems that the standard deviations of small samples from the same parent population should vary widely and erratically about the population true σ, and progressively larger samples should tend toward the true σ. This situation is confirmed by the actual and unique frequency distributions for different sample sizes of a quantity called "chi-square":

$$\chi^2_{(\nu)} = \sum_{i=1}^{n} \frac{(x_i - x_{mean})^2}{\sigma^2} = \frac{\nu s^2}{\sigma^2} ,$$

where ν = degrees of freedom = (sample size) $-$ 1 = n $-$ 1, and x_{mean} is the sample mean value of x. Note that for a fixed sample size, the corresponding chi-square distribution (χ^2_ν) represents in effect the relative occurrence frequencies of s^2/σ^2, which is the ratio of sample variance to parent population "variance." Typical chi-square distribution curves are shown in Fig. A1-3. Considering the total area under this curve as unity, the area between an arbitrary pair of limits must represent the probability that a random sample of size consistent with the curve (i.e., curve and sample ν are the same), drawn from any normally distributed infinite population, will have a $\nu s^2/\sigma^2$ value within the chosen limits. It follows that confidence in the s value of a sample being within arbitrary limits about the parent distribution σ is equivalent to the probability that the $\nu s^2/\sigma^2 = \chi^2_\nu$ value is within corresponding limits of the appropriate χ^2 distribution. Example 1.4.2.3 illustrates the use of the chi-square distribution area versus interval tables for this case, including the simple conversion from interval in chi-square to interval in s.

1.4.1.3 Confidence with Respect to the Mean of an Exponentially Distributed Random Variable

Much reliability work presumes the constant failure rate λ for each component or system. Age at failure for replaceable elements, or time between failures for repairable units, is then the exponentially distributed random variable of interest. Confidence is determined for an interval about a mean time to failure (MTTF) or a mean time between failures (MTBF), whichever is appropriate; by inference, the confidence interval may also be expressed in terms of λ values. A variety of procedures are available to cover different kinds of observations. Two of these are illustrated by Examples 1.4.2.1 and 1.4.2.2.

The simpler numerical example represents the case where a number of like components are all observed from startup through failure, or where

ORNL-DWG 72-2254

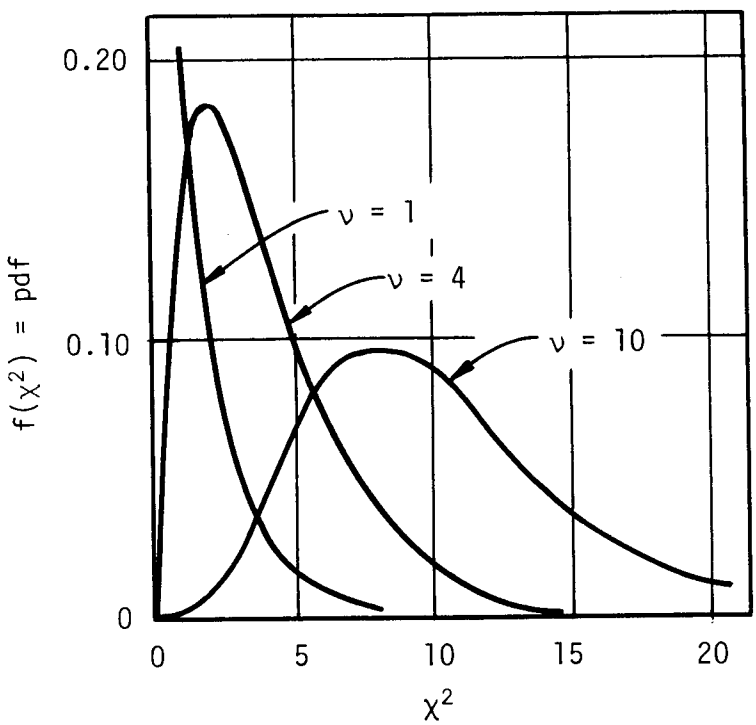


Fig. A1-3. Chi-square distribution.

a repairable system is observed over an interval that includes several failures and ends with a failure. Direct use is then made of a property of exponential distributions, namely, that the quantity

$$2r \frac{m_{sample}}{m_{population}}$$

is distributed as chi-square. Here, r is sample size and m is the value of the mean.

More generally, components are observed under test or field conditions where a number are unfailed at the end of observation period; this may be true, for instance, where failures are replaced as they occur. Confidence is then based on relationships similar to the above, but selecting chi-square distributions suitable for truncated tests. In Example 1.4.2.2, the chi-square procedure is based on the Poisson probability law for number of failures observed in a fixed time.

1.4.1.4 Confidence in Binomial Distributions

The binomial confidence evaluation can be thought of as placing arbitrary "limits of improbability" on an actual observation and then back calculating to find binomial distributions that satisfy the limits. To

illustrate the procedure, suppose a sample of four showed one defective and three good pieces. A first estimate of the parent binomial distribution then would be that p, the proportion of defectives, is 1/4 or 0.25, and q, the proportion of good pieces, is 3/4 or 0.75. The binomial expansion of probabilities for the sample size is:

p^4 (P: all 4 defective)	+	$4p^3q$ (P: 3 def., 1 good)	+	$6p^2q^2$ (P: 2 def., 2 good)	+	$4pq^3$ (P: 1 def., 3 good)	+	q^4 (P: all 4 good)	= 1

A pair of limits in p is sought corresponding to 80% "symmetrical" confidence, that is, with the uncertainty divided equally between upper and lower limits. The lower limit then is considered to be that population (i.e., p value) for which 10% of repeated samples of four would yield one or more defective; this limit should satisfy

$$p^4 + 4p^3q + 6p^2q^2 + 4pq^3 = 0.1$$

Similarly, in a population with the upper limiting value of p, 10% of the samples of four would have one or less defective, thus satisfying

$$4pq^3 + q^4 = 0.1$$

Fortunately, these calculations have all been worked out and the results made available in tables and curves. The practical formula used is that for probability of "r or more occurrences" in one sample:

$$P\,(s \geq r \mid n,p) = \sum_{s=r}^{n} \frac{n!}{s!\,(n-s)!}\, p^s\, q^{n-s}$$

where

n = sample size,
s = number of items found in state corresponding to p,
p = proportion of "p state" in main population,
q = proportion of "q state" in main population,
r = arbitrary whole number, less than n.

Binomial confidence finds application both in production sampling testing and in sequential operating tests. These produce, typically, a large number of successes and no or very few failures; the confidence interval is determined for the ratio of successes to failures, which is then regarded as the success probability.

1.4.1.5 Poisson Probabilities

Section 4.2.1.3 indicated how the Poisson distribution is a limiting case of the binomial distribution. The Poisson distribution describes the

probability of observing exactly r occurrences in time t, where the events are random and occur at some known average rate of m in time t. Accordingly, confidence intervals about sample estimates of m are determined from cumulative Poisson probabilities of r or more occurrences in time t. The method is otherwise analogous to that for the binomial confidence interval in p, and curves for the cumulative Poisson probabilities are available. Since t/m is the MTTF of interest in many observations, the Poisson probabilities offer an alternative method to the chi-square for determining confidence limits for random failure rates.

1.4.2 Examples of Confidence Calculations

1.4.2.1 Confidence Evaluation of System Mean Time between Failure (MTBF): Exponential Distribution Assumed

A system is operated for 30,000 hr, during which time it accumulates seven reportable failures. Determine the lower confidence limit (i.e., upper is then ∞) such that there is 90% confidence that MTBF is not less than the limit.

$T \equiv$ system running time

$= 30{,}000$ hr

$r \equiv$ number of failure accumulated

$= 7$

$\hat{m} \equiv$ estimate of MTBF

$= T/r$

$= 4286$ hr

$C_L \equiv$ lower confidence limit

$$= \frac{2r\hat{m}}{\chi^2\ (0.10,\ 2r)}$$

[χ^2 (0.10, 14) stands for: a) The particular χ^2 distribution for samples with 14 degrees of freedom (see Fig. A1-3). b) The particular value of χ^2 on the above distribution about which 90% of the χ^2 values are smaller and 10% are larger.]

From tables:

$\chi^2\ (0.10,\ 14) = 21.064$

$$C_L = \frac{2 \times 7 \times 4286}{21.064} = 2840 \text{ hr}$$

1.4.2.2 Confidence Evaluation of Component Mean Time to Failure (MTTF): Exponential Distribution Assumed

Four redundant safety channels each have one unit of a particular device. Any failure of one of these devices is annunciated, and the device can be replaced on line in a very short time. The system has operated the equivalent of over five years continuous, and it is desired to assess the MTTF of the device class. The experience was as shown in Table A1-1.

Assume all failures are "random," that is, there are no known wear-out mechanisms or other factors to the contrary. Determine a symmetrical

Table A1-1. Component Failure Data for Examples 1.4.2.2—1.4.2.4

1	2	3	4	5
Event No.	Time Elapsed Since Initial Startup (hr)	Failure Channel (A, B, C, or D)	Order of Failure in Channel (e.g., 1st, 2d, etc.)	Device Operating Time to Failure (hr)
	(0)	(all new)		
1	303	B	1	303
2	3,996	C	1	3,996
3	4,784	A	1	4,784
4	9,613	C	2	5,617
5	10,524	B	2	10,221
6	11,078	D	1	11,078
7	12,781	A	2	7,997
8	12,946	A	3	165
9	14,632	C	3	5,019
10	16,663	B	3	6,139
11	17,821	D	2	6,743
12	20,505	A	4	7,559
13	21,374	C	4	6,742
14	26,933	A	5	6,428
15	28,260	C	5	6,886
16	28,711	B	4	12,048
17	28,792	D	3	10,971
18	32,626	A	6	5,693
19	36,710	D	4	7,918
20	37,087	C	6	8,827
21	38,546	B	5	9,835
22	39,539	A	7	6,913
23	44,088	D	5	7,378
24	44,407 (terminate observation)	C	7	7,320

90% confidence interval about the MTTF, based on chi-square distribution of the MTTF for samples from a parent exponential distribution of the MTTF.

Regard the experience as the equivalent of a test with a "fixed truncation time," and in which each failure is replaced. (See Ex. 1, p. 175, Ref. 6.)

$n \equiv$ number of devices placed on test at time $t = 0$

$= 4$

$t^* \equiv$ time at which life test is terminated

$= 44{,}407$ hr

$\theta \equiv$ mean life, or MTTF

$r \equiv$ number of failures accumulated to time t^*

$= 24$

$1 - \alpha \equiv$ confidence level

$= 0.9$ for this example, or 90%

$\alpha \equiv$ acceptable risk of error

$= 0.1$, or 10%

$T = nt^*$

$T = 4 \times 44{,}407$

$= 177{,}628$ hr

$\hat{\theta} \equiv$ mean life estimate, nt^*/r

$$\hat{\theta} = \frac{4 \times 44{,}407}{24}$$

$= 7401$ hr.

$$\text{Confidence interval} = \left[\frac{2T}{\chi^2\left(1 - \frac{\alpha}{2}, 2r\right)}, \frac{2T}{\chi^2\left(\frac{\alpha}{2}, 2r + 2\right)}\right]$$

From tables:

$\chi^2\ (0.05, 50) = 34.8$

$\chi^2\ (0.95, 48) = 65.1$

$$\frac{2T}{\chi^2\ (0.05, 50)} = \frac{2 \times 177{,}628}{34.8} = 10{,}200$$

$$\frac{2T}{\chi^2\ (0.95, 48)} = \frac{2 \times 177{,}628}{65.1} = 5{,}450$$

90% confidence interval for MTTF is

<u>5,450</u> to <u>10,200</u> hr

1.4.2.3 Confidence Evaluation of Component MTTF and Standard Deviation: Normal Distribution Assumed

The problem background is the same as in Example 1.4.2.2, and the data are from Table A1-1. The data again suggest that of a truncated test, that is, one cut off at a specific time before the last element has failed. There are methods for treating the truncated test problem (see Ref. 2, p. 233), but the fact of several unfailed devices left at the end of the test complicates the problem greatly. Noting that the remaining devices in this case (i.e., in channels A, B, and D) have operated long enough to rule out premature failures, it seems reasonable to ignore the survivors and analyze only the actual failure data.

Proceeding on the latter basis, a 90% confidence interval for the mean is determined by areas under the normal curve tails as follows:

$\hat{\theta} \equiv$ mean time to failure estimate, or estimate of μ for population

$= \overline{X}$

= average of column 5, Table A1-1

= 6941 hr

$s \equiv$ standard deviation of sample

$$= \sqrt{\sum_{i=1}^{i=24} \frac{(X_i - \overline{X})^2}{n-1}}$$

where n = sample size and X_i = time to failure of component i

s = 2920.

From tables:

$$\begin{bmatrix}\text{area under} \\ \text{one curve tail}\end{bmatrix} = 0.05 \times \begin{bmatrix}\text{total area} \\ \text{under curve}\end{bmatrix},$$

when tail proceeds from a point ±1.645 standard deviations displaced from curve midpoint (mean).

Population mean at 90% confidence

$$= \text{sample mean} \pm \frac{1.645\ s}{\sqrt{n}}$$

$$= 6941 \pm \frac{1.645 \times 2920}{\sqrt{24}}$$

$$= 6941 \pm 980$$

A 90% confidence interval for the standard deviation σ is determined from the chi-square distribution curve areas as follows:

$$\nu = n - 1 = 24-1 = 23;\ \chi^2\ (0.05,\ 23) = 13.10;\ \chi^2\ (0.95,\ 23) = 35.16$$

$$\sigma_{\text{upper limit}} = \sqrt{\frac{\nu s^2}{\chi^2\ (0.05,\ 23)}}$$

$$= \sqrt{\frac{23 \times 8.53 \times 10^6}{13.10}} = 3865$$

$$\sigma_{\text{lower limit}} = \sqrt{\frac{\nu s^2}{\chi^2\ (0.95,\ 23)}}$$

$$= \sqrt{\frac{23 \times 8.53 \times 10^6}{35.16}} = 2360$$

Population standard deviation at 90% confidence is interval between 2360 and 3865 hr.

1.4.2.4 Confidence Evaluation of Component MTTF: Small Sample; Normal Distribution Assumed

The problem is the same as for Example 1.4.2.3, except that the sample is now limited to the first ten data points of Table A1-1. No points are excluded, or censored, although events 1 and 8 suggest premature failure.

A 90% confidence interval for the mean is determined from the Student's t distribution curve areas as follows:

$\alpha \equiv$ probability of a larger absolute value of t

$= 1 - \text{confidence}$

$= 1 - 0.9$

$= 0.1$

From tables, t for sample size 10 is value for $n - 1 = 9$ degrees of freedom:

$$t\ (0.1,\ 9) = 1.833$$

Population mean at 90% confidence

$$= \text{sample mean} \pm \frac{ts}{\sqrt{n}}$$

$$= 5532 \pm \left[\frac{1.833 \times 3625}{\sqrt{10}}\right]$$

$$= 5532 \pm 2100$$

(Sample mean and standard deviation obtained as in Ex. 1.4.2.3, but for first ten data points only.)

Note: To assume the normal distribution for these particular data is questionable, since the sample mean and standard deviation range suggest that the population could include many negative values of time to failure. Other distributions should be better suited to the data.

Table A1-2. Comparison of Confidence Intervals for Population Mean Values, 90% Confidence

Data from Table A1-1

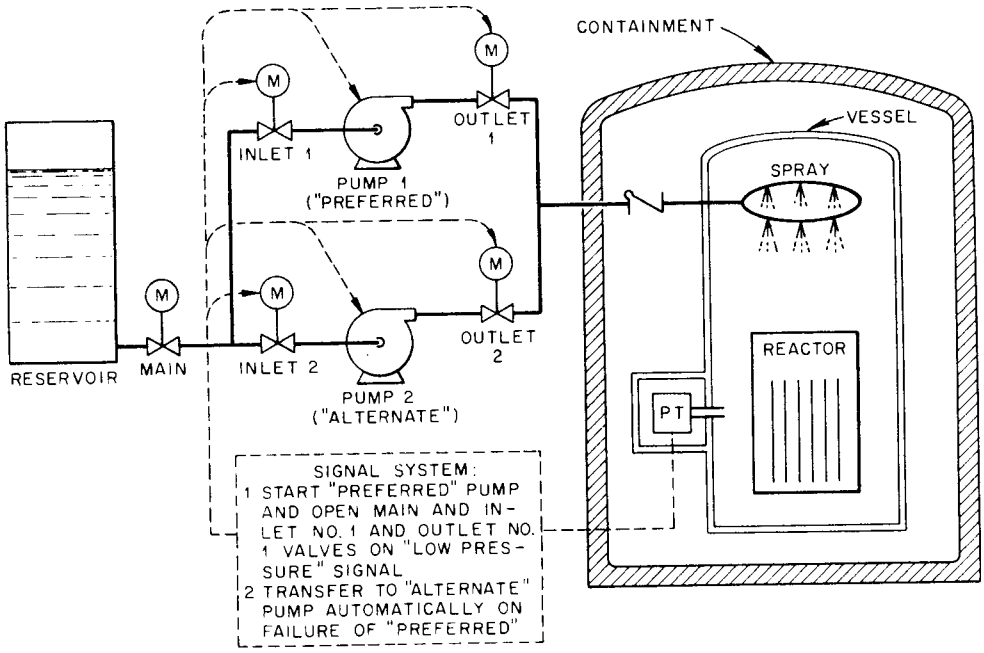
Problem Treatment	Lower Limit for 90% Confidence (hr)	Upper Limit for 90% Confidence (hr)
Ex. 1.4.2.2: exponential distribution, 24-point sample	5,450	10,200
Ex. 1.4.2.3: normal distribution, 24-point sample	5,961	7,921
Ex. 1.4.2.4: normal distribution, 10-point sample	3,432	7,632
Same as Ex. 1.4.2.4, but 2 points censored to give an 8-point sample[a]	5,096	8,616
Same sample as Ex. 1.4.2.4, but exponential distribution of 10-point sample[a]	3,940	12,300

[a]Calculations not shown.

Part 2: Practical System Analysis Exercise

2.1 Basis System and Reliability Problem Statements

2.1.1 Function Diagram for System Conceptual Design: Core Spray System



2.1.2 System Performance Objective

The spray system must start when the reactor pressure falls below a set-point value and then run for 1 hr; demand may occur at any time in a reactor operating cycle of 10,000 hr.

2.1.3 System Reliability Problem Statement

The principal "reliability" figure of merit in this problem is the probability as a function of time that the spray system would start on demand and complete 1 hr of operation. A second factor of interest is the same probability averaged over one operating cycle of the reactor.

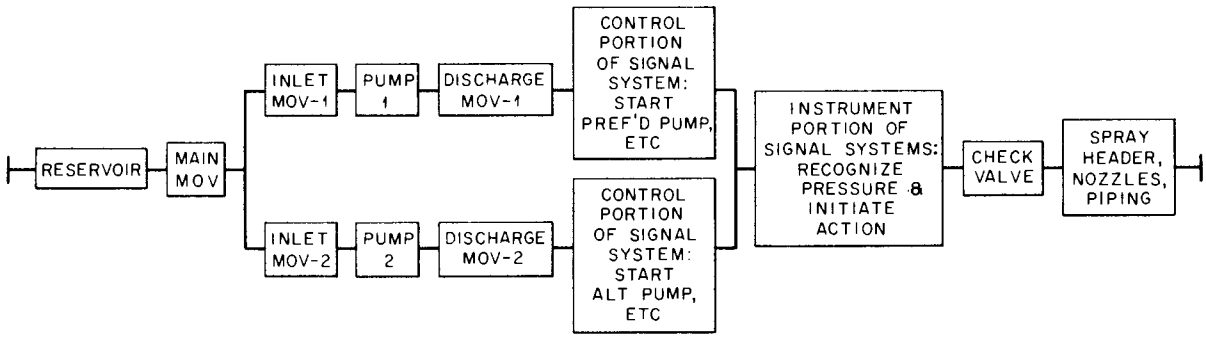
2.2 "Simple" Reliability Analysis Formulation for System Conceptual Design

2.2.1 Basic Assumptions and Method

The simplest form of system problem, mathematically, is an array of components functionally connected in series and parallel, etc., and each characterized by a constant failure rate (i.e., exponential failure distribution) over the entire interval of interest. Accordingly, and wherever reasonable, the data are manipulated toward this

form. Where this form is unrealistic, it is attempted to assign values to the parameters such that the results will always be more conservative than for the rigorous mathematical analysis.

2.2.2 Analysis Block Diagram, or Model



2.2.3 Data Input and Adaptation

2.2.3.1 Numerical values below are not from any actual data but are intended merely to illustrate typical ways in which data banks summarize information

a) Reservoir: no data expected
b) Motor-operated valve:
   valve body and parts subject to full stress,
   2×10^{-5} failure/hr
   operator mechanisms, 1 failure/1000 cycles
c) Pump, centrifugal, including motor and starter:
   1×10^{-4} failure/hr in operation
d) Control portion of signal system:
   (estimate might be based on assumed parts count of relays, etc.; for the present, use 1 failure/500 cycles for each matrix)
e) Instrument portion of signal system:
   (estimate might be based on experience with instrument channels of same general category; for the present, use 1×10^{-4} failure/hr)
f) Check valve: 1×10^{-5} failure/hr
g) Spray header and nozzles: no data expected

2.2.3.2 Problem Interpretations of Components Failure Data

a) Reservoir: assume "perfect" reliability, or $\lambda = 0$ and $R(t) = 1$
b) Main motor-operated valve:
   Consider valve body and parts as being subject to full stress during entire interval of reactor operating cycle; accordingly, use basic data directly:

$$R(t) = e^{-(2 \times 10^{-5})t}.$$

The motor operator mechanism is required to operate just once if there is a demand for system operation. Since the reliability is a function of cycles rather than time, it is appropriate to express the failure probability as a constant instead of an exponential function of time, <u>for any one reactor operating interval</u>:

$$R(t) = (\text{constant}) = 0.999.$$

c) Components in redundant pump legs:

Each element of leg 1 ("preferred") is on standby until the system is called upon and then is expected to operate for one cycle or 1 hr. Each element of leg 2 ("alternate") is on standby until, first, the system is called upon and, second, leg 1 fails. To represent this situation rigorously would require the complex expressions for standby, as shown in Example 1.2.2.3. The following simplifying assumptions shall be made, perhaps because the problem is to be executed on a computer that is not programmed for anything more complex. Assume that all valve bodies and parts are continuously subject to full stress; actually, they are isolated by the main valve and (partially) by the check valve, so that they should be lightly stressed during standby:

$$R(t) = e^{-(2 \times 10^{-5})t}, \text{ each valve.}$$

If leg 1 functions correctly, its valves need operate just once to open. If leg 1 fails, at least one of its valves must close to prevent recycle of leg 2 pumpage, and both of the leg 2 valves must open to permit flow. A "conservative" simplification would be to assume that each valve must operate twice upon system demand:

$$R(t) = (\text{constant}) = 0.998, \text{ each valve.}$$

Although the pumps are in standby, assume they have failure rates the same as in continuous service. In addition, introduce another factor from "judgment" to reflect the possibility of pump failure on startup, noting that service reliability would be (unrealistically) perfect at the beginning of a reactor operating cycle:

$$R(t) = e^{-(1 \times 10^{-4})t} \times 0.995, \text{ each pump.}$$

Use value of controls reliability as originally estimated:

$$R(t) = 0.998, \text{ each leg.}$$

d) Instruments (as originally estimated):

$$R(t) = e^{-(1 \times 10^{-4})t}$$

e) Check valve (as originally estimated):

$$R(t) = e^{-(1 \times 10^{-5})t}$$

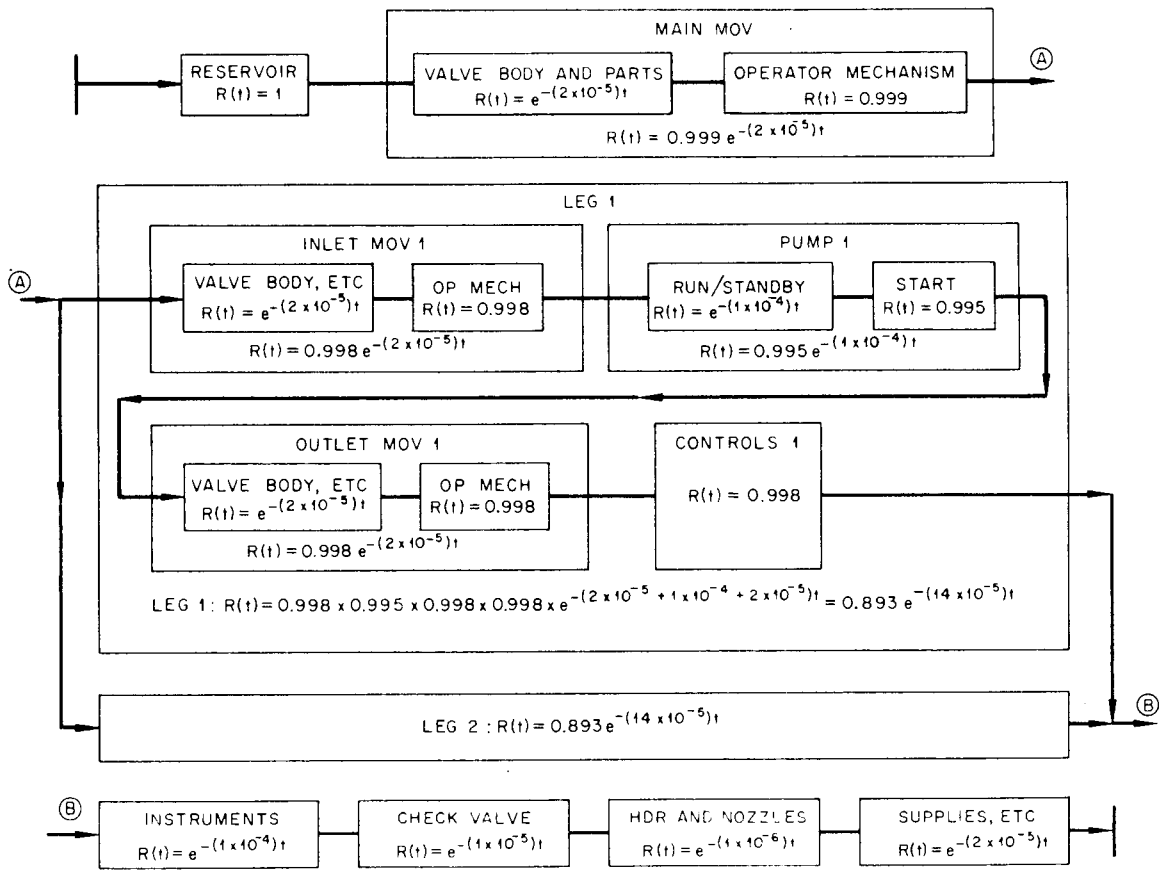
f) Spray header and nozzles: Since no data are available, a reliability design preliminary objective may be assumed. Use

$$R(t) = e^{-(1 \times 10^{-6})t}.$$

g) Power supplies, lube oil, instrument air, etc: Reliability estimates for these subsystems might be developed by separate studies. Here, however, a lumped design objective is used:

$$R(t) = e^{-(2 \times 10^{-5})t}.$$

2.2.4 Calculation of System Reliability



R(t): legs 1 & 2 in parallel

$$= 2 \times \left[0.893e^{-(14 \times 10^{-5})t}\right] - \left[0.893e^{-(14 \times 10^{-5})t}\right]^2$$

$$= 1.786e^{-(14 \times 10^{-5})t} - 0.893e^{-(28 \times 10^{-5})t}$$

R(t): system

$$= \left[1\right] \times \left[0.999e^{-(2 \times 10^{-5})t}\right] \times \left[1.786e^{-(14 \times 10^{-5})t} - 0.893e^{-(28 \times 10^{-5})t}\right] \times \left[e^{-(1 \times 10^{-4})t}\right] \times \left[e^{-(1 \times 10^{-5})t}\right]$$

$$\times \left[e^{-(1 \times 10^{-6})t}\right] \times \left[e^{-(2 \times 10^{-5})t}\right]$$

$$= 1.78e^{-(29.1 \times 10^{-5})t} - 0.892e^{-(43.1 \times 10^{-5})t}$$

Average R of system over reactor cycle of 10,000 hr

$$= \frac{1}{10,000} \int_{t=0}^{t=10,000} [R(t) : \text{system}]\, dt$$

$$= \frac{1.78}{10,000} \left[\frac{-10^5}{29.1} \left(e^{-2.91} - 1\right)\right] - \frac{0.892}{10,000} \left[\frac{-10^5}{43.1} \left(e^{-4.31} - 1\right)\right]$$

$$= 0.374$$

2.2.5 Assessment of "Simple" Reliability Analysis

a) From the numerical results it is concluded that the system is unreliable.

b) From inspection of the model it is evident that major improvements can be obtained from added redundance of the instruments, the check valve, and/or the main MOV.

c) If the parallel pump legs had been a major source of unreliability, it might be worth while to redo the problem more realistically, that is, develop a more rigorous standby model.

d) Similarly, if the results of this analysis were to be compared with the results for other configurations, it would be necessary to treat the problem more rigorously.

2.2.6 Additional Refinements

a) Sensitivity analysis: By varying the failure rate parameters one at a time, it can be determined where reliability improvements have the most effect at least cost. For example, changing the "instrument" reliability from

$$e^{-(1 \times 10^{-4})t} \text{ to } e^{-(1 \times 10^{-6})t}$$

improves the average system reliability from 0.374 to 0.532.

b) Testing: An improvement in system average reliability equivalent to the above can be obtained with the less reliable instruments if they are tested at intervals of 200 hr.

2.3 Failure Mode and Effect Analysis (FMEA)

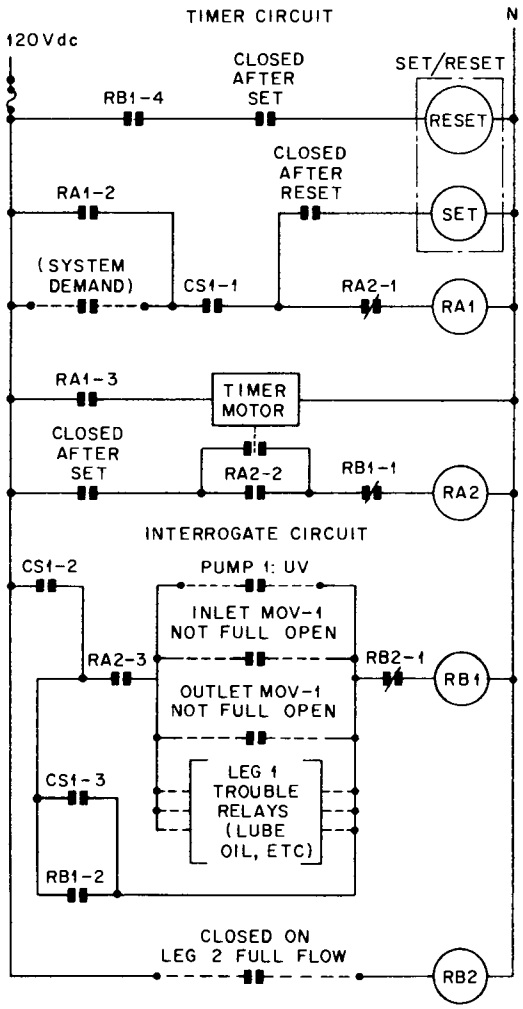
2.3.1 FMEA for One Component of Conceptual Design (Note: Content of this analysis is intended for comparison with material of following example, which treats FMEA of corresponding detailed design.)

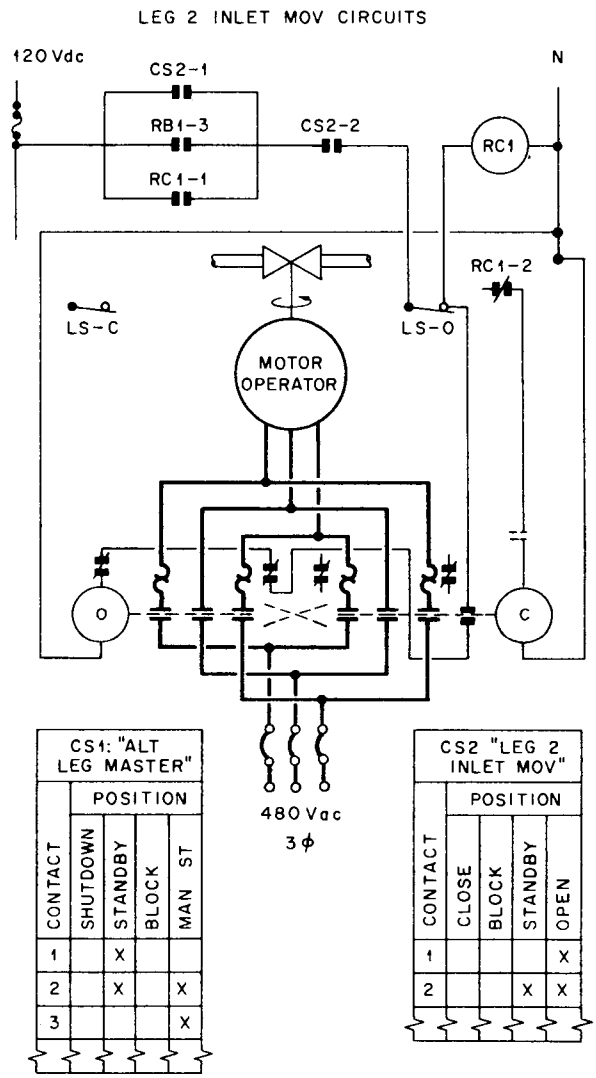
Item Identification	Failure Mode and Possible Causes	Probability Category: X = Possible O = Unlikely	Effect on System	Required Response to Compensate, and Comments
Control portion of signal system	1. Fail to initiate pump start or opening of either valve in "pref'd" leg	X	Preferred leg disabled	System design must provide for recognition of pref'd. leg failure and automatic initiation of alt. leg operation, and/or provide opportunity for operator to correct situation manually
	2. Fail to initiate pump start or opening of either valve in "alternate" leg — following failure of pref'd. leg	X	System fails	System design should provide opportunity for operator to correct situation manually (Note: this leg is the second line of defense)
	3. Fail to initiate closure of pref'd. leg valves following failure of pref'd. leg	X	If net result of both failures is that both valves in pref'd. leg remain fully or partially open, system is failed or degraded due to recirculation of alt. leg output	System design should provide opportunity for operator to correct situation manually
	4. Inadvertent initiation of system operation	X	Reactor shutdown and subsequent cleanup of boron	System design should provide redundant means to prevent accidental operation (economic)
	5. Inadvertent opening of both valves in one leg plus main block valve; no pumps operating	O	Depend entirely on check valve to prevent primary system blowdown	System design should provide independence of valve control circuits to ensure against this
	6. Fail to initiate opening of main block valve	X	System fails	Modify design to provide redundant valve
	7. False signal initiates transfer from pref'd. to alt. leg	X	Transfer to alt. leg	Alt. leg must operate; design should permit operator to restore pref'd. leg to service if alt. leg fails
	(Etc.)			

2.3.2 Failure Mode and Effect Analysis — Detailed: For Automatic Transfer to Alt. Leg

2.3.2.1 Scheme: When system is called upon, preferred leg attempts to operate. At the same instant, the timer circuit is energized and proceeds to time out. At the end of its interval, it makes up a circuit that interrogates the preferred leg components; if any of these are not indicating correct operation, the final control circuitry initiates concurrent startup of the alternate leg and shutdown of the preferred leg. Manual controls can initiate or block actions.

2.3.2.2 Circuits





2.3.2.3 Detailed Failure and Effect Analysis for Portion of Automatic Transfer Control

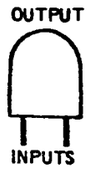
Item Identification	Failure Modes and Possible Causes	Probability Category: X = Possible O = Unlikely	Effect on System	Required Response to Compensate, and Comments
	Control Portion of Signal System			
	(A) Automatic initiation of alternate pump leg operation			
1) Timer circuit	1-1)[1] Fails to time out or develop output response (i.e., energize RA2)		1-1) In conjunction with pref'd. leg failure, prevents automatic transfer to alt. leg. Transfer can still be effected by manual controls: CS1 for master control or individual element controls (CS2, etc.)	1-1) Manual control by operator; if this is too slow, consider redundant timer circuit
	a) Control power fails*	X		a) ---
	b) "System Demand" contact does not make up*	X		b) ---
	c) Relay RA1 coil fails*	X		c) Consider reversing aspect of RA1 so that it is "fail-safe" (risk leg 2 false start)
	d) Relay RA1 contact 3 hangs open*	O		
	e) Relay RA2 coil fails	X		
	f) Set/Reset relay stays in "Reset"	X		
	g) Timer motor fails	X		
	h) Relay RB1 contact hangs open	O		
	. . .			. . .
	x) Operator error: CS1 not in "standby"	X		x) CS1 spring-return to standby position
	1-2)[2] Delivers false output signal when there is no demand for spray		1-2) Alt. leg valves open and pump starts: pump operates against blocked inlet (main MOV) and outlet (pressure > pump characteristic), and could sustain damage	1-2) Consider adding annunciator to indicate alt. leg start
	a) System demand contact jarred or vibrated closed	X		
	b) Short circuit around "Set" and RA2-2 contacts in RA2 coil circuit	O		
	c) RA1 relay jarred or vibrated closed	X		
	1-3)[3] Delivers premature output signal when there is a demand for spray		1-3) Pref'd. leg startup aborted; alt. leg startup initiated. Overall system response delayed and automatic operation of system depends entirely on alt. leg reliability	1-3) Manual correction by operator, if desired
	a) Timer contacts improperly set	X		
	b) Timer was interrupted in mid-cycle during test and not reset	X		b) Select timer with automatic (spring) return-to-start feature
	c) RA2-3 contact jarred or vibrated closed before pref'd. leg valves completely opened	O		

2) Interrogate circuit (similar development)
3) Inlet MOV-2 control circuit (")
4) Outlet MOV-2 control circuit (")
5) Pump motor control circuit (")

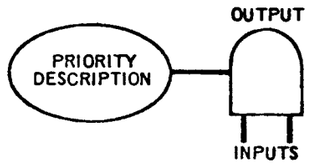
Notes:

*Shown on Fault Tree, Ex. 2.4.2
1. Could also follow from item 3, Ex. 2.3.1
2. Could also follow from item 4, Ex. 2.3.1
3. Could follow from item 7, Ex. 2.3.1

LOGIC OPERATIONS:

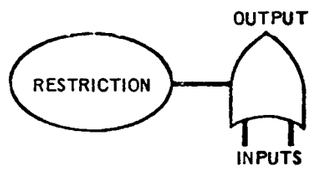


THE **AND GATE** DESCRIBES THE LOGICAL OPERATION WHEREBY THE COEXISTENCE OF ALL INPUT EVENTS ARE REQUIRED TO PRODUCE THE OUTPUT EVENT.

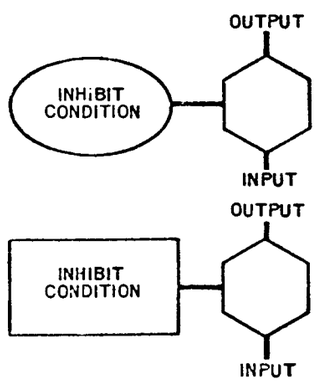


THE **PRIORITY AND GATE** PERFORMS THE SAME LOGIC FUNCTION AS THE **AND GATE** WITH THE ADDITIONAL STIPULATION THAT SEQUENCE AS WELL AS COEXISTENCE IS REQUIRED.

THE **AND/OR GATE** DEFINES THE SITUATION WHEREBY THE OUTPUT EVENT WILL EXIST IF ANY OR ALL OF THE INPUT EVENTS IS PRESENT.

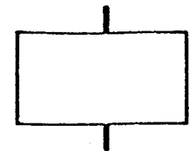


THE PRIORITY **EXCLUSIVE OR GATE** FUNCTIONS AS AN **OR GATE** WITH THE RESTRICTION THAT SPECIFIED INPUTS CANNOT CO-EXIST.



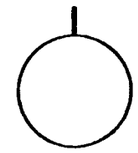
THE **INHIBIT GATES** DESCRIBE A CAUSAL RELATIONSHIP BETWEEN ONE FAULT AND ANOTHER. THE INPUT EVENT DIRECTLY PRODUCES THE OUTPUT EVENT IF THE INDICATED CONDITION IS SATISFIED. THE CONDITIONAL INPUT DEFINES A STATE OF THE SYSTEM THAT PERMITS THE FAULT SEQUENCE TO OCCUR, AND MAY BE EITHER NORMAL TO THE SYSTEM OR BE THE RESULT OF EQUIPMENT FAILURES. IT IS REPRESENTED BY AN OVAL IF IT DESCRIBES A SPECIFIC FAILURE MODE, OR A RECTANGLE IF IT DESCRIBES A CONDITION WHICH MAY EXIST FOR THE LIFE OF THE SYSTEM. COULD CONTAIN PROBABILITY NUMBERS WHICH ARE EITHER INHERENT TO SYSTEM OR ARE FUNCTION OF EFFECTS.

EVENT PRESENTATION:

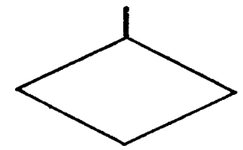


THE **RECTANGLE** IDENTIFIES AN EVENT, USUALLY A MALFUNCTION, THAT RESULTS FROM THE COMBINATION OF FAULT EVENTS THROUGH THE LOGIC GATES.

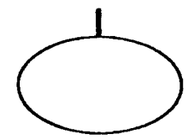
THE **RECTANGLE** IS ALSO USED TO DESCRIBE CONDITIONAL INPUTS TO **INHIBIT GATES**. IT INDICATES A CONDITION THAT IS PRESUMED TO EXIST FOR LIFE OF THE SYSTEM.



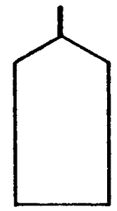
THE **CIRCLE** DESCRIBES A BASIC FAULT EVENT THAT REQUIRES NO FURTHER DEVELOPMENT. THIS CATEGORY INCLUDES COMPONENT FAILURES WHOSE FREQUENCY AND MODE OF FAILURE ARE DERIVED THROUGH LABORATORY TESTING.



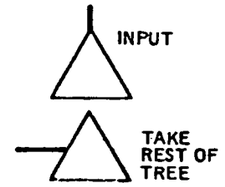
THE **DIAMOND** DESCRIBES A FAULT EVENT THAT IS CONSIDERED BASIC IN A GIVEN FAULT TREE; HOWEVER, THE CAUSES OF THE EVENT HAVE NOT BEEN DEVELOPED EITHER BECAUSE THE EVENT IS A INSUFFICIENT CONSEQUENCE OR THE NECESSARY INFORMATION IS UNAVAILABLE.



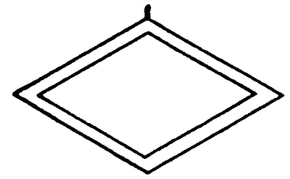
THE **OVAL** IS USED TO RECORD THE CONDITIONAL INPUT TO AN INHIBIT GATE. IT DEFINES IN STATE OF THE SYSTEM THAT PERMITS AN EVENT SEQUENCE TO OCCUR, AND MAY BE EITHER NORMAL TO THE SYSTEM OR BE THE RESULT OF EQUIPMENT FAILURES.



THE **HOUSE** INDICATES AN EVENT THAT IS NORMALLY EXPECTED TO OCCUR. FOR EXAMPLE, IT MAY BE USED TO REPRESENT THE EVENT, "TIMING PULSES PRESENT." USED STRICTLY FOR DESCRIPTION (i.e., WHAT IS GOING ON? ..IN GROUND RULES OF EFFECTS.)



THE **TRIANGLES** INDICATE TRANSFER SYMBOLS. A LINE FROM THE APEX OF THE TRIANGLES DENOTES A TRANSFER-IN AND A LINE FROM THE SIDE DENOTES A TRANSFER-OUT. REFERS TO A WHOLE SUB-FAULT-TREE REPEATED ELSEWHERE.

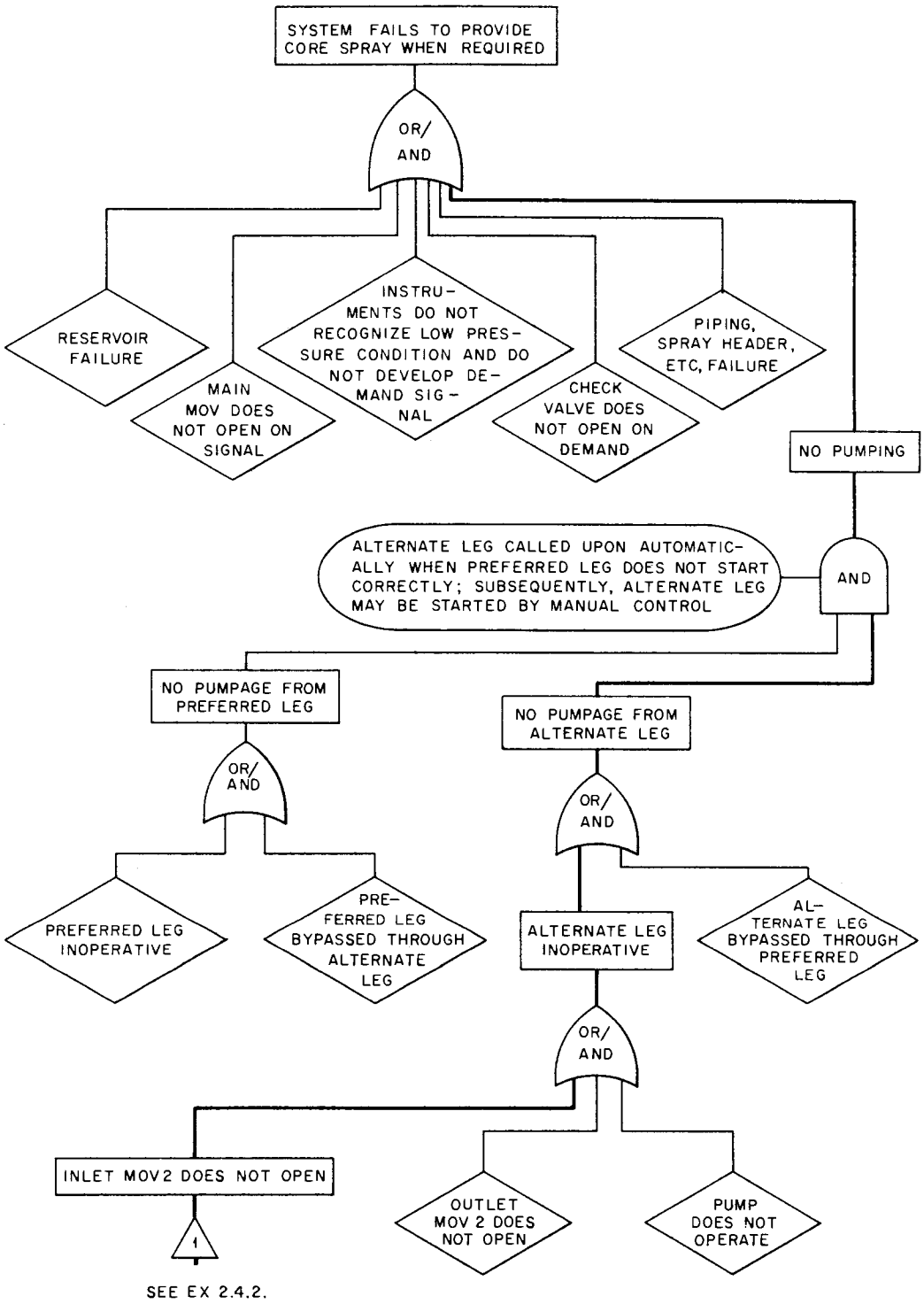


THE **DOUBLE DIAMOND** IS USED IN THE SIMPLIFICATION OF THE FAULT TREE FOR NUMERICAL EVALUATION. THE EVENT DESCRIBED RESULTS FROM CAUSES THAT HAVE BEEN DEVELOPED BUT ARE NOT SHOWN ON A PARTICULAR VERSION OF THE FAULT TREE.

Fig. A2-1. Standardized symbols and symbol definition for fault tree construction.

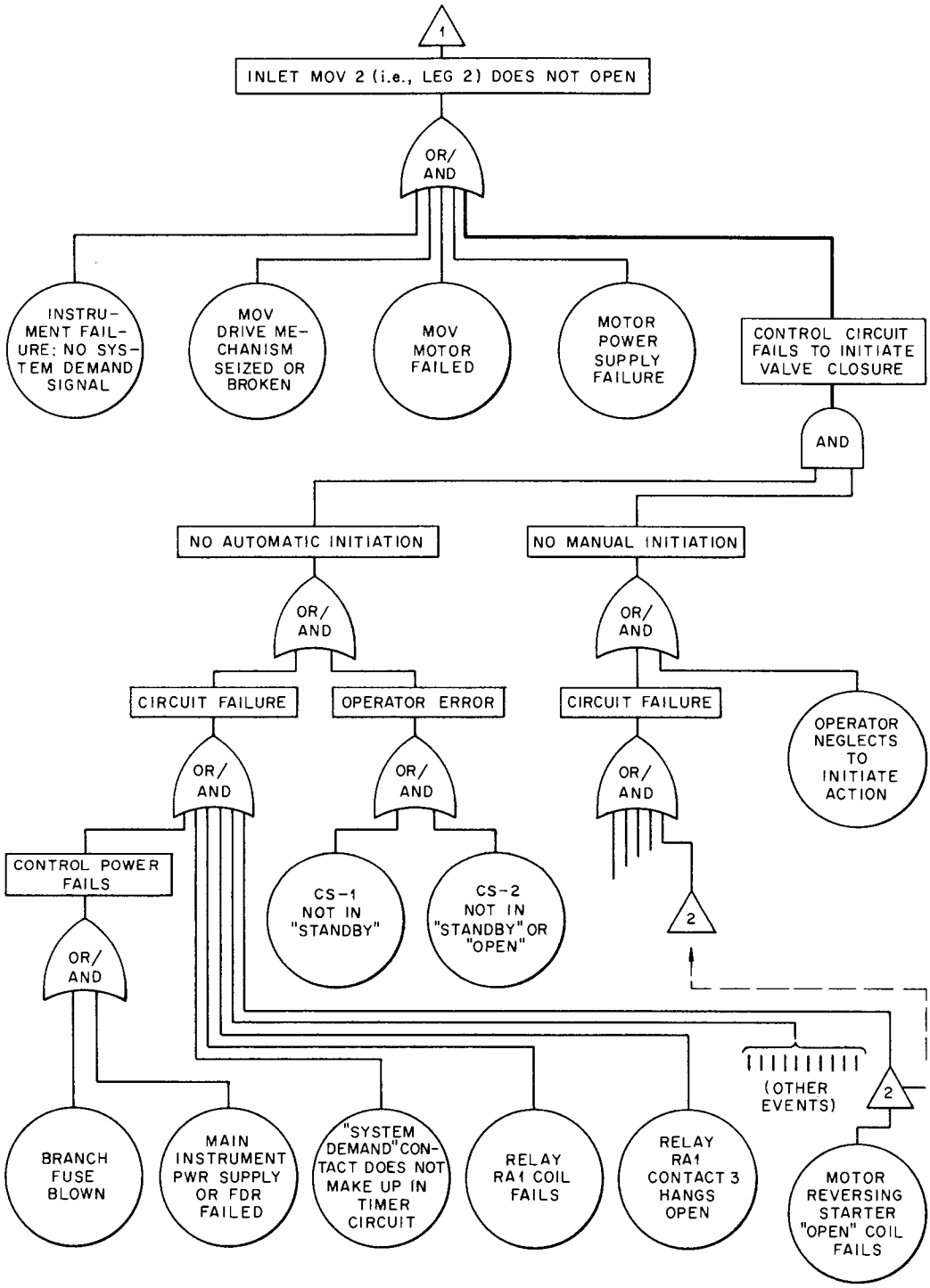
2.4 Fault Tree

2.4.1 Fault Tree for "Gross" Events

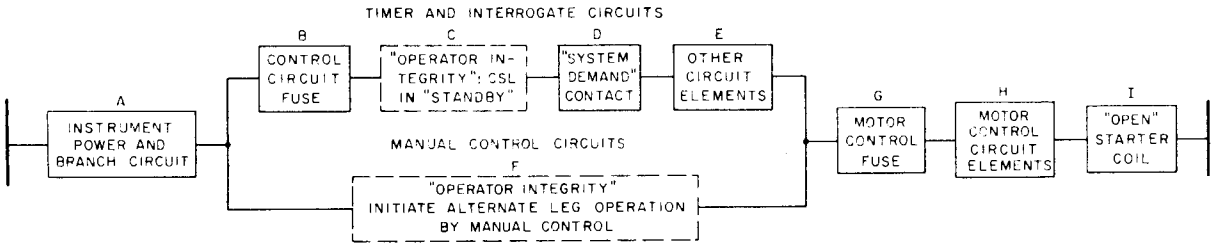


SEE EX 2.4.2.

2.4.2 Fault Tree for "Fine Structure" Events

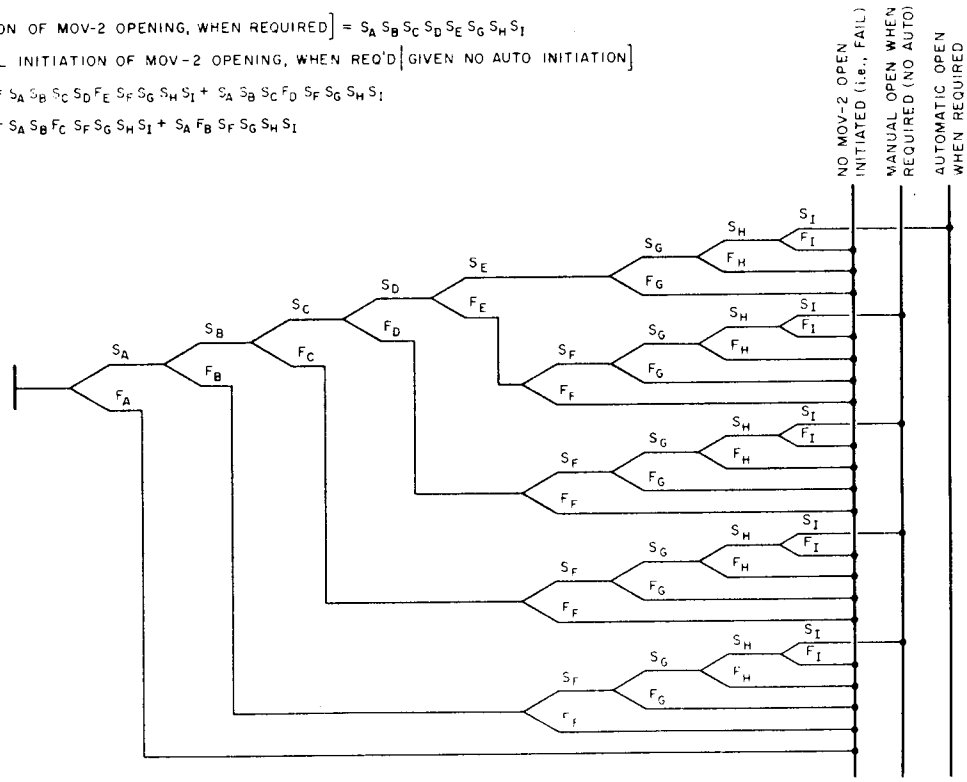


2.5 Decision Tree for Events in Example 2.4.2: "Multiple Outcome" Tree



$S_S = [\text{P: AUTOMATIC INITIATION OF MOV-2 OPENING, WHEN REQUIRED}] = S_A S_B S_C S_D S_E S_G S_H S_I$

$[S_S\text{: DEGRADED}] = [\text{P: MANUAL INITIATION OF MOV-2 OPENING, WHEN REQ'D} \mid \text{GIVEN NO AUTO INITIATION}]$

$= S_A S_B S_C S_D F_E S_F S_G S_H S_I + S_A S_B S_C F_D S_F S_G S_H S_I$

$+ S_A S_B F_C S_F S_G S_H S_I + S_A F_B S_F S_G S_H S_I$