REPORT No. FAA-RD-76-77

10

CRITICALITY ANALYSIS METHODOLOGY

GEORGE MILL

A. SARI

4

JUNE 1975

FINAL REPORT

Document is available to the public through the
National Technical Information Service,
Springfield, Virginia 22161.

Prepared for

U.S. DEPARTMENT OF TRANSPORTATION

FEDERAL AVIATION ADMINISTRATION

Systems Research & Development Service

Washington, D.C. 20590

NOTICE

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

Technical Report Documentation Page

19

1. Report No. 18 FAA-RD-76-77	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle 6 Criticality Analysis Methodology.		5. Report Date 11 Jun[redacted]75 6. Performing Organization Code SRDS/RADC
7. Author(s) 10 George/Mill ~~and~~ A./Sari		8. Performing Organization Report No. 12 121 p.
9. Performing Organization Name and Address Hughes Aircraft Corporation Ground Systems ~~Division~~ Group Fullerton, CA 92634		10. Work Unit No. (TRAIS) 11. Contract or Grant No. 15 DOT-FA73WA-3282 New 13. Type of Report and Period Covered 9 Final Report. Sep[redacted]73 — Feb[redacted]75,
12. Sponsoring Agency Name and Address Department of Transportation Federal Aviation Administration Systems Research and Development Service Washington, D.C. 20590		14. Sponsoring Agency Code ARD-350
15. Supplementary Notes		

16. Abstract

This report definitizes criticality in numerical levels to enable the system designer to most effectively reduce criticality to the level consistent with factors such as economics, weight space, or whatever other limitations may exist. Relationships are developed between reliability, mainta nability as they relate to demand and need to develop quantizatiɔn of criticality indices. Fault trees, FMECA's are given as well as the steps and procedures in the development of an analysis. Included is a specification in the report to demonstrate the implementation of the critical ty methodology to FAA procurements and equipments.

17. Key Words ~~Criticality Methodology~~ C	18. Distribution Statement Document is available to the public through the National Technical Information Service Springfield, Virginia 22151.

19. Security Classif. (of this report) UNCLASSIFIED	20. Security Classif. (of this page) UNCLASSIFIED	21. No. of Pages 122	22. Price

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

dm

FOREWORD

1. PURPOSE. This Handbook has three basic purposes. One is to present general background information relative to Criticality concepts. The second purpose is to provide guidance to the FAA in establishing Criticality requirements, defining Criticality Analysis programs, and monitoring the contractor's Criticality Analysis program. The third purpose is to provide a contractor with technical and administrative guidance in accomplishing the elements of required Criticality Analysis programs.

2. ORGANIZATION. The handbook is organized to assist in the use of the Criticality Specification. In general Section 1.0 defines the scope and application of the Handbook, Section 2.0 identifies related documents, Section 3.0 covers the basic concepts of Criticality, developing/allocating requirements, organizing and directing a Criticality Program, performing the required tasks, and documenting and reporting the results.

INTRODUCTION

The Federal Aviation Administration (FAA) is charged with insuring the safe and efficient use of the nation's airspace. In support of this duty the FAA must operate and maintain the National Airspace System (NAS), a nation wide facility. This facility must provide for the safe and expeditious flow of air traffic, both civilian and military. The NAS supplies navigation and landing aids along with flight control via Controllers to Pilots. The FAA must also provide for planning, and developing improved elements for the NAS. Operating on budgets that are not unlimited, techniques must be used that optimize expenditures. One such technique is Criticality Analysis. This technique provides a standard methodology for quantifying the contribution of the various NAS equipments to safety and delay within the National Airspace System. It will permit the FAA to select among alternate equipments, or to institute equipment modification, or advanced development on the basis of the Criticality leve, which is translatable into service and economic factors. It is an interdisciplinary technique, which draws heavily upon related system engineering disciplines. In establishing Criticality Analysis as a general requirement for NAS equipments, there has been developed a Criticaliyt Analysis Methodology Specification, and a Criticality Analysis Methodology Handbook. The Specification imposes the analysis requirement, while the Handbook establishes the uniform analysis methodology to be used. The Specification to be used was prepared in conjunction with this Handbook.

CRITICALITY ANALYSIS

TECHNIQUES

AND

METHODOLOGIES

Criticality Analysis is a formalized technique/methodology for analyzing the Critical States of units, elements, subsystems or systems to determine the level of Criticality. Criticality is defined as the probability that an equipment, element, subsystem or system will fail to meet some functional demand when required, and which can be directly related to increased delays and/or hazard level in the National Airspace System. Thus this methodology provides for a detailed, quantitative investigation of Critical functional failures or abnormal operation, due either to internal or external causes. In many systems it is much more informative to investigate failure, rather than successes. This Handbook prescribes standard methods of Criticality Analysis to assist the FAA in making decisions with the objective of maximizing the effectiveness of agency capital expenditures on new or improved systems.

ABBREVIATIONS

ARSR	– Air Route Surveillance Radar
ARTCC	– Air Route Traffic Control Center
ARTS	– Automated Radar Terminal System
ASDE	– Airport Surface Detection Equipment
ASR	– Airport Surveillance Radar
ATC&NS	– Air Traffic Control and Navigation System
ATCT	– Air Terminal Control Tower
ATCRBS	– Air Traffic Control Radar Beacon
ATIS	– Airport Terminal Information System
ATMS	– Air Traffic Management System
BUEC	– Back Up Emergency Communication
C	– Criticality
CAS	– Criticality Analysis Methodology Specification
CASS	– Criticality Analysis Summary Sheet
CBD	– Criticality Block Diagram
CEBS	– Cost Element Breakdown Structure
CFM	– Critical Failure Mode
CS	– Critical State
DF	– Direction Finder
DME	– Distance Measuring Equipment
ELOS	– Expected Loss of Service
FAA	– Federal Aviation Administration
FFBD	– Fundamental Flow Block Diagram
FSS	– Flight Service Station
FT	– Fault Tree
GPWS	– Ground Proximity Warning System

IFR	–	Instrument Flying Rules
ILS	–	Instrument Landing System
LAWRS	–	Limited Airport Weather Station
L/F Range	–	Low Frequency Range
LRR	–	Long Range Radar. This is the ARSR
MLS	–	Microwave Landing System
NAVAIDS	–	Navigation Aids
NAS	–	National Airspace System
O&S	–	Operating and Support
PAR	–	Precision Approach Radar
PI	–	Production Investment
RAPCON	–	Radar Approach Control
RATCC	–	Radar Air Traffic Control Center
RB	–	Radar Beacon
RCAG	–	Remote Communication Air to Ground Facility
RCO	–	Remote Communication Outlet
R&D	–	Research and Development
RDO BCN	–	Radar Beacon
RML	–	Radio Microwave Link
RTR	–	Remote Transmitter - Receiver
RVR	–	Runway Visual Range
TRACON	–	Terminal Radar Control
TVOR	–	Terminal VOR
UE	–	Undesirable Event
VORTAC	–	Visual Omni Range and Tactical Air Control and Navigation
VOR	–	Visual Omni Range
WR	–	Weather Radar

TABLE OF CONTENTS

1.0 SCOPE AND CLASSIFICATION

1.1 Scope. This Handbook contains the technical and administrative guidance needed by the FAA and contractors to specify and fulfill Criticality Analysis requirements imposed in procurements. A specification entitled Criticality Analysis Methodology Specification has been developed for this purpose. The Handbook applies to all ground electronic, electrical, electro mechanical equipment in the NAS. The major equipments of the NAS are shown in the figures 1.1.1 to 1.1.4 with their major system groupings, i.e. FSS, ARTCC, ATCT and NAVAIDS. It provides for uniform Criticality Analysis techniques and methodologies which may be used by the FAA or a contractor. The primary objective of the Analysis results is to assist the FAA in making decisions which will maximize the effectiveness of agency capital expenditures on new and/or improved systems.

1.2 Classification. This Handbook can be used to implement Criticality Analysis requirements for any of the types of contract or equipment defined in the Specification. The level of analysis, required data collection, and documentation will generally differ, depending upon the level of system definition. Four standard programs were defined in the Specification which can be applied to Design Studies, Development Model Equipment, Preproduction Equipment, and Production or Existing Equipment respectively. The standard programs are only rough guides. Each contract must be individually assessed in terms of available funding, impact on the NAS and schedule. Since Criticality Analysis is concerned with basic NAS characteristics, that is, traffic capacity, traffic delays, and increased hazards to equipment/passengers, it must be a part of every procurement program. Realistically, however, the analysis can only be conducted when adequate information is available. This requires a level of system definition, and development. The basic data needs of the Criticality Analysis are:

1. System definition in terms of mission/performance requirements and operating environments.

2. Reliability, maintainability information in terms of failure and repair rates. These may be applied to functions as well as hardware, and includes fucntional failure due to external as well as internal causes.

3. Definition of demands on the system, and allowable restoration delays. The level of definition of this data determines, to a large extent, the depth of the Criticality Analysis possible. However, as shown in Section 3.0, , some NAS equipments involve a higher risk level than others, with the result their Criticality requirements are more stringent. Equipments with stringent requirements should be prime candidates for Criticality Analysis regardless of the level of definition of the above data. Ideally criticality Analysis should be initiated during the

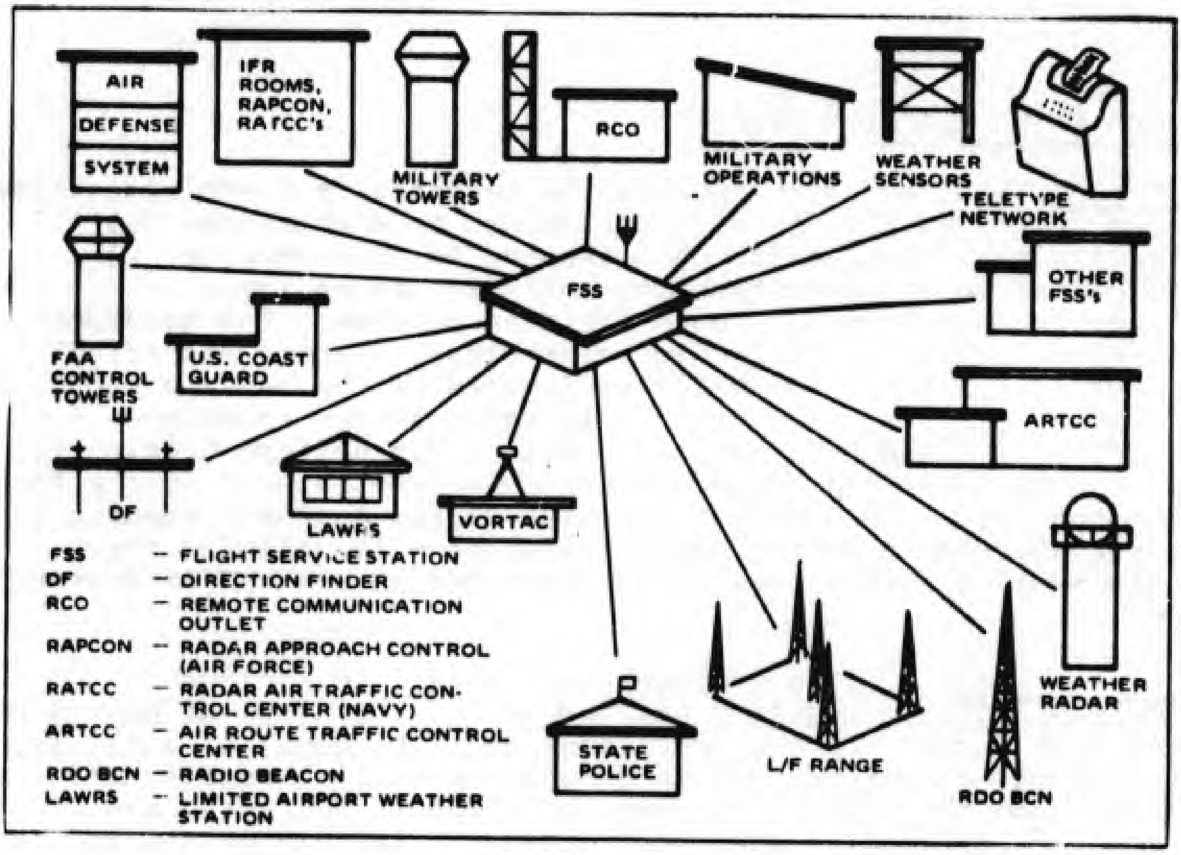

AIR
DEFENSE
SYSTEM
IFR ROOMS, RAPCON, RATCC's
MILITARY TOWERS
RCO
MILITARY OPERATIONS
WEATHER SENSORS
TELETYPE NETWORK
OTHER FSS's
FSS
FAA CONTROL TOWERS
U.S. COAST GUARD
ARTCC
DF
LAWRS
VORTAC
WEATHER RADAR
STATE POLICE
L/F RANGE
RDO BCN
FSS — FLIGHT SERVICE STATION
DF — DIRECTION FINDER
RCO — REMOTE COMMUNICATION OUTLET
RAPCON — RADAR APPROACH CONTROL (AIR FORCE)
RATCC — RADAR AIR TRAFFIC CONTROL CENTER (NAVY)
ARTCC — AIR ROUTE TRAFFIC CONTROL CENTER
RDO BCN — RADIO BEACON
LAWRS — LIMITED AIRPORT WEATHER STATION

Figure 1.1.1 Flight Service System

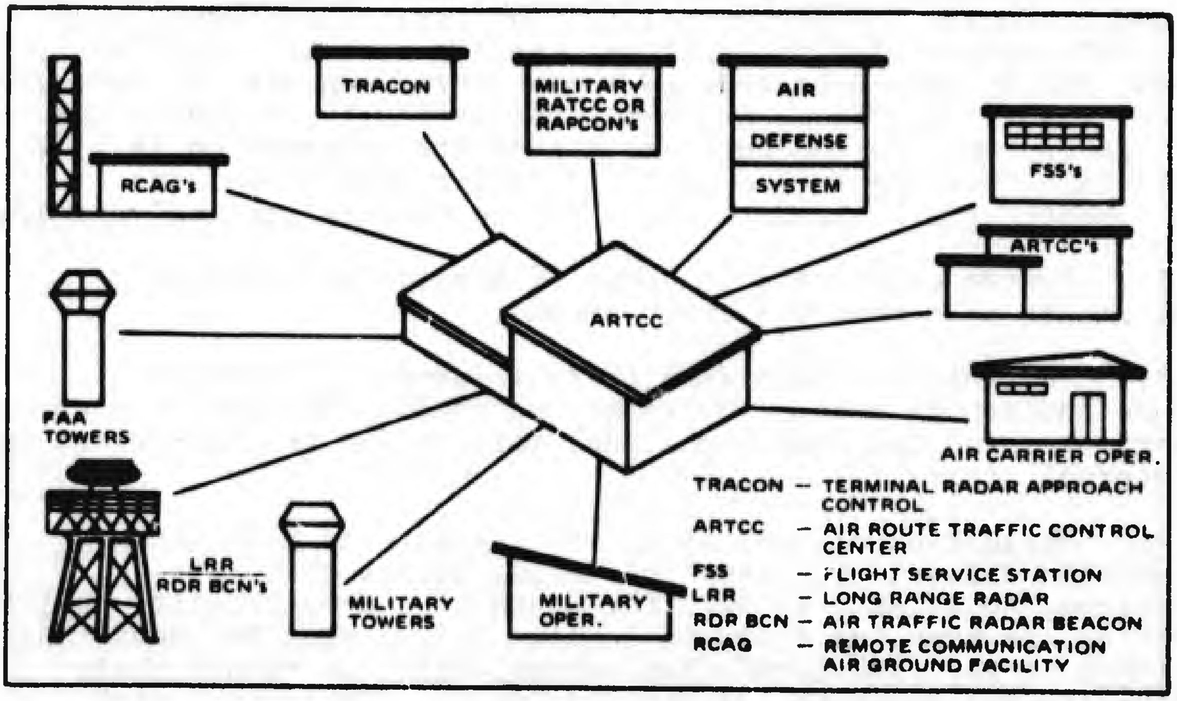

RCAG's
TRACON
MILITARY RATCC OR RAPCON's
AIR
DEFENSE
SYSTEM
FSS's
ARTCC's
ARTCC
FAA TOWERS
AIR CARRIER OPER.
LRR
RDR BCN's
MILITARY TOWERS
MILITARY OPER.
TRACON — TERMINAL RADAR APPROACH CONTROL
ARTCC — AIR ROUTE TRAFFIC CONTROL CENTER
FSS — FLIGHT SERVICE STATION
LRR — LONG RANGE RADAR
RDR BCN — AIR TRAFFIC RADAR BEACON
RCAG — REMOTE COMMUNICATION AIR GROUND FACILITY

Figure 1.1.2 Enroute Control System

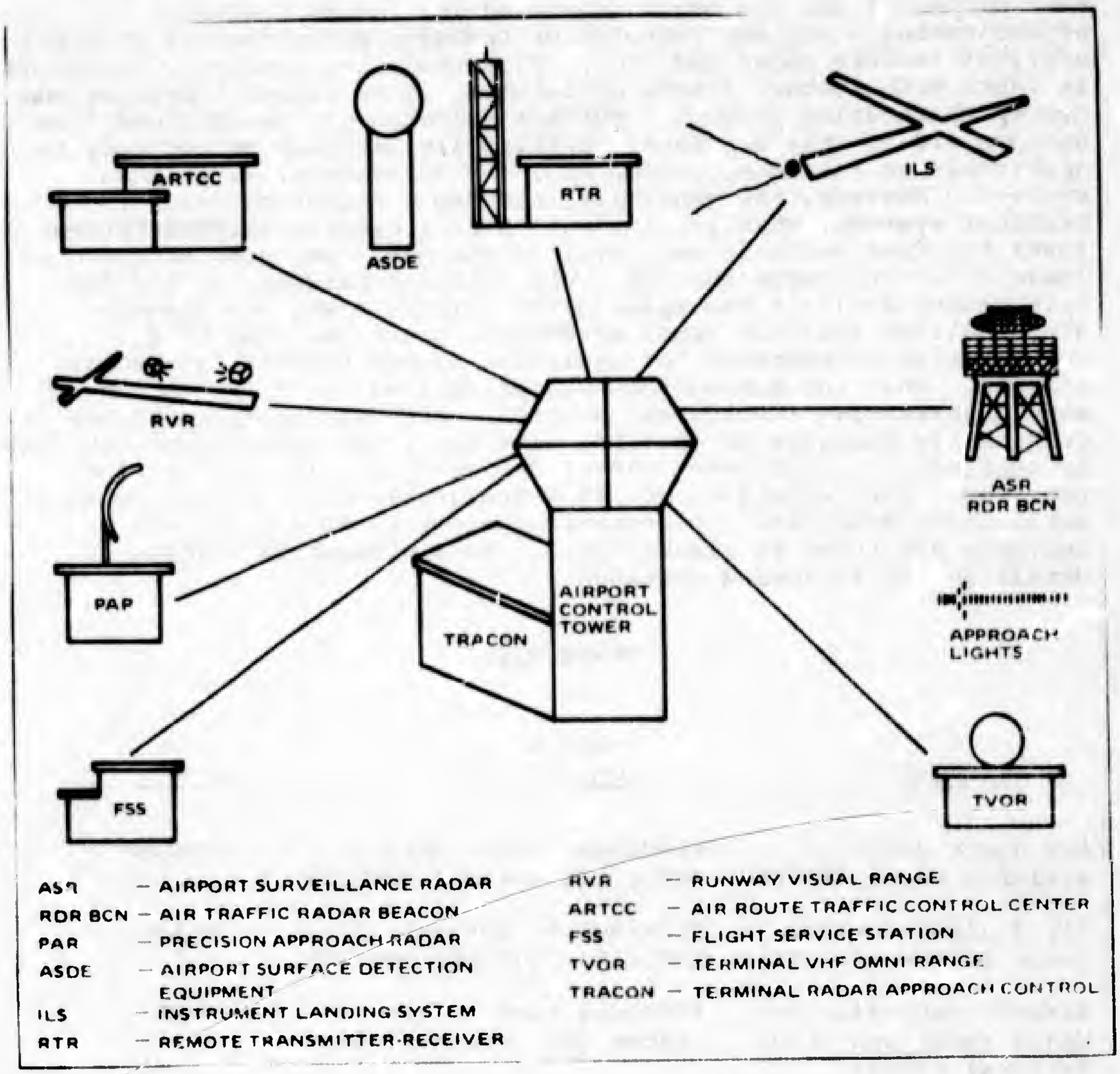

ARTCC
ASDE
RTR
ILS
RVR
ASR
RDR BCN
PAP
AIRPORT CONTROL TOWER
TRACON
APPROACH LIGHTS
FSS
TVOR
ASR — AIRPORT SURVEILLANCE RADAR
RDR BCN — AIR TRAFFIC RADAR BEACON
PAR — PRECISION APPROACH RADAR
ASDE — AIRPORT SURFACE DETECTION EQUIPMENT
ILS — INSTRUMENT LANDING SYSTEM
RTR — REMOTE TRANSMITTER-RECEIVER
RVR — RUNWAY VISUAL RANGE
ARTCC — AIR ROUTE TRAFFIC CONTROL CENTER
FSS — FLIGHT SERVICE STATION
TVOR — TERMINAL VHF OMNI RANGE
TRACON — TERMINAL RADAR APPROACH CONTROL

Figure 1.1.3 Terminal Control System

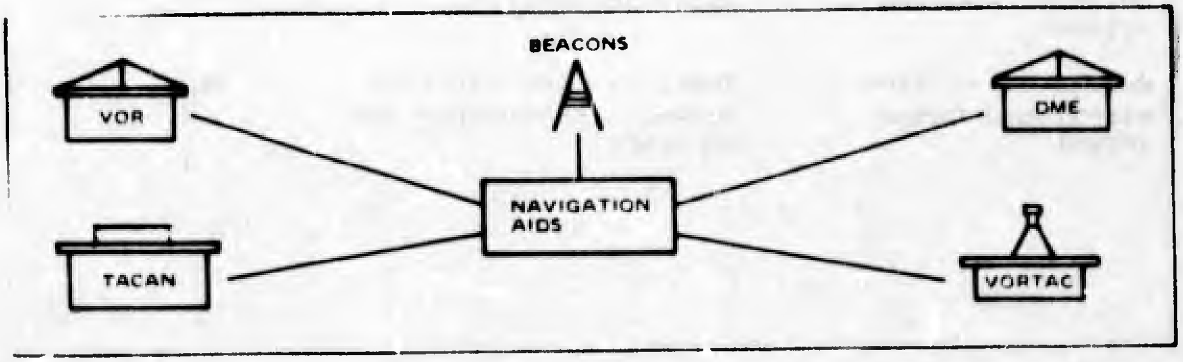


Figure 1.1.4 NAVAIDS System

conceptual phase in order to be most effective and productive. In this manner it has its major impact on the design process necessitating a minimum retrofit or redesign effort toward reducing critical failure modes and etc,. It should then continue, expanding in depth with further system definition, as an integral part of the System Engineering process. Further guidance can be obtained from Section 3.0 of this Handbook. Criticality Analysis Methodology is applicable to elements, components, and subsystems, as well as systems. However, the generally intended application level is to Critical systems, that is, hardware with a clearly defined system level function which is essential to the NAS. The systems shown in Table 1.2.1 represent the top level Critical hardware of the NAS. Criticality Analysis encompasses the Failure Modes and Effects (Criticality) Analysis (FMEA or FMECA), providing a unified, quantitative methodology for analyzing system failures and their effects. Thus the methodology may be applied to FMEA requirements when quantitative results are desired. Although the primary use of Criticality Analysis is as a planning tool, the methodology can also be applied as a real-time control device to aid in traffic flow problems. The techniques are also applicable to a straightforward Reliability Analysis. The essential elements of a Criticality Analysis are shown in Figure 1.2.1. Each element is covered in detail in the following sections.

TABLE 1.2.1

Equipment	Function Required	Criticality	Analysis Required
Air Route Surveillance Radar (ARSR)	Provides target data to ARTCC for enroute control	Medium	R*
Air Traffic Control Radar Beacon (ATCRBS)	Provides target data to ARTCC for enroute control	Medium	R
Airport Surveillance Radar (ASR) and other Terminal Radars	Provides target data to Tracon for terminal control	High	Yes
ARTS - Terminal Systems	Processes target data for Terminal Control	High	Yes
NAS - Stage A En Route Control System	Processes target data for En Route Control	Medium	R
Remote Controlled Air-Ground Commo (RCAG)	Provides communication between controllers and aircraft	High	Yes

Back Up Emergency Communications (BUEC)	Provides communication between controllers and aircraft	Medium	R
Radio Microwave Link or TELCO	Transmits data from LRRS to ARTCC	Medium	R
VHF OMNI Directional Range (VOR), TACAN A&D VORTAC, DME, DR, RB	Provides Navigation Aids to aircraft	Low	O*
Discrete Address Beacon System (DABS)	Provides target data and communication controllers/ aircraft	High	Yes
Instrument, or Microwave Landing System (ILS, MLS)	Provides for Category II and III Landings	High	Yes
HERL, CL, HITLS, MITLS	Runway lighting systems assists night/weather landings	High	Yes
VASI, REIL	Visual slope approach indicator, and runway end identification light	Low	O
Terminal VOR (TVOR)	Provides terminal guidance	High	Yes
ASD-E Radar	Provides data on Ground Traffic	Medium	R
Flight Service Station (FSS)	Provides flight data to aircraft	Low	O
Remote Communication Outlet (RCO)	Provides communication outlet for FSS	Low	O
Airport Weather Station (LAWRS)	Provides weather information for FSS and aircraft	Low	O
Weather Radar (WR)	Provides weather data	Low	O
Precision Approach Radar (PAR)	Provides aircraft position data for terminal control	High	Yes
Remote Transmitter-Receiver (RTR)	Provides communication outlet for Control Tower	High	Yes

Airport Terminal Information System (ATIS)	Provides flight condition information to airports	Low	O
Flow Control Facility	Correlates traffic flow to airport computer	Medium	R

*R - recommended
O - optional

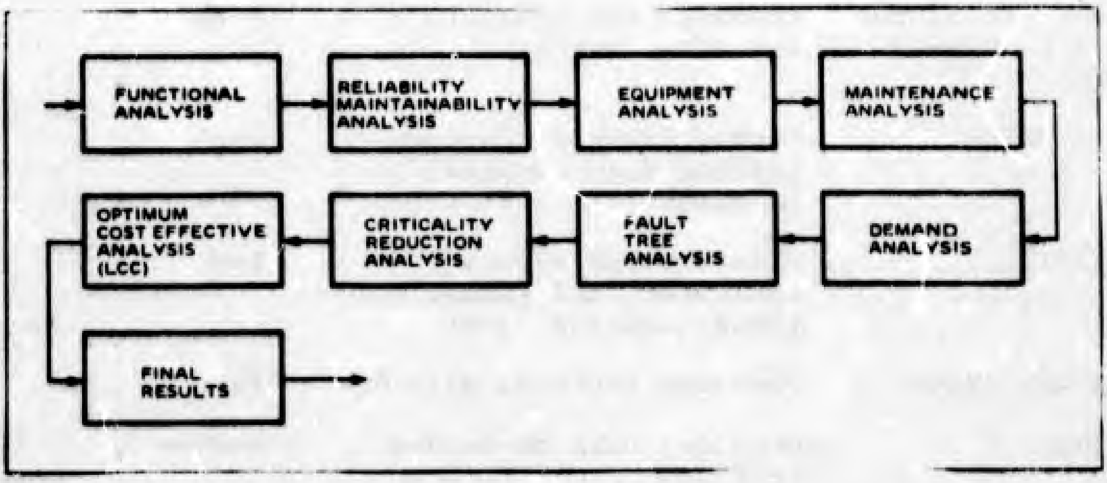


Figure 1.2.1 Criticality Analysis Flow Chart

2.0 APPLICABLE DOCUMENTS

This paragraph, in the Criticality Analysis Methodology Specification lists the documents which are binding on the Criticality Analysis contract. Their primary purpose is to provide a source of standard definitions, and standard analyses in support of the Criticality Analysis. The documents cited are all FAA Specifications, and Handbooks with the exception of MIL-STD-721, on definition of terms. The FAA documents, including the Criticality Specification and Handbook, form a family of documents for establishing, allocating and analyzing requirements for Reliability, Maintainablity, and Criticality. Those documents are listed here for reference and guidance. In addition a list of documents related to Criticality Analysis are also given. These latter documents provide background, and guidance in Criticality Analysis, and are referenced throughout the Handbook.

2.1 Specification Documents:

FAA-ER-650-018c	Reliability Program Plan Requirements
FAA-ER-650-019	Reliability Handbook
MIL-STD-721	Definition of Terms for Reliability, Maintainability, Human Factors, Safety
FAA-ER-350-	Criticality Analysis Methodology Specification
FAA-ER-350-020	Maintainability Program Requirements for Electronic and Associated Support Equipment
FAA-ER-350-022	Maintainability Handbook

3.0 REQUIREMENTS

3.1 Definitions

A. Specification. This paragraph in the Specification is used to define terms peculiar to Criticality, and not found in other FAA documents.

B. Handbook. The definitions from the Criticality Specification are repeated here, along with other definitions, to facilitate reading and understanding of the Handbook.

Critical Failure Mode(CFM). A failure in a system which results in loss or degradation of performance capability.

Critical State. A state which exists when a critical failure mode occurs simultaneously with a demand for that lost or degraded capability, and an allowable restoration delay is exceeded.

Criticality. The probability of being in a Critical State.

Undesirable Event. An event characterized by an increase in delay and/or hazard level in the National Airspace System(NAS).

Criticality Analysis. A detailed, quantitative System Analysis, designed to identify and quantify the System Critical States, and Critical Failure Modes, and to determine economic methods of reducing the System Criticality.

C. Applicable Military Source Definitions

The following definitions are mainly from MIL-STD-882 System Safety, MIL-STD-721B Definition of Effectiveness Terms, and MIL-STD-499 System Engineering Management.

Random Failure. Any failure whose occurrence is unpredictable in an absolute sense but which is predictable only in a probabilistic or statistical sense.

Maintainability. A characteristic of design and installation which is expressed as the probability that an item will be retained in or restored to a specified condition within a given period of time, when the maintenance is performed in accordance with prescribed procedures and resources.

Maintenance. All actions necessary for retaining an item in or restoring it to a specified condition.

Meant-Time-To-Repair (MTTR). The total corrective maintenance time divided by the total number of corrective maintenance actions during a given period of time.

Redundancy. The existence of more than one means of accomplishing a given function. Each means of accomplishing the function need not necessarily be the same.

Reliability. The probability that an item will perform its intended function for a specified interval under stated conditions.

Downtime. That element of time during which the item is not in condition to perform its intended function.

System. A system is a composite of equipment, skills, and techniques capable of performing and/or supporting an operational role. A complete system includes all equipment, related facilities, material, software, services, and personnel required for its operation and support to the degree that it can be considered a self-sufficient unit in its intended operational environment.

Figure of Merit (FOM). A measure of effectiveness through which quantitative system requirements and characteristics can be related to mission objective in optimizing the system design.

Life Cycle Costs. The costs of acquisition plus operation and logistic support costs for the specified operational life-time.

Failure Rate. The number of failure of an item per unit measure of life, (cycles, time, miles, events, etc., as applicable for the item.)

Repair Rate. The number of repairs of an item per unit measure of life.

Repair or Restoration. To return an item to a specified operating condition such that it performs its function as required.

Outage. A condition which exists when an item can no longer perform its specified function.

Functional Demand. Requests for use of a function.

Safety. Freedom from those conditions that can cause injury or death to personnel, damage to or loss of equipment or property.

Hazard. Any real or potential condition that can cause injury or death to personnel, or damage to or loss of equipment or property.

Hazard Level. A qualitative measure of hazards stated in relative terms.

Minimum Cut-Set. The minimum number of elements, which when they are in a failed state, the system is in a failed state.

Delay. Departure of an air carrier from its scheduled time of departure, or time of arrival.

Undesirable Event. An event characterized by an increase in delay and/or hazard level in the National Airspace System.

3.2 General Concepts

A. Basic Concepts of Criticality

The Criticality of a system, subsystem, function or unit is an important measure of how it performs in its real world environment. It has been subjectively defined as "a measure of the indispensability of an equipment or of the function performed by an equipment", or as "the degree of effect of a failure on system performance". These definitions are often adequate for identifying equipments/functions which are Critical, and those that are not Critical. However, if we want to know how Critical an equipment is, then the qualitative nature of these definitions makes them inadequate.* The basic objective of this Handbook is to provide methods for Quantifying Criticality in order to permit rational planning and decision making. Since the treatment of Criticality in the Handbook is quantitative and mathematical, definitions need to be established to avoid confusion. Those given in paragraph 3.1 attempt to fulfill this need.

Figure 3.2.1 illustrates the important elements of Criticality. It is one realization of the compound random process, Criticality, involving the system, demand and an allowable delay.* The system and the demand are both treated as two-state (binary) processes. Further clarification is provided by Figure 3.2.2a which shows the possible system states, including an allowable restoration delay state. In Figure 3.2.2b the Critical State is shown with the adjoining states to which it can depart. Criticality is defined as the probability of being in a Critical State, which is further defined as a state in which a function has failed when it was required and the restoration time has exceeded any allowable delay, i.e.

Where

C - Criticality of the i^{th} failure mode

*That time not counted as failed time that an equipment, system or function is allowed to go from a failed on/off state to on-line. Anything in excess of this is a fouled condition. The delay time can be as small as zero if no delay is allowed.

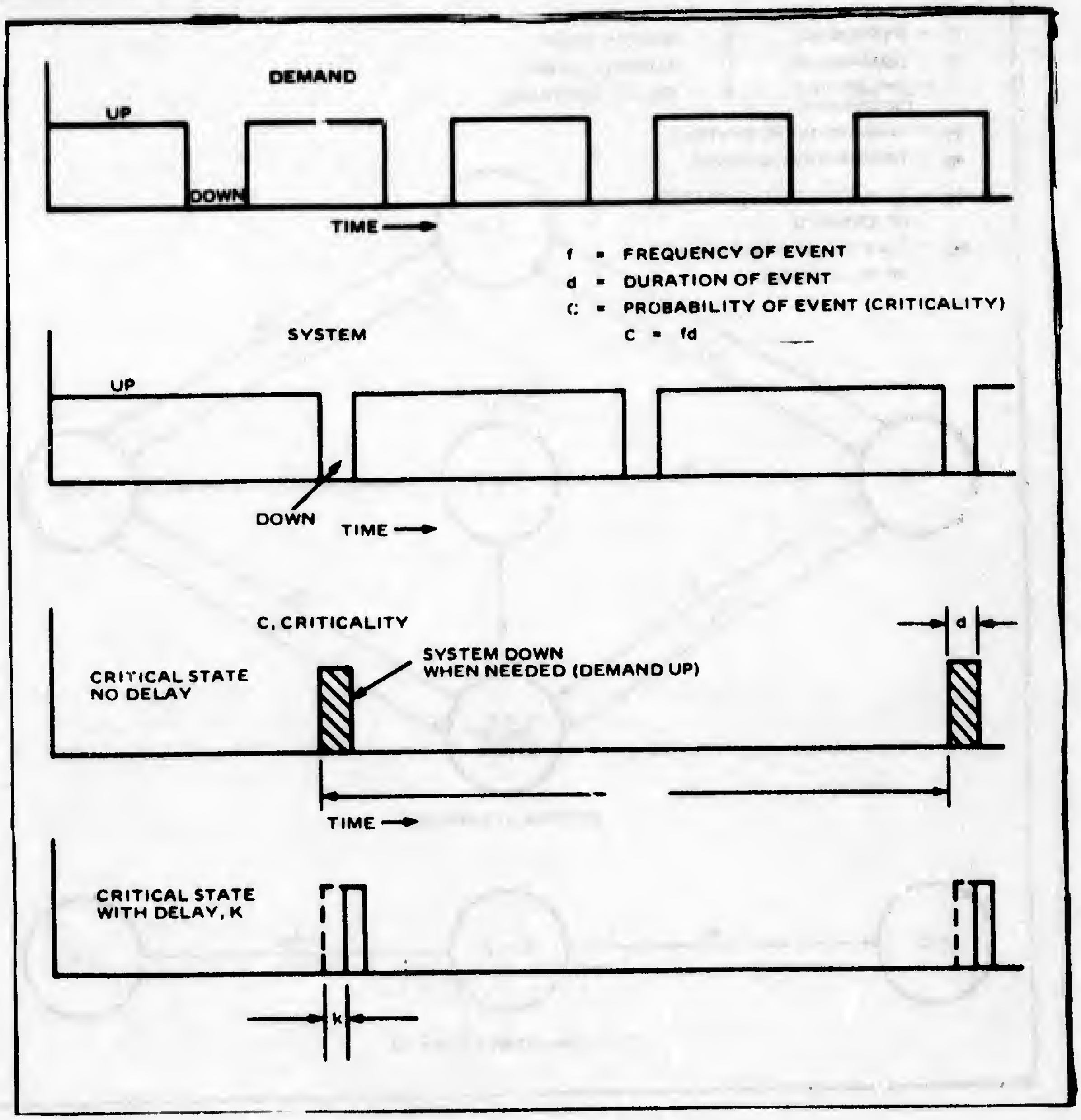
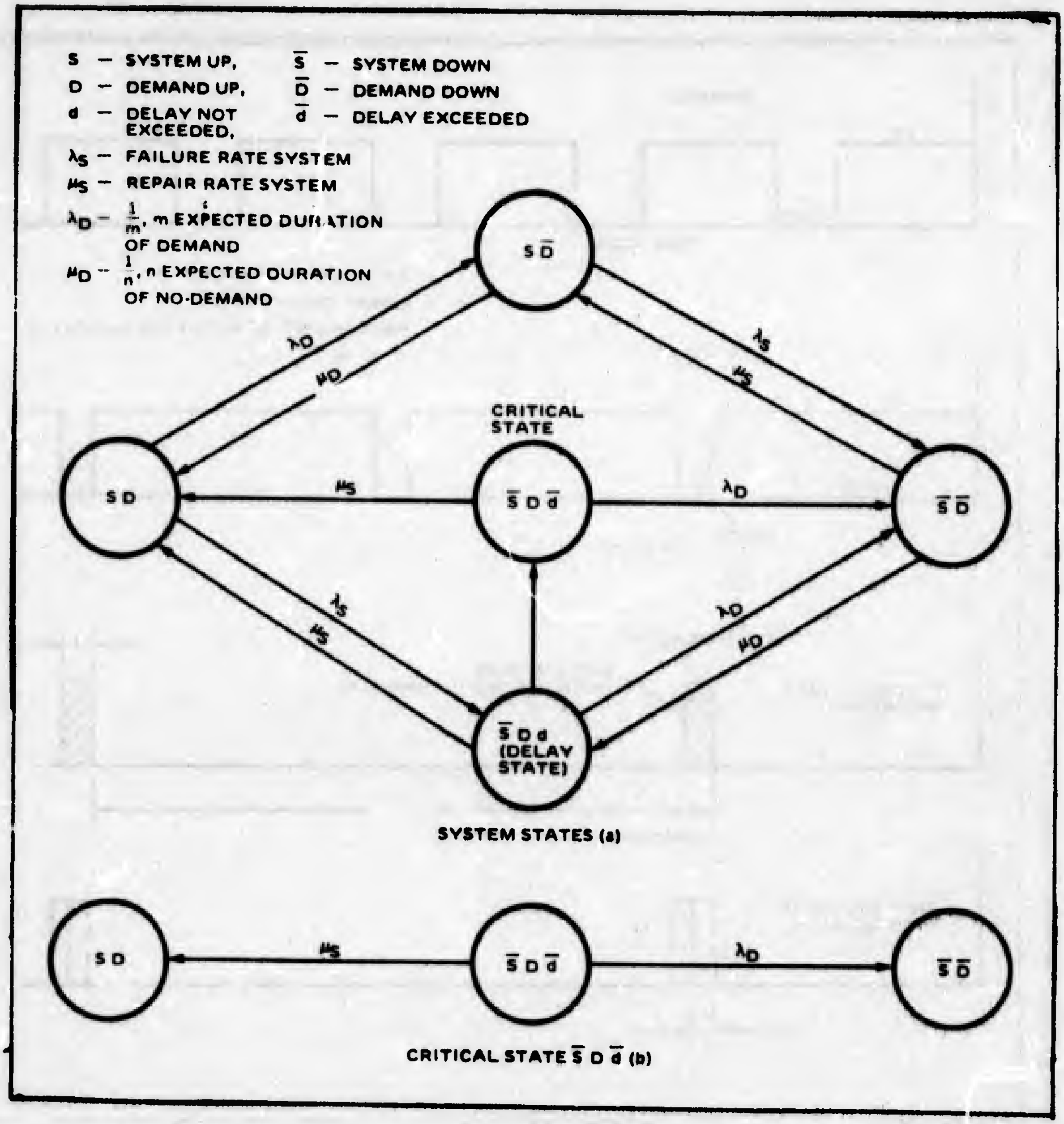


Figure 3.2.1 Criticality Illustrated



SYSTEM STATES (a)

CRITICAL STATE $\bar{S}$ D $\bar{d}$ (b)

Figure 3.2.2 State Diagrams for Criticality

P_i - Probability that the i^{th} function is failed

Q_i - Conditional probability of a demand for the i^{th} function given it is failed

k_i - Allowable delay in restoring the i^{th} function

d_i - Mean time in the i^{th} Critical State

For this exposition these items are assumed independent and in the steady state with no time dependence. Time dependent conditions are analyzed in references 2, 24 and 25 of Appendix A and can be obtained as an output of Fault Tree computer evaluation programs. The total Criticality of the System is approximately given by,

$$C = \sum C_i's$$

This is an upper bound, and a good approximation when C << 1, which is the usual case.

Two other parameters of interest are the expected duration, d, and the frequency of occurrence, f, of the Critical States. They are defined as follows:

$$\text{DURATION}, d_i = 1/(\mu_s + \lambda_o)$$

$$\mu_s = i^{th} \text{ FUNCTION RESTORATION RATE}$$

that is, the inverse of the rate of departure from the Critical State, which is evident from Figure 3.2(b). μ_s is the repair rate for the i^{th} function and λ_o is the inverse of the expected duration of the i^{th} function demand.

The frequency f_i, is given by

$$f_i = C_i/d_i = C_i\mu_i$$

where μ_i is the rate of departure from the i^{th} Critical State.

The overall expected frequency of the Critical States is approximated by

$$f \simeq \sum f_i$$

The overall expected duration is approximated by

$$d \simeq \frac{c}{f}$$

Two other parameters can be calculated as follows:

Expected yearly occurences of a Critical States,

$$N_i = f_i \text{ (8760 HOURS)}$$

And expected hours per year in Critical States,

$$D_i = C_i \text{ (8760 HOURS)}$$

The total occurrences and hours per year of the Critical States are given approximately by

$$N \approx \sum_i N_i$$

$$D \approx \sum_i D_i$$

All of these parameters are summarized in Table 3.2.1.

B. Steady State Equations

For a simple two State System as shown in Figure 3.2.3a, the Steady-State probability of a Critical Failure Mode (CFM), P is given by

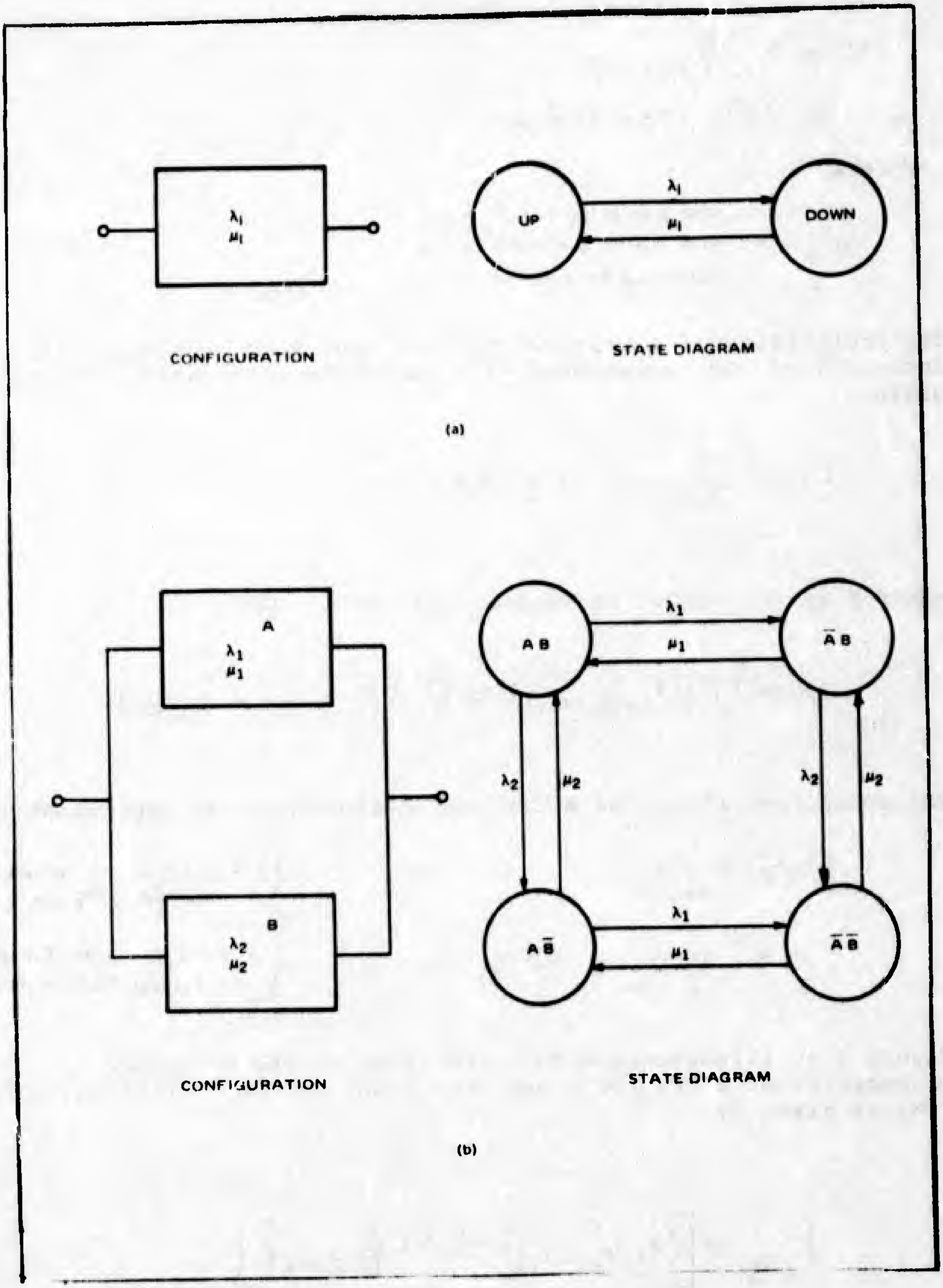


Figure 3.2.3 Probability of Critical Failure Mode

$$P_i = \lambda_i / (\lambda_i + \mu_i)$$
$$\simeq \lambda_i \tau_i \text{, FOR } \lambda << \mu$$

where

λ_i := FAILURE RATE OF THE i^{TH} CFM
μ_i = REPAIR RATE OF THE i^{TH} CFM
τ_i = MEANTIME TO RESTOR i^{TH} CFM $= 1/\mu_i$

The probability of a Critical Failure Mode when redundancy in incorporated and implemented with independent hardware elements is given by

$$P_i = \prod_j P_j \qquad j = 1, 2, 3 \cdots m$$

where M is the number of elements in the i   CFM

$$P_i = \prod_j (\lambda_i / [\lambda_i + \mu_i]) \simeq \prod_j \lambda_j \tau_j \text{, WHEN } \lambda_i << J_i$$

The total probability of a Critical Failure mode is approximately:

$$P = \sum \lambda_{jj} \tau_{ij}$$
$$= \sum_i \prod_j P_{ij} = \sum_i P_i$$

$j = 1, 2, 3, \cdots M$ ELEMENTS IN THE i^{TH} CFM

$i = 1, 2, 3 \cdots N$ FOR N CRITICAL FAILURE MODES

Figure 3.3b illustrates with state diagrams the occurence probability of a CFM for a dual redundant system. State AB, the CFM, is given by

$$P_{\bar{A}\bar{B}} = \left[(\lambda_1 / [\lambda_1 + \mu_1]) \cdot (\lambda_2 / [\lambda_2 + \mu_2]) \right]$$

TABLE 3.2.1

Parameter	Symbol	Equation
Criticality of the i th Critical State	C_i	$C_i = P_i Q_i e^{-k_i/d_i}$
System Criticality	C	$C \approx \sum_i C_i$
Expected Time in the i th Critical State	d_i	$d_i = \frac{1}{\mu_s + \lambda_D}$
Frequency of occurrence of the i th Critical State	f_i	$f_i = C_i/d_i$
Expected Frequency of occurrence of a Critical State in the System	f	$f \approx \sum_i f_i$
Expected System Downtime	d	$d \approx C/f$
Expected Annual occurrence of the i th Critical State	N_i	$N_i = f_i\ 8760$
Expected Annual Hours in the i th Critical State	D_i	$D_i = C_i\ 8760$
Total Annual expected occurrences of Critical States	N	$N = \sum_i N_i$
Total Annual expected hours in Critical States	D	$D = \sum_i D_i$

The probability of a demand for the i^{TH} function, Q_i is given by

$$Q_i = \frac{m_i}{m + n}$$

m_i = MEAN DURATION OF DEMAND FOR THE i^{TH} FUNCTION

n_i = MEAN DURATION OF NO DEMAND FOR THE i^{TH} FUNCTION

The probability that the time in the i^{TH} Critical State d_i (including undetected failure time) will exceed an allowable restoration delay k_i,

$$P(d_i > k_i) = e^{-k_i/d_i}$$

Table 3.2.2 summarizes these Criticality equations.

TABLE 3.2.2

Parameter	Symbol	Equation
Probability of jth Element Failure	p_i	$p_j = \frac{\lambda_j}{\lambda_j + \mu_j} = \lambda_j \tau_j$
Probability of ith Critical Failure Mode	P_i	$P_i = \prod_j p_j$
Probability cf Demand on ith Function	Q_i	$Q_i = \frac{m_i}{m_i + n_i}$
Probability Time in ith Critical State will exceed ith allowed delay	$P(d_i > k_i)$	$P(d_i > k_i) = e^{-k_i/d_i}$

C. Establishing and Allocating Criticality Requirements

The requirements for Criticality Analysis are detailed in the equipment specification. The requirements for the analysis may appear alone or combined with a quantitative Criticality requirement. In the former case, this would be similar to a Failure

Modes and Effects Criticality requirement with the objective of the analysis to identify and quantify the Critical States and Critical Failure Modes. In the latter case a Criticality level would have been established for the particular equipment, and the analysis would be intended to verify that the Criticality requirements were met. The analysis procedure would not differ for either case.

A Criticality Analysis may be required without the procurement document specifying quantitative Criticality requirements. On the other hand the contractor may perform his own preliminary analysis, and actually impose a quantitative Criticality requirement, and an analysis requirement. As a minimum a Criticality Analysis requirement, should be imposed on all medium or highly Critical equipments. The results may be studied in terms of single-point failure probabilities, "graceful degradation", and fail-safe properties, and decisions made on the adequacy of the design. Ultimately some quantitative standard must be raised against which the system performance can be measured. The following paragraphs are intended to provide guidance in establishing these quantitative standards.

D. Criticality Requirements

Criticality is the probability that a system function is in a failed state (outage) when an up condition is required. When an allowable delay in function restoration exists, then this delay time must also be exceeded. A Critical State is reached when all these conditions exist, thus Criticality is defined as the probability of being in a Critical State. When a system is in this state, there exists the possibility of increasing the hazard level or incurring excessive delays in the NAS. Whether or not these latter events transpire depends on the options available for the lost function, and the correlation between system functional loss and the increase in delay and/or hazard level for the NAS. For example if an Instrument Landing System function is lost or malfunctions, when required, a delay in landing is almost certain. There is also an increase in the hazard level. On the other hand if a Long Range Radar Site (LRRS) function is lost, when required, the resulting traffic delay may not be immediately evident. If the demand for service from airborne traffic is in an overlapping zone, another LRRS may assume the load, and no immediate delay may be incurred. If the demand is during a period of high traffic intensity, and a non-overlapping region, then some delay is almost inevitable. The same type of reasoning can be applied to an ARTCC and an ATC to obtain some indication of the incurred delay, and/or increase in the hazard level. What we wish to know ultimately is - the joint probability of the Undesirable Event and the Critical State - which is defined as an increase in delay and/or hazard level in the NAS resulting from the incidence of the Critical State. This can all be expressed in the following form:

$$P(UE,C) = P(UE/C) \times P(C)$$

where, P(UE,C) is the joint probability of the Undesirable Event and the Critical State. P(UE/C) is the conditional probability of UE given the system is in a Critical State, C. P(C) is the probability of being in the Critical State. Also

$$P(UE,C) = P(UE/C)\ P(C)$$

$$= P(C/UE)\ P(UE)$$

$$P(UE,C) = P(UE)$$

Since P(C/UE) = 1, P(UE,C) can be considered a risk level. It is the risk level attendant with less than perfection that is acceptable. In NAS delay and hazard level are functionally related, such that an increase in delay will in some instances result in a decrease in hazard level. In a simple, serial system model, hazard level is related to aircraft separation, hence a possible increase in delay, which generates greater separation and results in a smaller likelihood of collision. Thus, the hazard level is reduced. Although precise hazard levels have not been established by the FAA, we can assume that increased delays will always be opted for in lieu of an increase in hazard level, whatever it may be. In most of the cases being considered here, delay can always be exchanged for hazard level, thus it is possible to consider delay alone in risk assessment, implying a constant hazard level. In order to develop the ideas, the remainder of this section will consider only delays as the Undesirable Event. It should be noted, however, that for real-time, or near real-time applications, some dysfunctions may result in an immediate and significant increase in the hazard level.

E. Establishing the Delay Risk Level

Various reports have dealt with the problem of delays in the NAS, and the resulting cost penalties in terms of aircraft and passenger time, on the ground, and in the air. Reference 5 from Appendix A has estimated the total delay for the "Giant" category of airport in 1975 as more than 400,000 hours with a resulting cost of over half a billion dollars - using an average cost of $20 a minute combined aircraft and passenger time lost. With some 3.5 million yearly operations, this is an average of about 7.5 minutes per operation. Reference 7 from Appendix A cites a specification for aircraft arrival/departure delay distribution as: "The probability that delay is six minutes or less is 0.5, and the probability that delay is 15 minutes or less is 0.9 and, the probability that delay is 30 minutes or less is 0.999." Most of the delays in the study of reference five are attributed to lack of capacity at the airports. Only 10% of the delay is attributed to IFR conditions. There does not seem to be any existing data relating NAS equipment failures to system delays. Reference 5 of Appendix A determined a 10% decrease in delay due to terinal automation. In the absence of any data, it does not seem unreasonable to require that delays exceeding 30 minutes due to the NAS equipment be a small fraction of the total, for example, 10%. In this manner a requirement can be established, using reference 7, and this assumption, as follows:

"The probability of a traffic delay of 30 minutes or more due to any NAS equipment shall be less than 0.0001."

This derives from the latter part of the delay distribution in reference 7, that is, probability that delay is 30 minutes or less is 0.999, thus, probability that delay is 30 minutes or more is 0.001, and 10% of this is 0.0001. This is the joint probability of the Undesirable Event and the Critical State with a 30 minute delay factor. Thus,

$$P(UE, C) = P(UE/C) \times P(C) = 0.0001 \text{ or } 10^{-4}$$

$$\text{Criticality} = P(C) = P(UE, C)/P(UE/C) = 10^{-4}/P(UE/C)$$

To determine Criticality, it remains only to establish the conditional probability, P(UE/C), that is, the probability of an Undesirable Event, given the system is a Critical State. Estimates at a system level are shown in Table 3.3, along with the joint probability, P(UE, C), at 10^{-4}, and Criticality, P(C). This is essentially an allocation developed at a system level.

TABLE 3.2.3

System	P(UE,C)	P(UE/C)	Required Criticality Level, C
ATCT	10^{-4}	1.0	10^{-4}
ARTCC	10^{-4}	0.1	10^{-3}
FSS	10^{-4}	0.01	10^{-2}
NAVAIDS	10^{-4}	0.005	2×10^{-2}

These estimates are based upon a consideration of the individual system functions in the NAS developed from data extracted from the FAA. It appears reasonable that loss of an Airport Terminal Control Tower, when it was needed, is directly transformed into delays in the NAS. Loss of an ARTCC, FSS, and NAVAIDS are successively less felt in the total system.

With these assumptions and the derived data, the Criticality level for the various systems was calculated, and is shown as the last column in Table 3.3

These estimates are only meant to provide guidance to Handbook users in selecting a quantitative level of Criticality for inclusion in the prime equipment specification. Specific ATCTs, ARTCCs, FSSs, or NAVAIDS should be individually addressed to account for their uniqueness. A simpler approach is described in the next paragraph.

F. Expected Loss of Service (ELOS) as a Criterion

The Criticality level is a direct measure of expected lost service for a particular facility. It is the probability that a function is lost when needed or has exceeded an allowable delay in restoration of service. By associating the previous estimate of dollars per minute of delay, and translating lost service into delay by the coordinating equations, we can obtain the "cost" of ELOS, thus

$$\text{Cost (ELOS)} = P(UE/C)\ C \times M \times K$$

where M - aircraft handled per hour, K - cost per hour delay per aircraft ($1200/hr estimate), P(UE/C) - Conditional probability of delay given the system is in a Critical State and C - probability of being in the Critical State. Table 3.2.4 shows the resulting expected hours of lost service per year, based on the Criticality levels established from Table 3.3, where

$$D \simeq C \times 8760 \qquad \text{hours/year lost service (expected)}$$

TABLE 3.2.4

System	C, Criticality	D, Hours Per Year Lost Service (Expected)
ATCT	10^{-4}	0.8760
ARTCC	10^{-3}	8.760
FSS	10^{-2}	87.60
NAVAIDS	10^{-2}	175.2

Based on present levels of achieved service, these numbers do not seem unreasonable. Once the expected hours of lost service per year, D, are specified for a particular facility, the Criticality level is simply obtained from,

$$C = D/8760$$

This is a very simple method of obtaining Criticality levels for the various NAS facilities. Although it is directly relateable to the previous delay risk level method, it avoids explicit considerations of probability of undesirable event, and the related conditional probabilities. In any event, with the assumptions made, both methods produce the same Criticality levels for the various facilities.

G. Frequency and Duration of Critical States

Once Criticality has been established it may also be desirable to specify the expected Frequency, f_i, and Duration, d_i, of the Critical States. Criticality, C_i, is given by

$$C_i = f_i d_i$$

An infinite number of combinations of F and d will produce the same C . The question to be answered is "do we want the yearly hours of lost service in one, two, three, or "n" increments during the year?" Also do we wish to establish a maximum downtime requirement? For some systems frequent, short interruptions may be more tolerable than infrequent long interruptions of service. The opposite condition may also be true for other systems. Since this is directly relatable to Reliability and Maintainability, considerations of mean-time-between-failures (MTBF) and mean-time-to-repair (MTTR) require their inputs as part of any determinations. Each system or facility must, however, be assessed in the light of its special conditions. In general, one or the other of these elements f or d should be specified along with Criticality. Tradeoffs should be considered when the requirements cannot be met or are exceeded.

H. Allocation of Criticality

The allocation of Criticality at a gross system level was discussed in previous paragraphs. The allocation was based on a conditional risk estimate, that is the proability of an undesirable event given that the Critical State existed for a particular facility. Alternately the allocation could be made on the basis of the expected hours of lost service for each facility. In the cases illustrated, they lead to the same allocation of Criticality to the various facilities. Allocation to lower levels is discussed in the following paragraphs.

Given a particular allocation of Criticality to a facility, allocation to the lower levels of the facility can be carried out in several ways. Consider a facility allocation of C, then

$$C \approx C_1 + C_2 + C_3 + \dots\dots\dots\dots C_i$$

Where the C are the various functional entities in a multi-function facility.

Each C_i is given by

$$C_i = P_i Q_i e^{-k_i/d_i}$$

The Q_i and k_i factors of demand and delay, respectively are fixed by the particular application and system useage. P_i is determined by the functional failure and repair rates which are under the contractor's design control. The allocation then comes down to allocatinq outage (unavailability) for which any of the methods developed for Availability allocation are suitable.

The most straightforward method is to allocate on the basis of the predicted functional outage that is

$$C_n = \frac{C\hat{P}_i}{\sum_i \hat{P}_i}$$

, WHERE $\hat{P}_i$ = PREDICTED OUTAGE OF THE i^{TH} CFM AND C = ALLOWABLE CRITICALITY FOR THE SYSTEM

Going one step further the Q_i factors can be incorporated in to reflect the demands for the particular function. The allocation would then be as follows,

$$C_n = C\left[\hat{P}_i Q_i / \sum \hat{P}_i Q_i\right]$$

Finally of course, one can include the entire Criticality equation, and allocation is made as follows,

$$C_n = C\left[\frac{\hat{C}_i}{\sum \hat{C}_i}\right],$$

WHERE $\hat{C}_i$ = PREDICTED CRITICALITY OF THE i^{TH} CRITICAL STATE

In reality, close examination of each functional entity will reveal where possible improvements exist and in turn will effect the allocation. When particular C_i's are better than their allocation, the surplus can be further allocated to those C_i's where the need exists. The Reliability and Maintainability Handbooks contain additional guidance on allocation methods for the failure and repair rates.

Where the various functions differ in importance, and it is not reflected in the demand factor, Q_i, nor the delay factor, k_i, then the allocation may consider an additional importance weighting factor W_i. The allocation would be proportional to W_i, where $0 \leq W_i \leq 1$, to impose a heavier requirement (smaller C_i) on the most important functions.

$$C_i = \hat{C}_i W_i / C_{REQ'D.}$$

W would be assigned in inverse proportion to the importance of the function, i.e., a smaller number (0 to 1) would indicate a more important function.

I. Optimal Allocation

When cost factors can be associated with the elements of Criticality, then the problem can be formulated in terms of an optimization problem in which it is desired to minimize the cost, subject to obtaining a particular level of Criticality, or alternately obtaining the minimum level of Criticality for some fixed budgetary cost. If only failure and repair rates are adjustable by the contractor, the optimum allocations of these parameters can be found by any of the standard optimization techniques (see reference 10 in Appendix A). Generally other constraints will also exist, as for example, maximum permissable downtime (90th percentile), and/or a minimum mean-time-between-occurrences (MTBO), or a maximum frequency of occurrence. All these

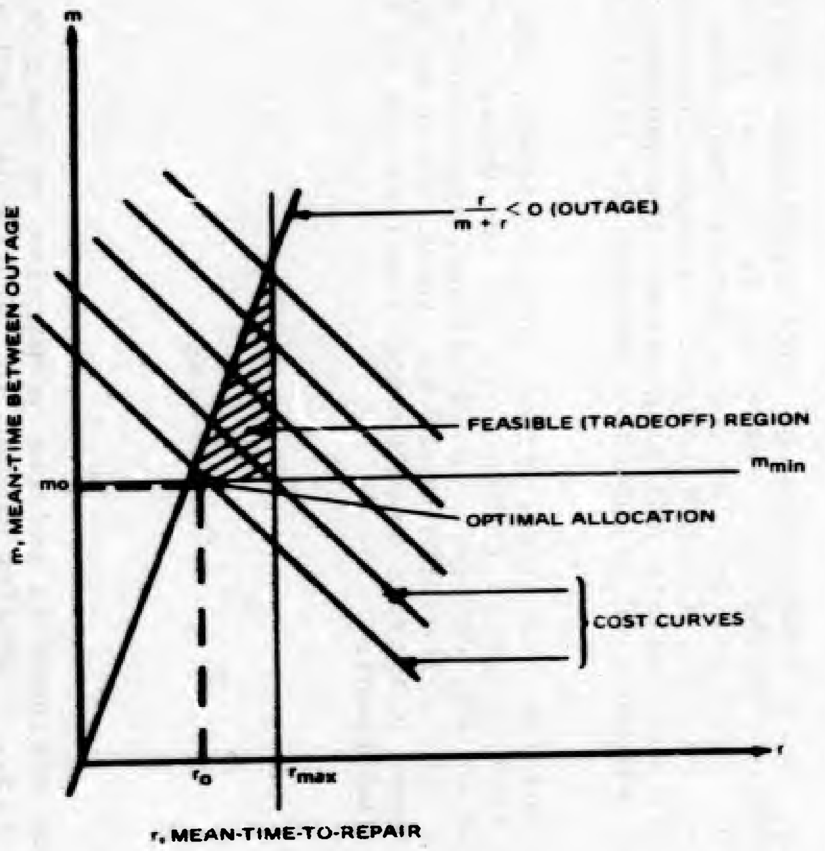
OPTIMIZATION EQUATIONS	GRAPHIC SOLUTION	OPTIMAL SOLUTIONS
MINIMIZE: COST = $\alpha m + \beta r$ SUBJECT TO: $\frac{r}{m+r} < \theta$ (OUTAGE) $m > m_{min}$ $r < r_{max}$ α, β LINEAR CONSTANTS		$r = r_o < r_{max}$ $m = m_o = m_{min}$

TABLE 3.2.4 Optimal Allocation

constraints can be factored into the problem and the optimal allocations obtained. Illustrated in Table 3.2.4 is a linear optimization case where the factors of cost, MTBF and MTTR can be traded off. More complex problems of allocation require computer programs for solution.

3.3 Criticality Analysis Procedures

3.3.1 Preliminary Criticality Analysis (PCA). The Criticality Analysis is conducted in two steps, viz: Prelimnary and Detailed. The objective of the PCA is to obtain a preliminary estimate of the system Criticality level, in order that the need for a detailed analysis may be established or not. It can also serve, with certain steps deleted, as a Criticality Analysis in the early stages of system design when the full operational environment is not defined. The data from the PCA is also be used directly in the Detailed Criticality Analysis (DCA). The major difference between the two levels of analysis is the use of the Criticality Block Diagram in the PCA and the Fault Tree, or equivalent logic diagram (such as Cause-Consequence charts) to symbolize the various Critical States in the Detailed Analysis. The Fault Tree is more flexible with regard to incorporating non-equipment type elements in the causal chain. Thus many more possible contributors to the Critical States may be considered. The function demand and any allowable delays are also easily incorporated. The major tasks in the PCA are shown in the flow diagram of Figure 3.3.1. Guidance in the performance of each task is covered in subsequent paragraphs. A step-by-step procedure for conducting the PCA follows:

Step 1. Identify the system Critical functions, that is, those functions which if lost will cause the system capability to be totally lost or degraded.

Step 2. Determine what the demand is on the system Critical functions. The demand is expressed as a percentage of time the function is normally required, or as a probability that it will be required any time in the future. It is expressed as a number from 0 to 1.0 which represents the ratio of functional demand uptime to total time of the base period. The base period is usually 24 hours.

Step 3. Determine the relationship between the equipment and the Critical functions. This is an output of the Equipment Analysis , paragraph 3.4.1.

Step 4. Construct a Criticality Block Diagram (CBD) in accordance with the instructions of paragraph 3.6.

Step 5. Determine the failure and repair rates for all Critical equipments. This is an output of the Reliability/Maintainability and the Maintenance Analysis tasks.

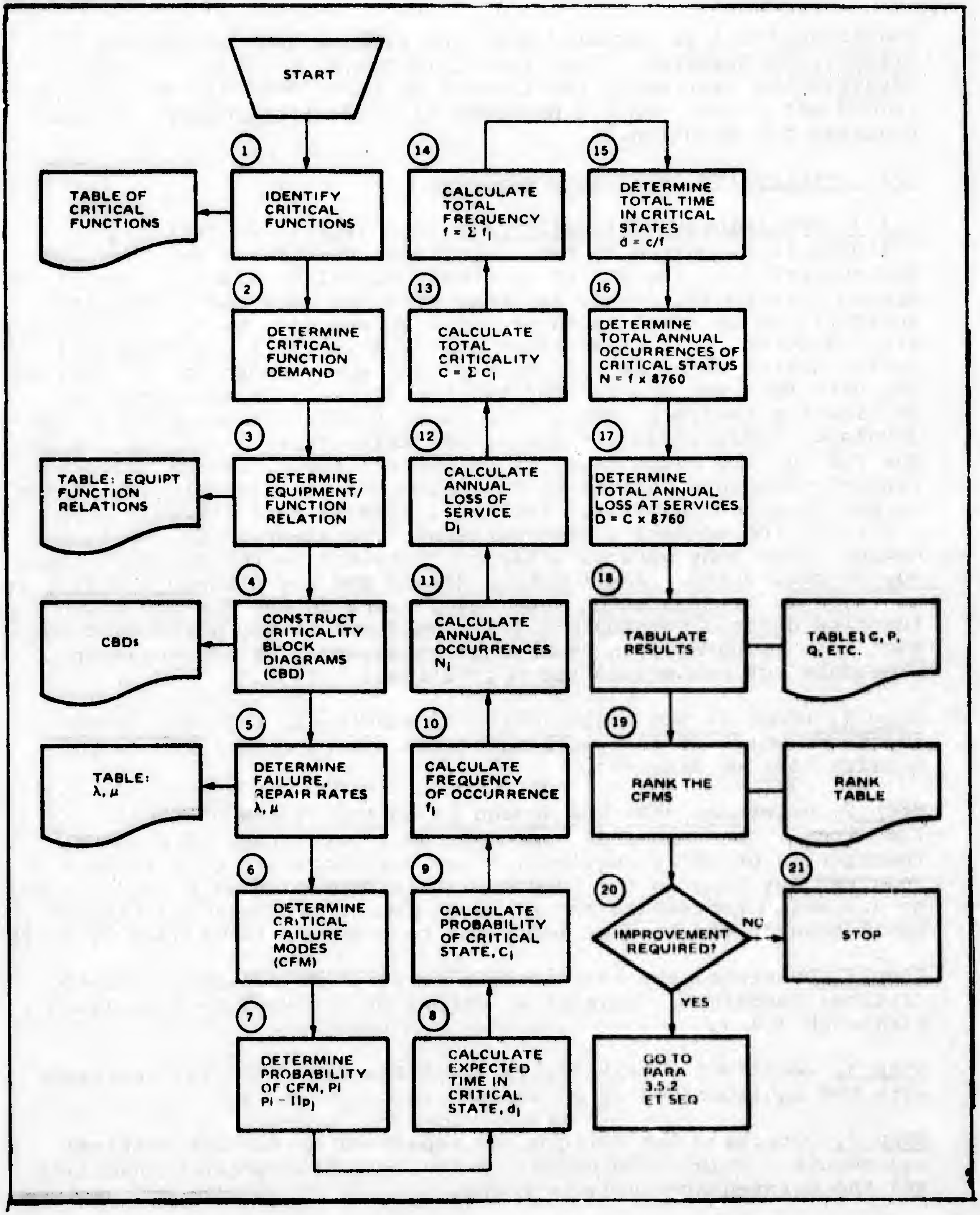

START
1
IDENTIFY CRITICAL FUNCTIONS
TABLE OF CRITICAL FUNCTIONS
2
DETERMINE CRITICAL FUNCTION DEMAND
3
DETERMINE EQUIPMENT/ FUNCTION RELATION
TABLE: EQUIPT FUNCTION RELATIONS
4
CONSTRUCT CRITICALITY BLOCK DIAGRAMS (CBD)
CBDs
5
DETERMINE FAILURE, REPAIR RATES λ, μ
TABLE: λ, μ
6
DETERMINE CRITICAL FAILURE MODES (CFM)
7
DETERMINE PROBABILITY OF CFM, Pi Pi - Πpj
8
CALCULATE EXPECTED TIME IN CRITICAL STATE, dj
9
CALCULATE PROBABILITY OF CRITICAL STATE, Cj
10
CALCULATE FREQUENCY OF OCCURRENCE fj
11
CALCULATE ANNUAL OCCURRENCES Nj
12
CALCULATE ANNUAL LOSS OF SERVICE Dj
13
CALCULATE TOTAL CRITICALITY C = Σ Cj
14
CALCULATE TOTAL FREQUENCY f = Σ fj
15
DETERMINE TOTAL TIME IN CRITICAL STATES d = c/f
16
DETERMINE TOTAL ANNUAL OCCURRENCES OF CRITICAL STATUS N = f x 8760
17
DETERMINE TOTAL ANNUAL LOSS AT SERVICES D = C x 8760
18
TABULATE RESULTS
TABLE: C, P, Q, ETC.
19
RANK THE CFMS
RANK TABLE
20
IMPROVEMENT REQUIRED?
NO
21
STOP
YES
GO TO PARA 3.5.2 ET SEQ

Figure 3.3.1 Flow Diagram of PCA Tasks

Step 6. Determine the Critical Failure Modes (CFM) from the CBD. For simple systems the CFM will be evident from the CBD. For complex systems the use of the Fault Tree and related computer programs may be necessary. This is discussed in the Detailed Criticality Analysis section, paragraph 3.3.2.

Step 7. Determine the probability, P , that the CFM will exist. When all the elements of the CFM are independent, the usual case, then

$$P_i = \prod p_j$$

$$i = i^{TH} \text{ CFM}$$

$j = 1, 2, 3 \cdots n$, WHERE n IS THE NUMBER OF ELEMENTS IN THE CFM AND p_j IS THE PROBABILITY OF FAILURE OF THE INDIVIDUAL ELEMENTS

Step 8. Calculate the expected time in the Critcal State, d , where

$$d_i = 1/(\mu_{si} + d_i)$$

where μ_{si} is the repair or restoration rate of the i^{TH} CFM, and is $1/m_i$, and m_i is the mean duration of the i^{TH} function demand.

Step 9. Calculate the probabilit/ of the associated Critical State, C , where,

$$C = P_i Q_i e^{-k_i/d_i}$$

and P_i = probability of the i^{TH} Critical Failure Mode.

Q_i = probability of a demand for the i^{TH} function.

k_i = allowable delay in restoring/repairing the i^{TH} function.

d_i = expected time in the i^{TH} Critical State, as determined in Step 8.

The allowable delay k_i is set at 0.5 hour in accordance with the discussion of paragraph 3.5.

Step 10. Calculate the frequency of occurrence, f_i, of each Critical State,

$$f_i = C_i/d_i$$

Step 11. Calculate the expected annual occurrences of each Critical State,

$$N_i = f \times (8760 \text{ HOURS})$$

Step 12. Calculate the expected annual hours of lost service due to each Critical State,

$$D = C_i \times (8760 \text{ hours})$$

Step 13. Calculate the approximate overall Criticality

$$C = \sum_i C_i$$

Step 14. Calculate the approximate overall frequency,

$$f = \sum_i f_i$$

Step 15. Determine the approximate overall expected time in the Critical States,

$$d = C/f$$

Step 16. Determine the expected annual occurrences of a Critical State,

$$N = f \times (8760 \text{ hours})$$

Step 17. Determine the expected lost hours of service per year.

$$D = C \times (8760 \text{ hours})$$

Step 18. Tabulate the results, using the System Summary Sheet (SSS), reproduced in Figure 3.3.2.

Step 19. Rank the Critical States by Criticality, and list the percentage contribution to the total, the expected annual occurrences, and the expected lost hours for each Critical State. Tabulate in System Summary Sheet.

Step 20. Determine if improvement in any area is required, or desired. If a quantitative Criticality requirement exists this is determined by whether or not the requirement is met. If no quantitative requirement exists then judgment must be applied at this point.

Step 21. If no improvement is desired, or required, the PCA is complete at this point. If improvement is required, reduction methods applied need be coordinated with system, design and R/M engineering to insure compatibility of requirements throughout. An evaluation of the CBD is given in paragraph 3.7.

If the system is too complex for the manual methods, then the Detailed Criticality Analysis, using the Fault Tree approach with computer aided solutions may be used.

Figure 3.3.3 graphically details the flow paths for a criticality analysis.

3.3.2. Detailed Criticality Analysis (DCA). The DCA is intended to expand the depth of the PCA, and has as its objective the identification and quantification of all possible modes of failure leading to Critical States. The graphic analysis tool used in the DCA is the Fault Tree. The Fault Tree is a logic diagram which starts from each undesirable event, and systematically identifies the sub-events which can cause each of these events. Detailed instructions for constructing the Fault Trees are contained in this paragraph. The Fault Tree is ideally suited for Criticality Analysis, since it is based upon a sequence of logical statements. In particular the demand function, and restoration/repair delays are simply included as additional AND events. Computer programs are available for Fault Tree evaluation, that permit the identification of the Critical Failure Modes, and the quantification of the parameters of the Critical States. The DCA is carried out as follows:

Step 1. Construct the Fault Tree, as per guidance in subparagraph 3.3.2.1.

Step 2. Evaluate the Fault Tree. When the PCA and/or DCA have been completed, and it is determined that reduction in the Criticality level, or any of the parameters is required, or desired then the efforts of system, R/M and design engineering are required to insure compatibility of requirements being met throughout.

3.3.2.1 System Models (Fault Trees)

A. Introduction

CRITICAL FAILURE MODE	RANK	FAILURE DESCRIPTION	EFFECT	PROBABILITY OF OCCURRENCE	EXPECTED FREQUENCY (EVENTS/HR)	EXPECTED DURATION (HOURS)	ANNUAL OCCURRENCES (EVENTS)	ANNUAL LOST SERVICE (HOURS)	WEIGHTING			CRITICALITY	
									DEMAND	DELAY	OTHER	C	PERCENT TOTAL

Figure 3.3.2 System Summary Sheet

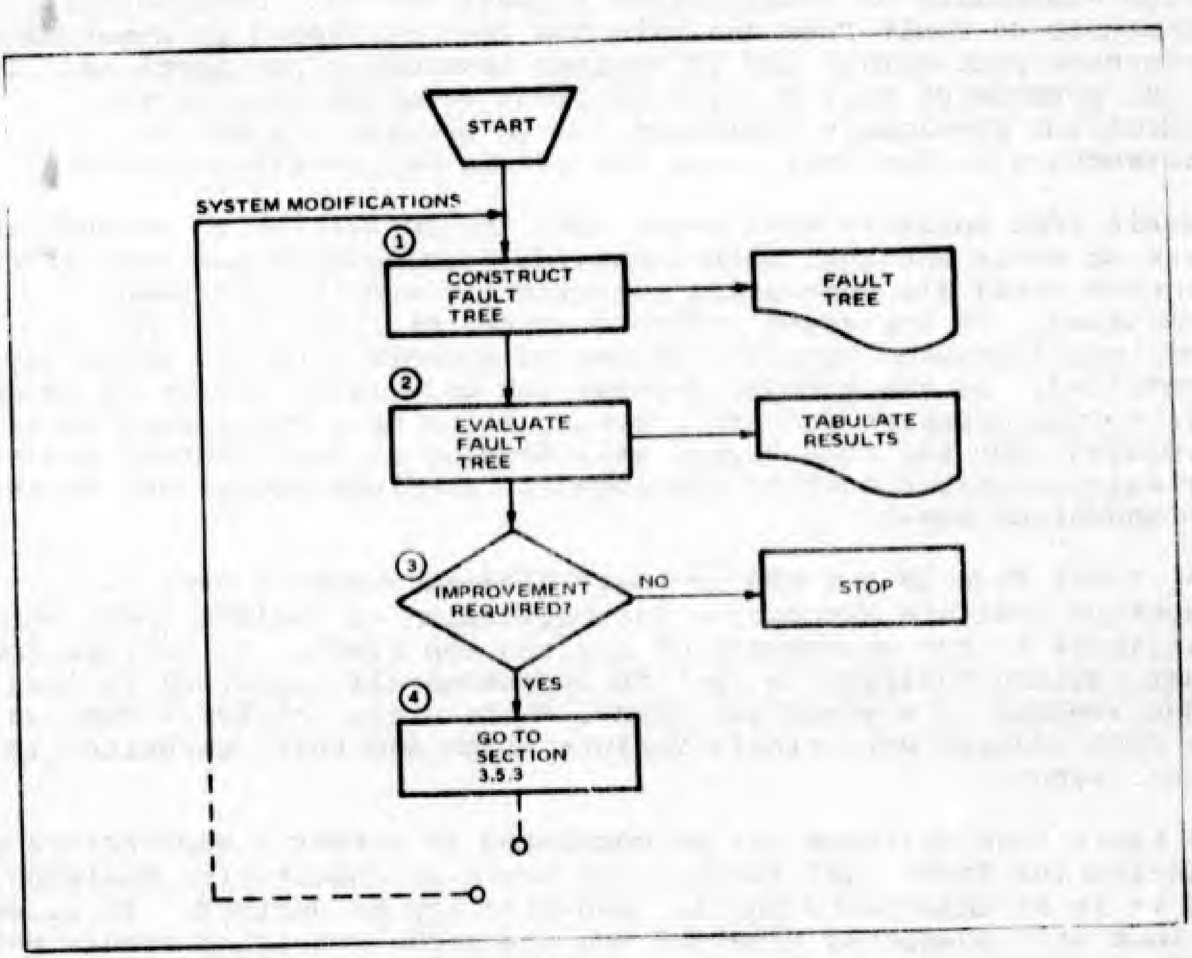


Figure 3.3.3 Flow Chart Detailed Criticality Analysis

The detailed modeling of Criticality utilizes techniques of Fault Tree Analysis which have proven useful in Reliability and Safety analysis of complex systems. Fault tree analysis is not the only modeling method available, but it has been found to be acceptable for developing an understanding of complex systems, and for ensuring a high visibility of contributary failure events. Considerable literature on Fault Tree Analysis has been published in numerous conference proceedings and in various government publications. It is the purpose of this section to bring together some of the information previously published and to provide a guide to construction of the fault tree for use in Criticality Analysis.

A Fault Tree Analysis must begin with the definition of an undesired state or event and then work downward, developing cause and effect branches until all underlying contributory events have been identified. In any given system a number of fault trees may be developed depending upon the number of undesired events which may be identified. As the tree(s) develop the underlying causes of events will become apparent and often events which were considered to be unrelated when the tree began, will develop as contributory causes for which controls must be developed to preclude occurrence of the top undesired event.

The Fault Tree is a symbolic-logic diagram which is used as a deductive analytic method for identification of failure modes which contribute to the occurrence of a given top event. It differs from other failure analyses in that it addresses all potential failure modes leading to a given top event, while other analyses such as the FMEA address only single failure modes and their relationship to an end event.

The fault tree analysis may be completed in either a qualitative or quantitative form. All fault trees begin as qualitative analyses, and it is at this state initial benefits may be derived. It is easy to look at a completed tree and see the paths requiring single point failure modes, and those which require multiple point failure modes. Those primary causes which connect to the end event through "OR" gates represent single point failures, while those primary causes which connect through "AND" gates are considered to be multiple point causes. Care must be exercised to ensure that multiple point failures are separate, unique failures not related or dependent upon each other. As long as they are truly independent, multiple point causes can often by considered as negligible contributors to the end event in a qualitative analysis. Single point failures, however, must be considered as primary causes of an undesired end event which should be reviewed to determine potential corrective measures which may be implemented.

Conduct of the quantitative analysis is directed at evaluation of the degree of severity for each leg of the tree, and the total cumulative probability of the Critical Event occurring. The specific techniques used in quantitative analysis are discussed in detail elsewhere in this handbook, however, the following presents a general overview of the techniques.

Two things are important in performing a quantitative analysis. First the determination of the probability of the end event occurring, and second the cut sets* which will result in occurrence of the end event.

> *Cut sets: The minimum number of elements which when failed will fail the system or function, they are identical to this critical failure modes, CFM.

Strictly speaking the cut sets are part of the qualitative analyses, however, their numerical factors determine the final event probability and it is this probability which identifies the most critical cut set(s). Once the significant cut set(s) have been identified in the system, they may be further ranked by probability of failure and duration of the failed state.

Engineering efforts toward corrective action may then be concentrated on the CFM's having the highest probability of occurrence and the results of the corrective action may be numerically assessed to determine overall impact on the system.

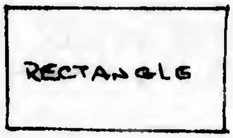
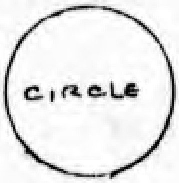
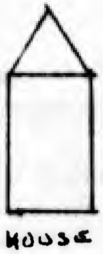
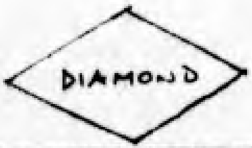
In performing these evaluations it should be remembered that the results are only as good as the data utilized in the inputs. Any assumptions, guesses, or engineering judgments used in development of the data base may be magnified in the output. In the event the inputs are inaccurate, often far out of proportion to the original error.

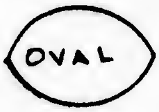
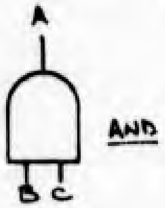
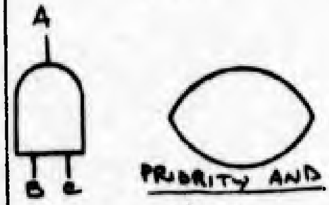
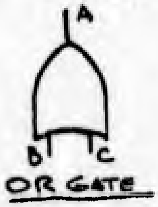
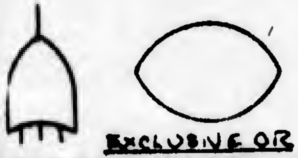
The fault tree analysis represents a logical symbology of events leading to an undesirable top event. The logical substatements represent the necessary and sufficient causes and their relationships as governed by the basic symbology and related logic steps.

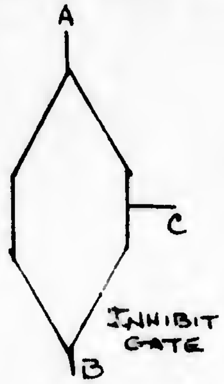
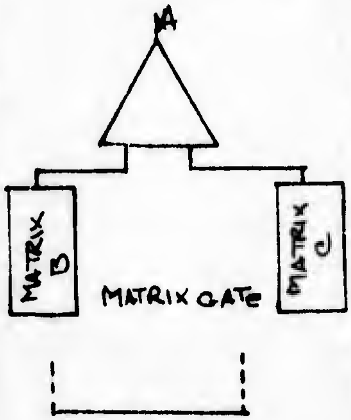
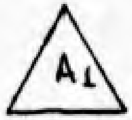
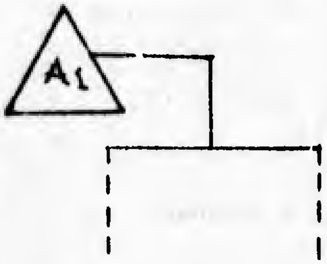
In preparing the tree it should be remembered that a logical approach to the system and to the related failure events is required. In the event that there is more than one undesired event in a system, there should be separate trees developed for each event. Care must be taken that the differing events are not just permutations of the same basic event, and that each can stand by itself. Basic symbology and logic representations are shown in Table 3.3.1

TABLE 3.3.1

FAULT TREE SYMBOLOGY

SYMBOL	USED TO REPRESENT	LOGIC
	(1) An Event. May be the top undesired event or a causative event elsewhere in the tree. May be a gate event or command event in the tree. (2) A description block used with an Inhibit Gate where special conditions govern the inhibit condition.	A statement or an outcome of an observation
	(1) A basic fault event which requires no further development. The failure rate and repair rate are known, and are generally identified adjacent to the event as lambda and tau. (2) A basic input event. Example: A part failure which results in an input to the undesired event.	
	(1) The house represents an event which must occur for the normal operation of the system. It does not represent a fault event. the probability of this event occurring is the reliability of the component. Example: Power must be applied to an interlock circuit for a set of conditions to exist.	
	(1) A Secondary fault event, basic to the logic diagram but for which there is insufficient data for quantitative evaluation.	

	Often used to describe fault events due to human error or due to environmental extremes beyong the specified parameters.	
	(1) The oval represents a conditional event or an input to a conditional inhibit gate. It may be a normal system condition, or it may represent a particular failure state in which an event can occur. (2) It may represent a conditional input to an AND or OR gate establishing conditions of inputs or sequential input requirements. Example: Event A must occur before Event B or as a conditional modifier, "System in Preventive Maintenance."	
	(1) The AND gate is the condition where two or more events must exist simultaneously for the output event to occur.	$A = (B^{o}C)$
	(1) The addition of the priority modifier to the AND gate provides for the use of conditional AND inputs.	$A = (B^{o}C)$ if Condition specified is met (e.g. B before C).
	(1) An OR gate identifies the condition wherein the output event will occur (Inclusive OR).	$A = (B+C)$
	(1) The conditional OR gate like the conditional AND gate exists when either B	

	or C occur, but not when both occur.	
	(1) Inhibit Gate. Used to describe a cause and effect relationship between one fault and another. The input event directly produces the output event if the conditional state is satisfied. This gate is considered as an AND gate in quantitative evaluation.	
	(1) A matrix gate is used when a set of events results in the output "A." The matrix of conditions will be shown in another area of the diagram and the conditions which result in the output event will be indicated with "1" while the conditions which do not result in an output event will be shown with a "0".	
 	(1) The transfer symbol is used to show continuity between two parts of a diagram. It may be used to transfer the diagram between pages, or it may be used to show that a given event is responsible for contributing to more than one final event. Symbol (a) is used to show a transfer out of the tree to a lower level development, while Symbol (b) is used to show a transfer from a lower level to an upper level development. The transfer symbol will contain a designation which shows where the transfer occurs.	

B <u>Fault Tree Structuring</u>

The Fault Tree is constructed from a series of events beginning with the final state and progressing downward through a series of "Gates" which describe the logical cause and effect relationship between the final state and the lower events (see Figure 3.3.4.) In general each lower event will consist of three components. First a primary failure event, contained withn a circle. Second, a command event which would lead to the upper event, contained in a rectangle. Last a secondary event which is contained is a diamond. The combination of primary failure, secondary failure, and command event make up the failure causes for any given failure event. Some events may not have all three causes, however, most will have at least two of the three, (the primary failure cause and a secondary cause). Command events will be further developed by additional gates and such failures or causes as may be appropriate to cause the command event. Circles and diamonds are end branches on the tree and are not developed further. As the fault tree develops each event and each gate must have an identification unique to the event or gate under analysis. Generally this is accomplished with an alphanumeric system of identification. For example, the gate leading into the final state of events would begin with "A-1," and all gates at that level would be "A" level gates. The next level downward would be the B level gates, etc. The events themselves would be identified with an alphanumeric code which would identify the system and subsystem in which they occurred, the type of failure event, and the failure effect.

The steps for performing a fault tree analysis may be described as follows:

1. Define the final state or undesired event. In the case of an FAA related system the undesirable event may be that condition or conditions which result in an unacceptable risk to air traffic or those conditions which cause unacceptable degradations in the air traffic control systems. For example, a condition wherein the separation distance between aircraft fall below some minimum acceptable criteria without the knowledge or intervention of a controller would constitute a top undesirable event. Similarly a condition wherein one of a group of radars providing coverage of a specific geographic area goes out of service could constitute an undesirable event. In addition to analysis of the effect on air traffice, the system operating modes may be divided into single phases or increments which may be analyzed separately. A fault tree branch for each top event or operating mode using a systematic and logical approach can then be constructed.

2. Once the basic event relationships are understood, proceed to identify the causative events for each end event by identification of the following at each level.

   a. Necessity

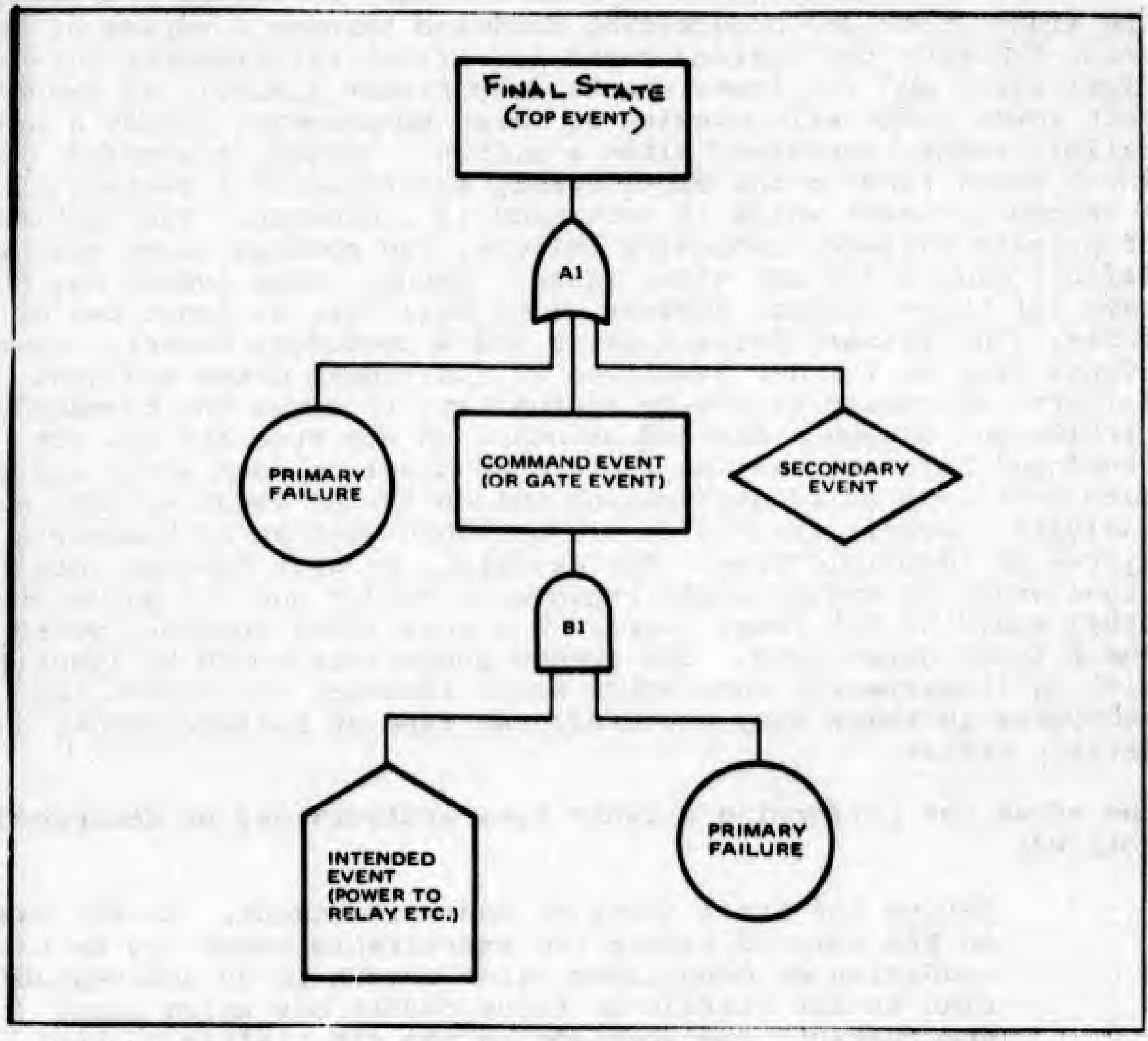


Figure 3.3.4 Primary Fault Tree Example

b. Sufficiency

c. Primary Fault Level

d. Secondary Fault Event (environmental, human, etc.)

e. Command Event

The questions of necessity and sufficiency must be answered for each of the events developed on the tree, but especially in the case of an AND gate. The question to be asked are: What are the fault event relationships required to determin the system unique events which result in the undesired end event? Are these events in themselves necessary and sufficient to cause the end event? While the question of necessity and sufficiency may be addressed for a given primary event, they must be logically addressed whenever a coexistence of events through an AND gate is required to result in the output event.

As these questions are answered, the three factors resulting in a failure event are developed. These factors, as noted previously, are (1) the primary failure event, (2) the secondary failure event, and (3) the command event, or th expected event which occurs at the wrong time. All will exist to some degree in all failure events, however, as the tree develops to the part level, command events will drop out, leaving only primary failure events and secondary failure events.

The primary failure event is the common event resulting from random failure of the part, component, or system under analysis. Events such as "Resistor fails open," or "Diode Short" or "Diode Open" represent the type of common part failure which would be described in primary failure event circles. At the system level events such as "Computer fails," or "Antenna fails" are primary type events.

The secondary failure event is generally environmentally caused, and would include such failures as opening of contacts under excessive vibration, shorted parts due to excess ambient temperature, etc. They could also include shorts due to water leakage or fire caused by leakage of a glycol solution onto a silver plated wire.

Command events are those events which occur due to the primary failures and associated gates.

Figures 3.3.5 and 3.3.6 represent a sample circuit and the fault tree for that circuit. The tree consists of the top event "Drive Motor Stops" and the events which may lead up to that condition. The event heading of "Drive Motor Stops" was chosen over "Drive Motor Fails" since stoppage of the drive motor from any cause will result in the undesirable condition, and it can be seen when looking at the tree that there are command events which can result in loss of drive motor function. In a real system the stop switch would probably be a relay contact located in the master control circuits of the radar, however, the representation on the fault tree as a command event would remain the same.

This circuit might be typical of a radar antenna drive motor. The relay is used to control prime power and the motor is started by depressing the start switch momentary contacts. Once the relay has pulled in contact B serves as a holding contact until the stop switch (S2) is depressed opening the return path for relay power. D1 is provided as a noise suppression diode.

Figure 3.3.5 represents a sample fault tree of this circuit and contains many of the elements found in more complex system level trees.

In Gate A1 (OR) the primary failure mode is "Motor Failure," the secondary failure mode is "Bearing Failure" and the command event is "Control Circuit Stops Motor." The primary and secondary failure events and their respective branches on the tree, however, the command event continues the tree to a lower level. Note that the event is identified as "Control Circuit Stops Motor," rather than "Control Circuit Failure." This is because there are conditions other than control circuit failure which may result in the circuit opening to stop the motor. Failures in other areas such as the relay power supply could also result in loss of the control circuit a[illegible] subsequent loss of the drive motor.

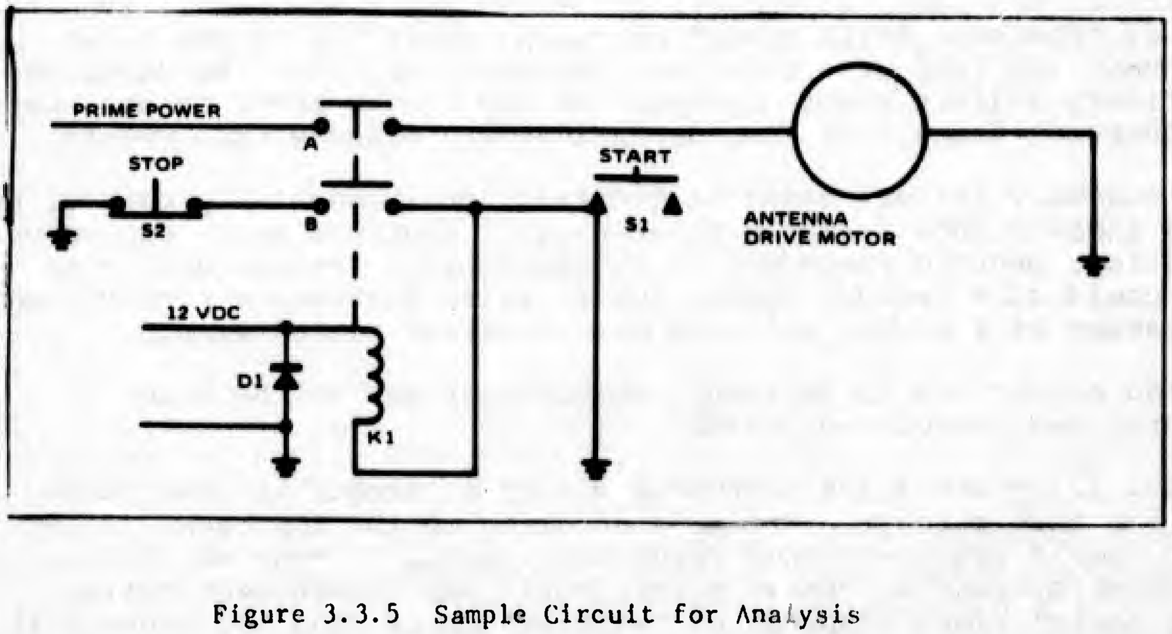


Figure 3.3.5 Sample Circuit for Analysis

Gate B1 (OR) branches to two events, either of which could result in the motor stopping. The first involves opening of the stop switch contacts, while the second involves the various modes and events which could result in the opening of the relay contacts.

Gate C1 (OR) branches into the three major modes under which the contacts of the stop switch could be expected to open. The primary failure mode "Stop Switch Fail Open" would include those random failures generally addressed by various failure rate data bases. The second event (shown in a diamond) is really a command event, and would normally be shown in a rectangle. However, in this case information on the frequency of occurrence is not available and therefore the information is entered on the diamond. The final contribution is from the secondary environmental failure, wherein shock or vibration cause a momentary opening of the contacts resulting in the interruption of power to the drive motor.

Gate C2 (OR) addresses the failure modes related to the relay itself which may result in the end event. The first is failure of the relay, and the second is failure of the relay power supply.

Gate D1 (OR) addresses the various failure modes associated with the relay itself which could result in the undesired output action.

Development of Gate D1 (OR) addresses only failure of the stop switch since the mode under development is Drive Motor Fails, assuming that the motor is running. In the other mode the top event would have to read drive motor fails or does not start. In this case, failure of the start switch to close could also be a mode of failure.

It should be noted that secondary environmental effects, shock, vibration, heat, etc., are addressed in the diamonds. This is necessary because the probability of occurrence is not available.

In performing the analysis of this tree the following steps were taken:

a. Describe the item to be developed

b. List the primary faults

c. List the secondary effects which may effect environmentally sensitive parts (i.e. those secondary events which can cause a primary failure mode to exist).

d. Define the input or command events which are basically in the normal sequence, but which occur at the wrong time thereby resulting in the undesired event.

e. Repeat the process for each level of gate until the bottom of the tree is developed to its logical conclusion.

C. System Level Fault Tree

A second example, at the system level, and incorporating all the elements of Criticality is shown in Figures 3.3.7 and 3.3.8. Figure 3.3.8 is the Fault Tree equivalent of this CBD.

In this example the top undesirable event is loss of either function A or B (or A and B). The "Critical" loss of either function occurs when they are needed (demand exists) and any allowable restoration delays have been exceeded. The demand and delay events are shown as inputs to the respective AND gates. The adjacent site coverage is also shown as an input to an AND gate. The ease of incorporating additional events is evident in the Fault Tree representation. Also evident is the lack of explicitness of the Critical Failure Modes, or Critical States. The CBD shows the failure modes more clearly, but becomes very unwieldy as input events increase.

References 11 of Appendix A contains more NAS examples of fault tree construction. Reference 15 discusses Cause-Consequence diagrams, an alternate system model, very similar to the Fault Tree and FMEA approach combined in one model.

3.3.2.2 Evaluation of the Fault Tree. The Evaluation of the Fault Tree consists of two basic steps:

A. Determine the Critical Failure Modes (CFM), that is the cut-sets.

B. Determine the probability of the Critical States.

These two steps are independent, and can be approached separately. The CFM are strictly a function of the system structure and are not effected by the probabilities. Once the CFM have been determined and reduced to a series of parallel structured elements as in Figure 3.3.9, then the steady state probability of outage is simply computed as,

$$P = \sum_{j} \prod_{i} p_{ij} \quad ,$$

i = 1, 2, 3 ··· m ELEMENTS IN A CFM

j = 1, 2, 3 ··· n CFM's IN A SYSTEM

In many cases i = 1, that is, a single point failure.

For simple systems the CFM are often obvious. For very complex systems many algorithms have been developed to determine the cut-sets. As noted previously the Criticality Block Diagram is adequate for non-complex systems, and its structure often displays the CFM, since any element, or group of elements, that cut the continuity

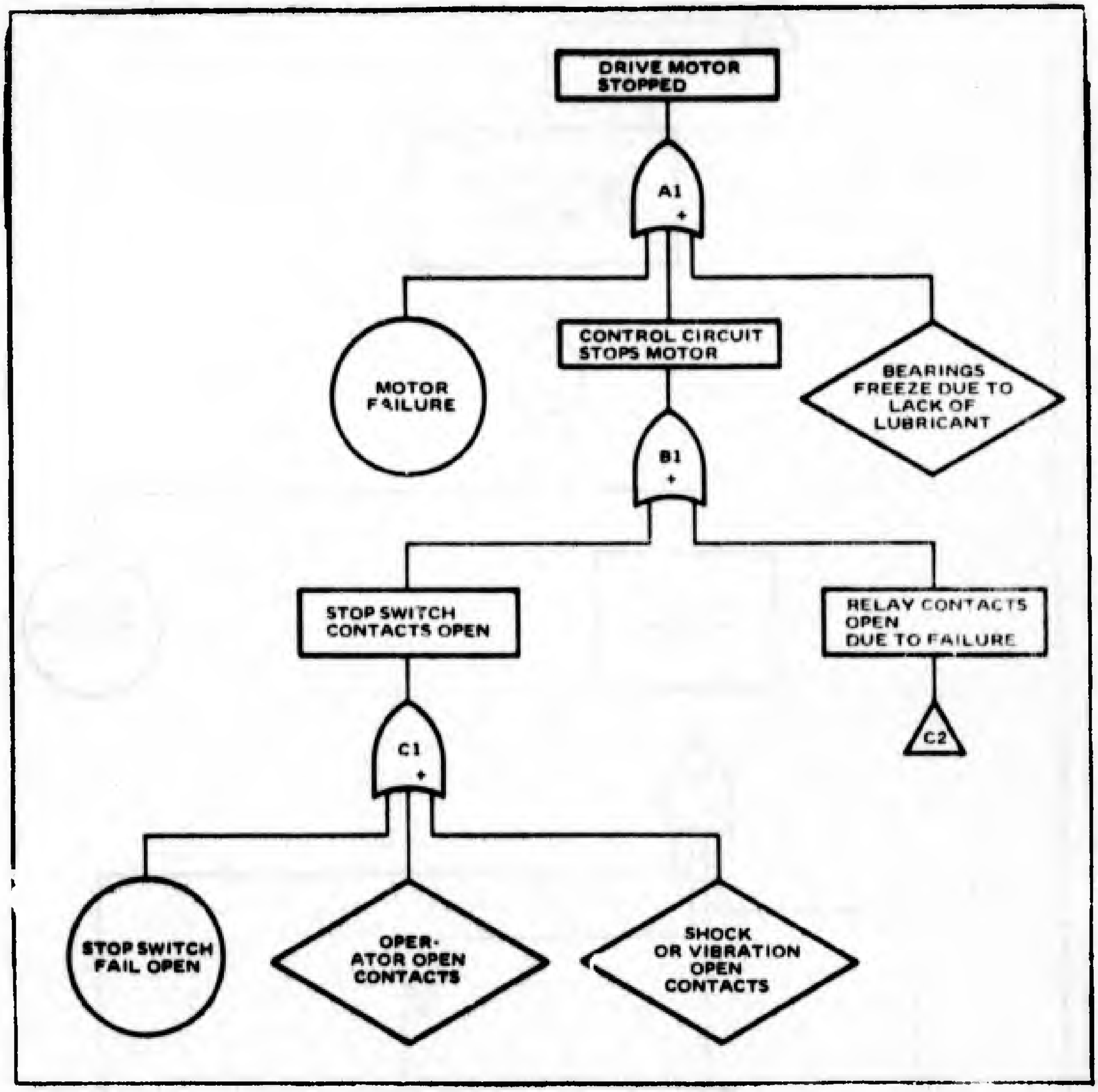

DRIVE MOTOR STOPPED
A1
+
MOTOR FAILURE
CONTROL CIRCUIT STOPS MOTOR
BEARINGS FREEZE DUE TO LACK OF LUBRICANT
B1
+
STOP SWITCH CONTACTS OPEN
RELAY CONTACTS OPEN DUE TO FAILURE
C2
C1
+
STOP SWITCH FAIL OPEN
OPER-ATOR OPEN CONTACTS
SHOCK OR VIBRATION OPEN CONTACTS

Figure 3.3.6 Sample Fault Tree (1 of 2)

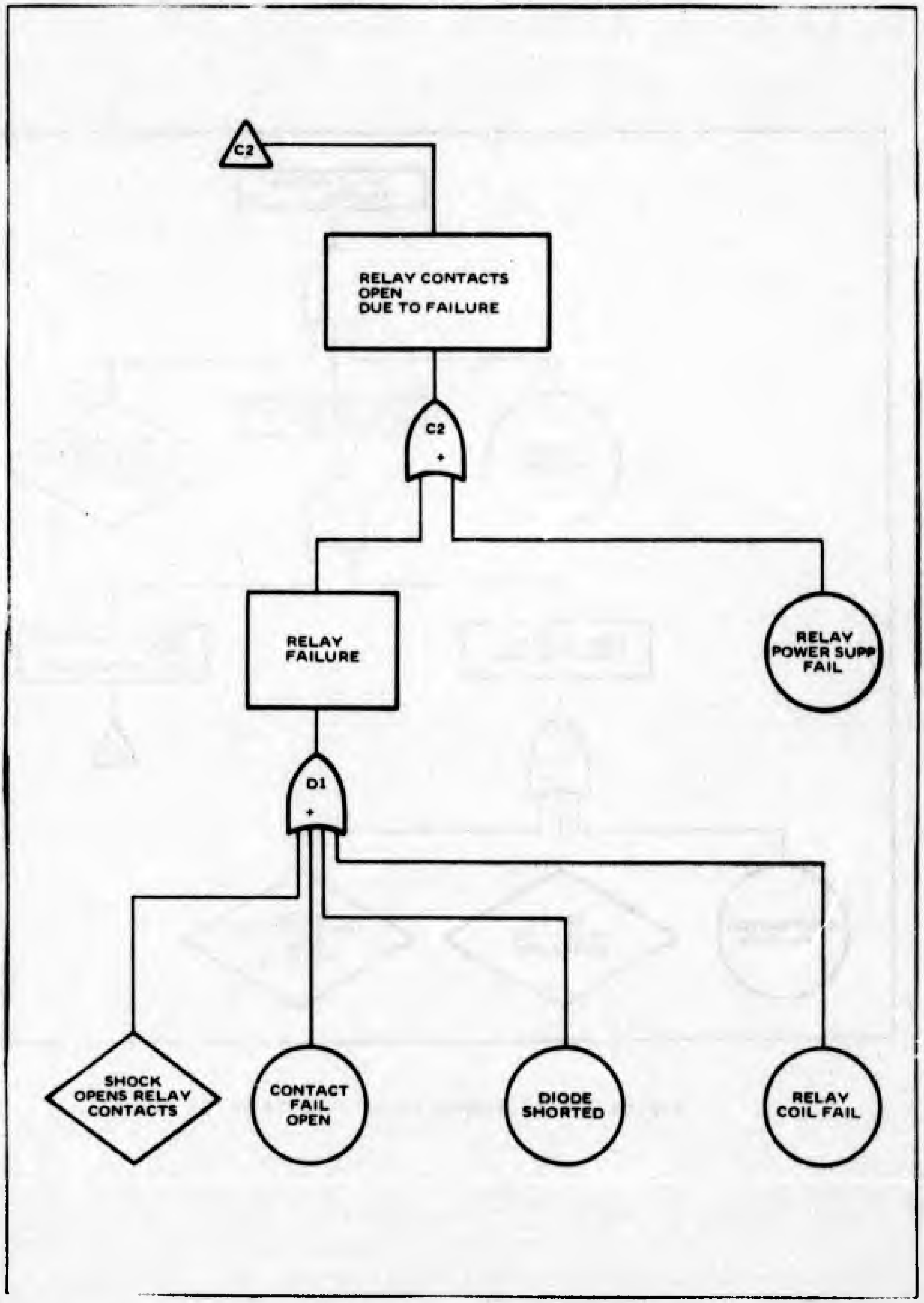


Figure 3.3.6 Sample Fault Tree (1 of 2) (Continued)

from input to output will result in loss of the function, and is thus a Critical Failure Mode. For a single function system the Criticality is approximately the sum of the probabilities of these failure modes, properly weighted for delay and duty cycle.

For multi-function systems the failure modes have to be associated with the loss of some function, which is usually a sub-event in the fault tree. Figure 3.3.9 illustrates a multi-function fault tree, spread out under a single top event. It is possible to evaluate each significant branch of the tree independently to obtain data on specific functions of multi-function systems. By properly structuring the Fault Tree this data can be obtained as a normal program output. Experience constructing fault trees, and using computer evaluation will often make this structure simplification evident. In any event the Fault Tree can be constructed as directed in section 3.3.2.1. Once the tree has been completed, and the event, or events of importance have been established, the first step is to determine the minimum cut-sets. The following paragraphs describe several methods of determining the minimum cut sets. Which method to use depends on the complexity of the system, and the detail information that is required.

A. Determining the Critical Failure Modes (cut-sets). To simplify the exposition, the fault trees are considered as abstract models. The events can be failures, demands, or delays - they are just elements in logic diagram. Four methods of determining the cut-sets, in common use are:

1. Boolean Algebra (Ref 3, Appendix A)

2. Reliability Block Diagram equivalent (Ref 17, Appendix A)

3. Deterministic Testing (Ref 1, 2, Appendix A)

4. Monte Carlo Testing (Ref 1,2, Appendix A)

1. Boolean Algebra. In the Boolean Algebra approach, the logic of the tree is written down and expanded. Then making use of basic Boolean Algebra rules the expansion is simplified until finally only a series (sum) of parallel structured elements remain, as in Figure 3.3.8. The logical steps to reduce a tree are shown in Figure 3.3.10.

2. Reliability Block Diagrams. The Reliability Block Diagram (RBD) equivalent procedure is shown in Figure 3.3.11. Using the logic rules developed in paragraph 3.3.1 the Fault Tree is reduced to an RBD as in Figure 3.3.12a.

The RBD in turn is then reduced to a series of cut-sets as shown in Figure 3.3.12b.

For non-complex systems the previous two methods may be manually performed. Both methods can be computerized, extending their usefulness to somewhat more complex systems. However, methods more amenable to computerization are available for complex systems, such as methods 3 and 4.

3. Deterministic Testing. Method 3 deterministic testing is a straightforward testing of the Fault Tree for the occurrence of the event of interest, as each element is successively failed. Testing is continued for pairs, and triples of element failure, or to whatever depth desired. Theoretically it is possible to test all possible combinations of components, but for trees having more than 100 components (resulting in 2^{100} combinations), the computer time becomes excessive. In most cases failure modes of more than 3 elements can be ignored, since they will usually be on the order of 10^{-6} probability or less. Thus it is not necessary to test all 2^{100} combinations, but only those of 1, 2, and 3 elements which results in considerably less tests. The number of tests is simply the number of arrangements of n things taken m at a time, where the order is not important, i.e.

$$N = n! \,/\, (n-m)!\, m!$$

Importance sampling can be used to reduce computer time (ref 14). This technique generates events in a manner which increases the frequency at which the various event combinations occur. The increased frequency is compensated for by the use of weighting factors inversely proportional to the increase. See reference 14.

A computer program to perform this deterministic testing method is available as COMBC from the FAA, and is further described in reference 1.

4. Monte Carlo. Method 4, Monte Carlo Testing, is a simulation in which failures are chosen according to the failure distributions. All components are assumed non-repairable and independent. The non-repairability assumption in no way effects the validity of the cut sets. In fact repair rates never have to be input to any program determining minimum cut sets - the information is simply not required until evaluation of the probabilities is undertaken. After a set of components has been failed, the tree is tested by a subroutine to determine if the event of interest has occurred. If it has the components are sorted to obtain minimal cut set, which is then checked against all previously found minimal cut sets to eliminate duplicates. A computer program FATE to perform this simulation is available from the FAA, and is described in reference 1.

Once the cut sets have been identified, probabalistic data about them can be developed by various methods. The following paragraphs discuss this aspect.

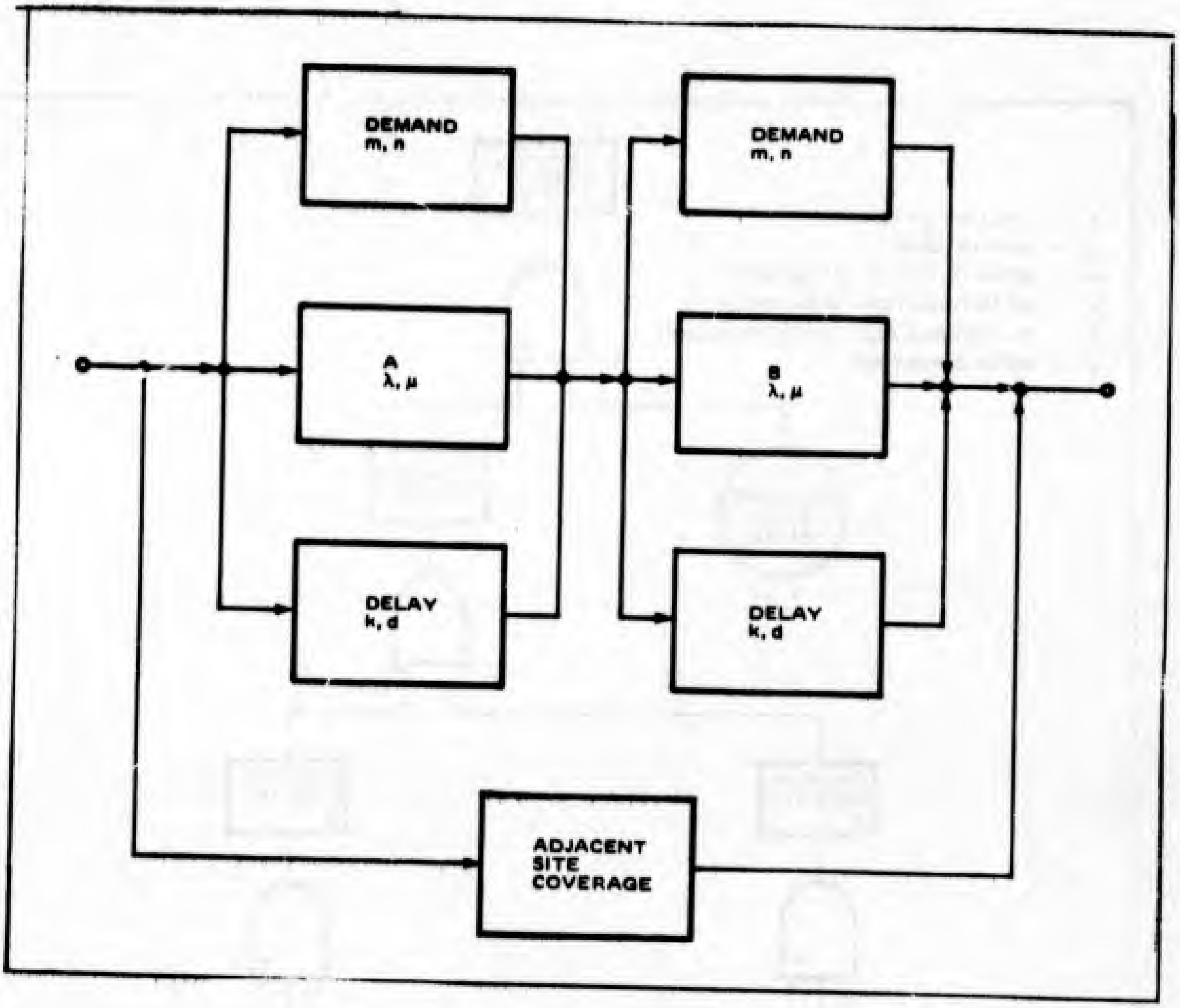


Figure 3.3.7 Multi-Function CBD with Adajcent Site Coverage

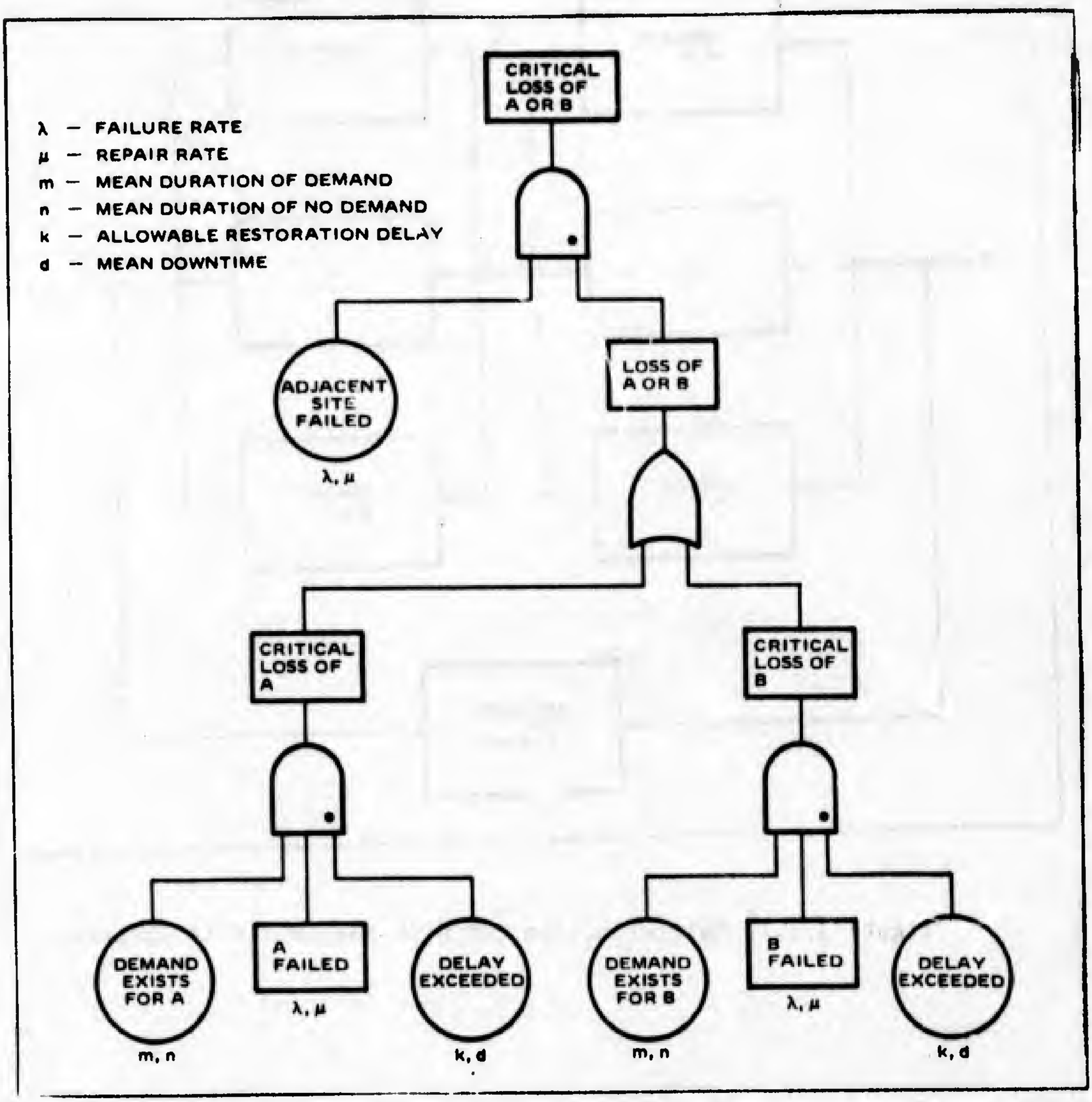


Figure 3.3.8 Criticality Fault Tree

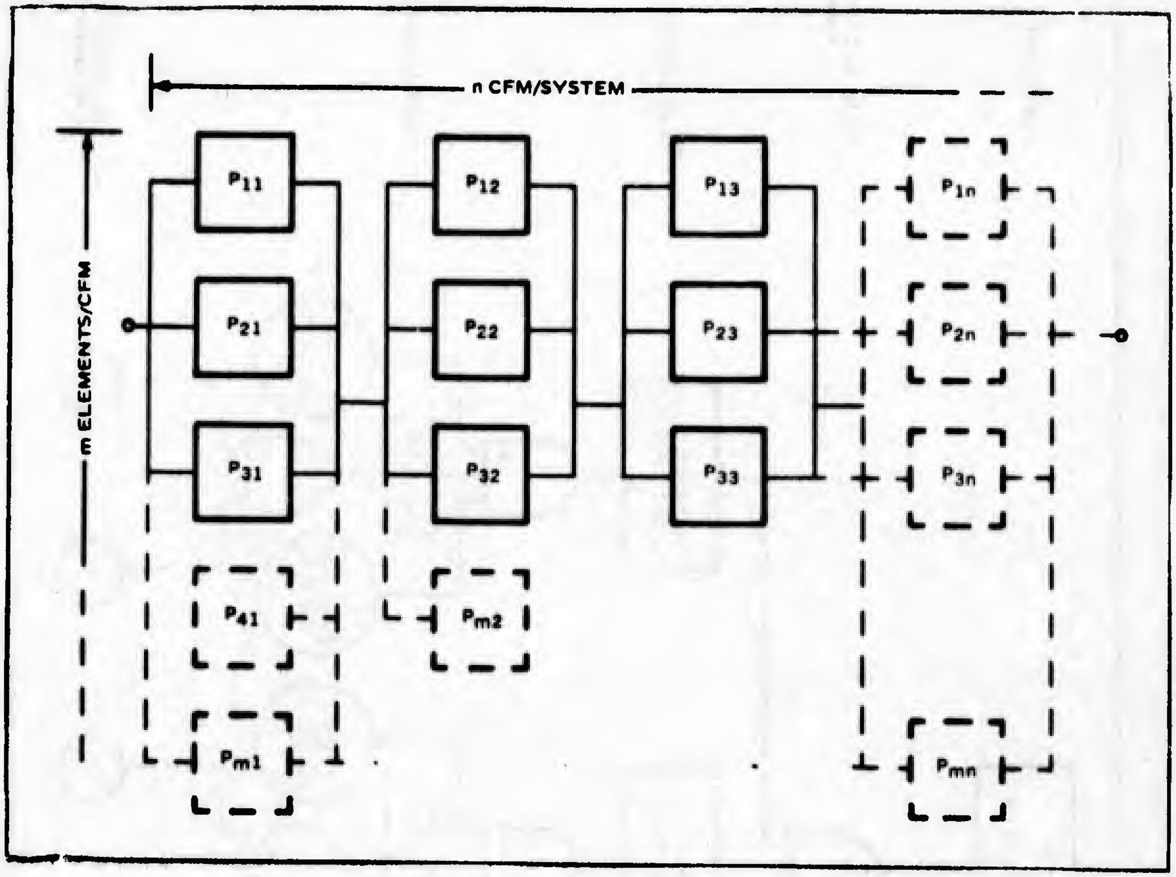


Figure 3.3.9 Canonical Form

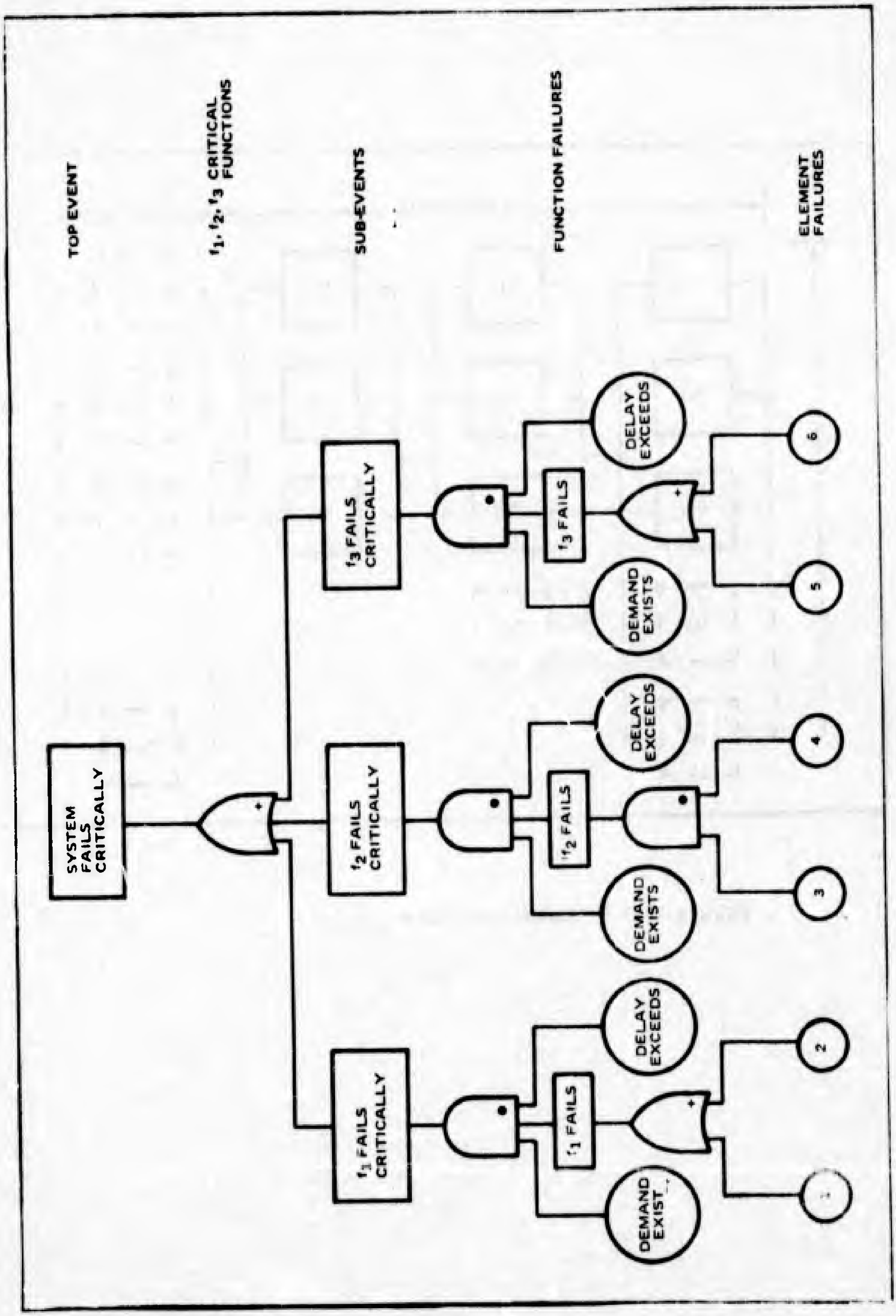
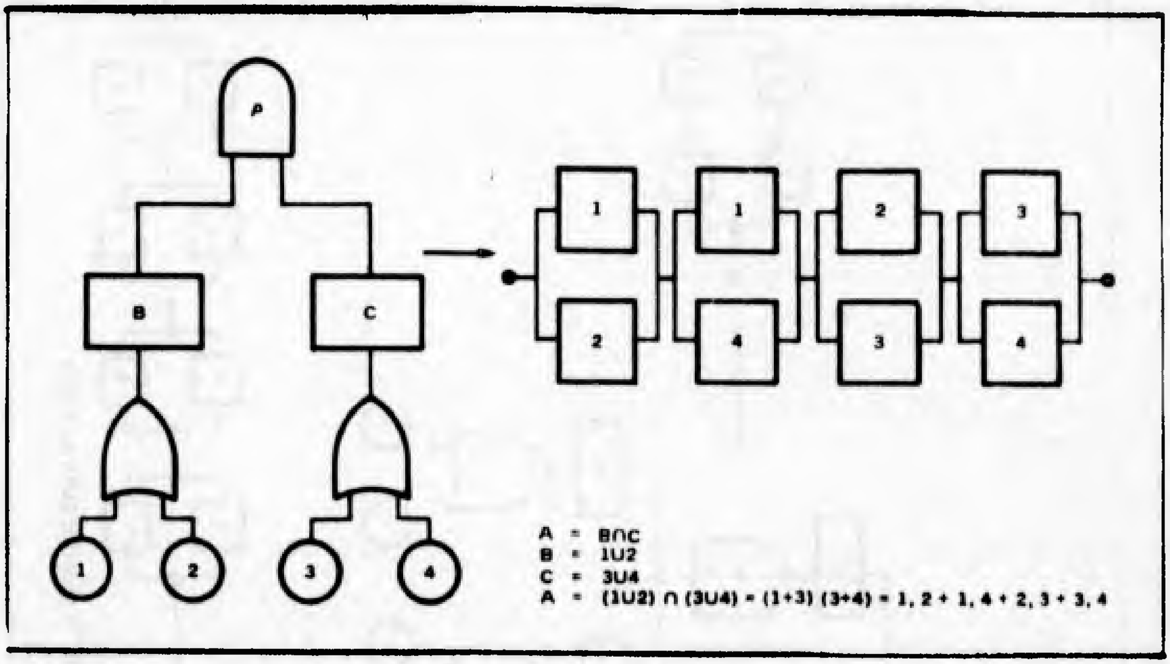
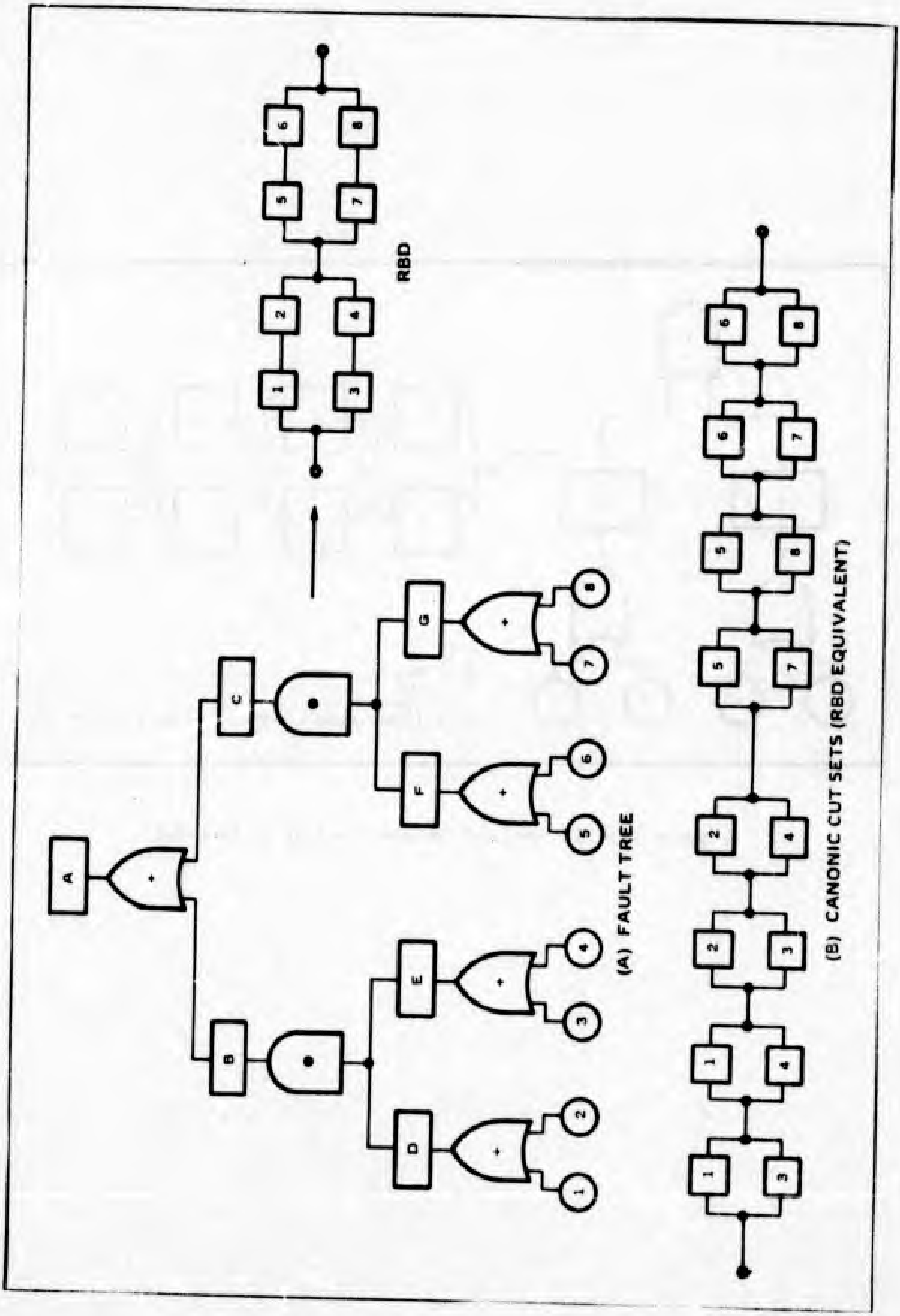


Figure 3.3.10 Critical Fault Tree



$$A = B \cap C$$
$$B = 1 \cup 2$$
$$C = 3 \cup 4$$
$$A = (1 \cup 2) \cap (3 \cup 4) = (1+3)\,(3+4) = 1,2 + 1,4 + 2,3 + 3,4$$

Figure 3.3.11 Boolean Determination of Cut Sets



(A) FAULT TREE

(B) CANONIC CUT SETS (RBD EQUIVALENT)

Figure 3.3.12

B Determining the Critical State Probabilities. There are several types of probabilistic outputs that can be derived from the identified cut-sets. Which outputs are selected will depend on the system structure, as well as its intended use. The following data types are possible:

1. Time-dependent failure data.

2. Time-dependent outage data.

3. Steady state outage data.

a. Time Dependent Failure. Time-dependent failure data is usually applicable to systems which have some specified mission time, and the item of interest is the probability that the system will fail during the mission. It is applicable to both repairable, and non-repairable systems. It is presently used by the FAA as one characteristic of site performance, where mission "length" is taken to be 24 hours. It really has little meaning as a performance criteria for repairable systems, in which the failure does not result in a catastrophic event. Since repair is still possible duration of the downtime would be of more interest. For systems, such as Automatic Landing Systems, particularly under Category III conditions (fully automatic to touchdown) it obviously has a serious meaning.

b. Time-Dependent Outage. Time-dependent outage data is concerned with failed state probabilities. It is applicable to repairable systems and gives the "transient" component of outage and availability. It can be very important when transient times are significant. It has been proposed for use in Electrical Power Distribution Systems where long repair times, resulting in long transient periods, are common. It may be applicable to FAA systems, when Criticality is used for near real-time control.

c. Steady-State. Steady State Outage data is concerned with the failed state probabilities after the time dependence has died out. This produces the well known Availability, Unavailability outputs, which are extensively used as effectiveness measures. It provides the basis for the Criticality definitions and discussions on Section 3.0. Note however, that Criticality can be applied to any of the types of data discussed, and is not restricted to steady state conditions. When Criticality is used as a planning tool, it is the steady state outages that are of concern, since they reflect, in a real sense, service and financial losses.

For real-time control applications, or where long transients are present, the complete time history of Criticality may be required.

c. Deriving the Data. There are many methods of deriving the required data, the following being most popular.

d. Time dependent failure data on the cut sets (failure modes) is usually derived by assuming exponential failure and repair distributions, assuming the failure rate is very much smaller than the repair rate, and using what is called the "Lambda-Tau" approximation. Each cut set is assumed to be composed of independent elements, thus the element probabilities simply multiply. The probability of a cut set is then given by,

$$P_j = \prod_i \lambda_i T \text{ , } i = 1, 2, 3 \cdots n \text{ ELEMENTS IN A CUTSET}$$

Where T is the "mission" length, or whatever time interval is of interest. For repairable, redundant systems, an equivalent failure rate must be determined for use in the equation. The equivalent lambdas for various structures (AND, OR) are given in Table 3.3.2.

b. Time-dependent outage data. This data can be obtained in various ways. The stochastic differential equations may be solved using Laplace transofrms, or z transforms for difference equations (reference 14, and 16). Matrix methods using eignevalues and eigenvectors may also be used. Reference 2 obtains a complete time history of availability, unavailability, reliability, and unreliability by a method termined by the author "Kinetic Tree Theory." He has written a computer program for the method, and it is described in reference 1. This program can be modified to provide complete time-dependent Criticality outputs, and has been used in the evaluation of Criticality for the Long Range Radar Site, reference 11. It is designed for Fault Tree evaluation and is recommended to contractors doing Criticality Analysis. It is available from the FAA or Idaho Nuclear.

c. Steady State outage data. This is the type of data usually required for planning purposes. It is obtained as an output of the computer program described above when time becomes long. For small, non-complex systems manual (or simple computer programs) methods can be used, by approximating the cut set probabilities by another "lambda tau" simplification. The cut set probability is given by,

$$P_j = \prod_i \lambda_i \tau_i \text{ , } \lambda_i \ll \frac{1}{\tau_i}$$

			2 INPUTS	3 INPUTS	n INPUTS
AND	's UNEQUAL	λ	$\lambda_1\lambda_2(\tau_1+\tau_2)$	$\lambda_1\lambda_2\lambda_3(\tau_2\tau_3+\tau_1\tau_3+\tau_1\tau_2)$	$\lambda_1\lambda_2\cdots\lambda_n(\tau_2\tau_3\cdots\tau_n+\tau_1\tau_3\cdots\tau_n$ $+\cdots+\tau_1\tau_2\cdots\tau_{n-1}$
		τ	$\frac{\tau_1\tau_2}{\tau_1+\tau_2}$	$\frac{\tau_1\tau_2\tau_3}{\tau_2\tau_3+\tau_1\tau_3+\tau_1\tau_2}$	$\frac{1}{\frac{1}{\tau_1}+\frac{1}{\tau_2}+\cdots+\frac{1}{\tau_n}}$
	's EQUAL	λ	$2\lambda_1\lambda_2$	$3\lambda_1\lambda_2\lambda_3{}^{2}$	$n\lambda_1\lambda_2\cdots\lambda\tau^{n-1}$
		τ	$\frac{\tau}{2}$	$\frac{\tau}{3}$	$\frac{\tau}{n}$
OR	's UNEQUAL	λ	$\lambda_1+\lambda_2$	$\lambda_1+\lambda_2+\lambda_3$	$\lambda_1+\lambda_2+\cdots+\lambda_n$
		τ	$\frac{\lambda_1\tau_1+\lambda_2\tau_2}{\lambda_1+\lambda_2}$	$\frac{\lambda_1\tau_1+\lambda_2\,2+\lambda_3\tau_3}{\lambda_1+\lambda_2+\lambda_3}$	$\frac{\lambda_1\tau_1-\lambda_2\,2+\cdots\lambda_n\tau_n}{\lambda_1+\lambda_2+\cdots+\lambda_n}$
	's EQUAL	λ	$\lambda_1+\lambda_2$	$\lambda_1+\lambda_2+\lambda_3$	$\lambda_1-\lambda_2+\cdots\lambda_n$
		τ	τ	τ	τ

TABLE 3.3.2 Lambda Tau Technique for Fault Tree Evaluation

The tau is this case is the Mean-time-to-repair, or mean time in the Critical state (rather than mission time as in the previous application). Table 3.3.2 can be used to find equivalents to complex AND, or OR structures.

3.4 Equipment Analysis

3.4.1 Equipment Analysis. A physical and performance analysis of the system equipment, layout, and location is necessary to determine the relation of Critical system functions to hardware, and to incure that all possible failure modes are included in the Fault Tree, including those that might be due to environments, layouts, or locations. Relating the Critical functions, to physical hardware permits failure and repair rates to be related to these functions. In order to construct the Fault Tree we must know the actual or proposed hardware implementation of the various functions which are used as top level events in the Fault Tree. Once the logical relationship has been established and the failure/repair rates of the associated equipment determined, the Fault Tree program, or manual methods can then be used to determine the probability of the Critical Failure Mode involving that Critical function. All NAS hardware is related to some top level NAS function. Reference 7 of Appendix A identifies 17 major functions in the NAS, which are correlated with 10 services performed by the NAS. The 17 functions were ultimately broken down into 265 sub-subfunctions or tasks. Since the interest was only in fucntions and tasks, there was no association with hardware. It is not difficult however, to make this association, and Table 3.4.1 shows this in matrix form. The abscissae are NAS equipments at subsystem level, while the ordinates show the 17 major functions. A "P" in the box indicates that the hardware has a prime role in the functions, while an "S" indicates a supporting, or secondary role. In the case of an advanced, non-operational system like the DABS it is duplicating the function of some other equipment as shown. In reality only one or the other would probably be operational, at a particular time.

This matrix may be used with the Function-Service matrix, Table 3.2.2a to estimate the importance of the system function and/or hardware. This in turn can be used to establish Criticality requirements for the various equipments, as discussed in Section 3.0.

All NAS hardware provides either a service, or data to support a particular function or functions. These data or services can then be related to the functions, which would provide an intermediate step to Table 3.4.1. The data or service can more easily be related to the particular system hardware. For example in the case of the Long Range Radar (LRR) it basically supplies data to the ARTCC. It supplies two major types of data - wide band, and narrow band. These data are principally used to support function #6, "Monitor Aircraft Progress." This is one of the prime functions of the ARTCC in support of the NAS. Hardware implementation of these data types at the LRRS is shown in a top level schematic in Figure 3.2.1. Each function can be individually laid out with its supporting hardware in this simple example. More complex systems may show a much greater degree of overlap in the hardware implementation. Data such as this will permit construction of the CBD or the Fault Tree.

The equipment performance and physical analysis consist in acquiring the hardware complement, defining the facility functions, associating the hardware with the functions, which in turn are related to higher level functions. The next step is to study the performance requirements and determine the capability loss resulting from a hardware failure. The capability is translated into a service or data interruption for incorporation into the Fault Tree or CBD. Degraded operation as well as total failure must often be considered.

Finally the effect of the phsycal layout, or surroundings must be studied to determine any possible failure modes that may result from this association. Since we are looking for events of very low probability, all possibilities must be initially considered. The actual steps, and outputs in the analysis are shown in the flow diagram of Figure 3.4.2. The equipment analysis provides the phsycail basis for the Criticality study, and must be carefully done to provide confidence in the study results.

3.5 Demand Analysis

A. Two State System-Function

An analysis of the demands on the various functions is necessary to determine the Q of the Criticality equation. Allowable delays in responding to the functional demands should also be an output of this analysis. This functional demand variation is reflected down to the facility equipment implementing the related sub-functions. Of the previously referenced 17 functions, only nine are considered Critical, these are:

1. Process Flight Plan
2. Issue Clearance
3. Monitor a/c progress
4. Maintain conformance with flight plan
5. Assure separation
6. Control Spacing
7. Provide Navigation Capability
8. Provide a/c guidance

NAS AIR TRAFFIC CONTROL & NAVIGATION SYSTEMS GROUND EQUIPMENTS NAS AIR TRAFFIC CONTROL AND NAVIGATION SYSTEMS TOP LEVEL FUNCTIONS P — PRIME S — SUPPORTING	1. AIR ROUTE SURVEILLANCE RADAR, ARSR	2. AIR TRAFFIC CONTROL RADAR BEACON, ATCRBS	3. COMMON DIGITIZER	4. RAPPI CONSOLES	5. DEFRUITERS	6. MAINTENANCE CONSOLES	7. BACKUP EMERGENCY COMMUNICATIONS, BUEC	8. RADIO MICROWAVE LINK, RML	9. TELCO	10. AIRPORT SURVEILLANCE RADAR, ASR	11. PRECISION APPROACH RADAR, PAR	12. AIRPORT SURFACE DETECTION EQUIPMENT, ASDE	13. INSTRUMENT LANDING SYSTEM, ILS	14. MICROWAVE LANDING SYSTEM, MLS	15. AUTOMATED RADAR TERMINAL SYSTEMS, ARTS	16. RUNWAY VISUAL RANGE, RVR	17. TERMINAL VHF OMNI RANGE, TVOR	18. ENROUTE CONTROL SYSTEM, NAS STAGE A	19. REMOTE COMMUNICATION AIR GROUND, RCAG	20. VHF OMNI DIRECTIONAL RANGE, VOR	21. TACTICAL AIR CONTROL AND NAV. TACAN	22. DISTANCE MEASURING EQUIPMENT, DME	23. DISCRETE ADDRESS BEACON SYSTEM, DABS	24. DIRECTION FINDER, DF	25. RADIO BEACON, RB	26. WEATHER RADAR, WR	27. AIRPORT TERMINAL INFORMATION SYSTEM, ATIS	28. FLOW CONTROL FACILITY
1. PROVIDE FLIGHT PLANNING INFORMATION															S			S								S	S	P
2. CONTROL TRAFFIC FLOW	S	S	S																									P
3. PREPARE FLIGHT PLAN																										S	S	P
4. PROCESS FLIGHT PLAN															P													
5. ISSUE CLEARANCES AND CLEARANCE CHANGES															P													
6. MONITOR AIRCRAFT PROGRESS	P S	P	S		S		S	S	S									P	P	S	S	S	P	S	S			S
7. MAINTAIN CONFORMANCE WITH FLIGHT PLAN	S	S	S		S		S	S	S									P	P	S	S	S	P	S	S			
8. ASSURE SEPARATION OF AIRCRAFT	P S	P S	S		S		S	S	S									P	P	S	S	S	P	S	S			
9. CONTROL SPACING OF AIRCRAFT	P S	P S	S		S		S	S	S			P						P	S	S	S	S	P	S	S			
10. PROVIDE AIRBORNE, LANDING & GROUND NAV. CAPABILITY										P	P	S	P	P	P	S	P		S									
11. PROVIDE AIRCRAFT GUIDANCE	P S	P S	S		S		S	S	S									P	S	S	S	S	P	S	S			S
12. ISSUE FLIGHT ADVISORY & INSTRUCTIONS	S	S	S		S		S	S	S									S	P	S	S	S	P	S	S			
13. HANDOFF	S	S	S				S	S	S									S	P	S	S	S	P	S	S			
14. MAINTAIN SYSTEM RECORDS		A	L	L																								
15. PROVIDE ANCILLARY AND SPECIAL SERVICES															P			P										
16. PROVIDE EMERGENCY SERVICES	S	S	S				S	S	S									S	P	S	S	S	P	S	S			
17. MAINTAIN SYSTEM CAPABILITY & STATUS INFORMATION	S	S	S	P		P	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S

TABLE 3.4.1 Equipment/Function Relation

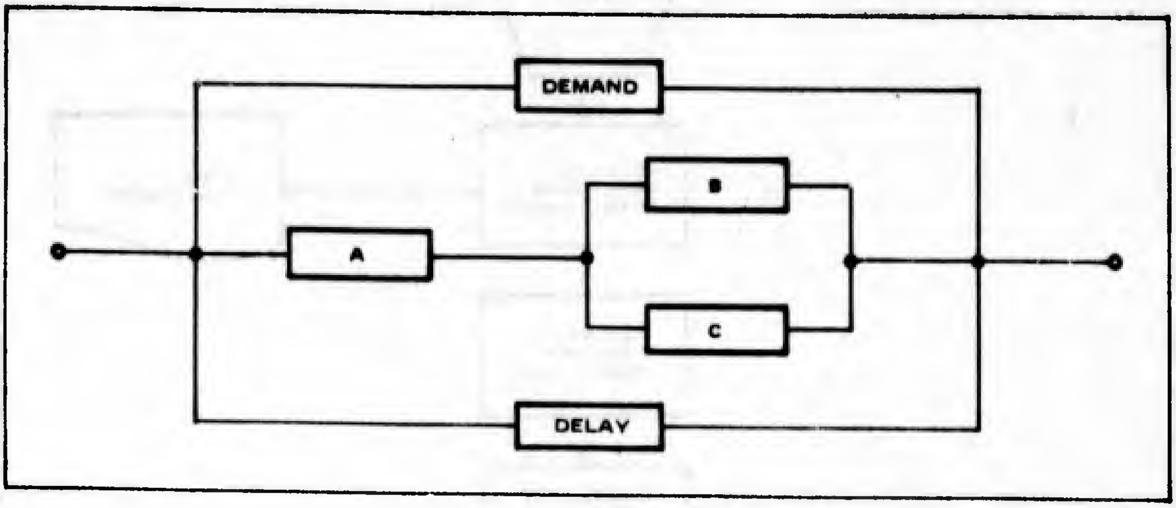


Figure 3.4.1 Criticality Block Diagram

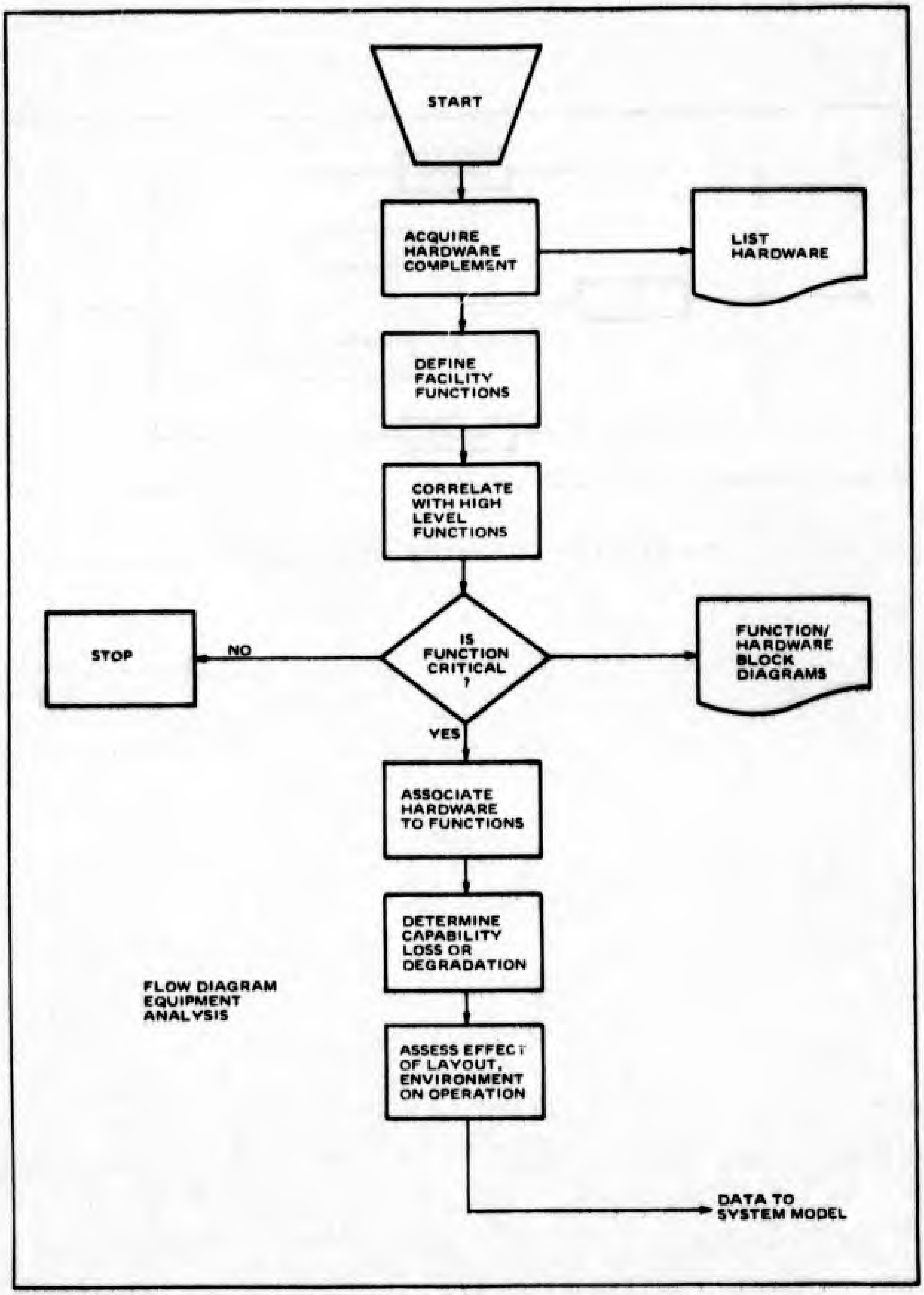

START
ACQUIRE HARDWARE COMPLEMENT
LIST HARDWARE
DEFINE FACILITY FUNCTIONS
CORRELATE WITH HIGH LEVEL FUNCTIONS
IS FUNCTION CRITICAL ?
NO
STOP
FUNCTION/ HARDWARE BLOCK DIAGRAMS
YES
ASSOCIATE HARDWARE TO FUNCTIONS
DETERMINE CAPABILITY LOSS OR DEGRADATION
FLOW DIAGRAM EQUIPMENT ANALYSIS
ASSESS EFFECT OF LAYOUT, ENVIRONMENT ON OPERATION
DATA TO SYSTEM MODEL

Figure 3.4.2 Flow Diagram Equipment Analysis

9. Issue flight instructions

The relation of the NAS equipment to these functions is shown in Table 3.4.1. These equipments and the related function are Critical in the sense defined in this Handbook. The demand on these function in some instances is random. They are also non-stationary in the sense their statistical characteristics may change with the time of day, or the month of the year. Figure 3.5.1 illustrates one realization of the stochastic process of functional demand. For simplicity the process is considered as 2-state, that is demand-function up or down. Multi-state systems are considered in paragraph 3.1.5B. In the demand model of Figure 3.5.1 the parameters of importance are the mean duration of a demand m, and the mean duration of the period of no demand, n. The total period is generally 24 hours, following the usual traffic patters. By taking actual data on existing systems the parameters m and n may be determined for any function.

By assuming that these parameters are the means of exponential distributions the demand function can be treated in a manner similar to the functional failure. The study state probability of a demand is then given by

$$Q_i = m_i / (m_i + n_i), \quad i = 1, 2, 3 \cdots n \text{ NUMBER OF FUNCTIONS}$$

where m + n = 24 hours in the usual case. Transient conditions are discussed in reference 4 and 12 (ch 10).

The demand and the function state may now be treated as two independent binary random processes, as shown in Figure 3.21a and b. The super process, "demand-function_, has four states, viz;

1. Demand up - function up DS

2. Demand down - function up $\bar{D}S$

3. Demand up - function down $D\bar{S}$

4. Demand down - function down $\bar{D}\bar{S}$

For Criticality analysis the only interest is in state 3, --demand up, function down, DS. This is the Critical State, C . Since the random processes are binary, and independent, the steady state probability of DS is

$$C_i = (P_i) Q_i$$

P_i = probability system is down.

Q_i = probability demand is up.

This super state is illustrated in Figure 3.5.2c.

The allowable delay in restoring a function is also a random variable, since it, too, will depend on the traffic density and the environment. Some functions may, in genreal, be more "important" than others, however, when a function is needed it usually assumes primary importance. Functional importance is considered in Section 3.0 at the top level of Criticality allocation. Assuming an exponential distribution for allowable delays (given the function has failed when needed), then

$$P_d(t > T) = e^{-\mu_i t}$$

A delay of one-half to one hour in restoring a NAS Critical function is generally accepted as reasonable. Flow control procedures operate on the basis that a one-hour delay can be absorbed before action must be taken (ref 23). NOTAMS use a delay of one hour in equipment restoration before they are issued (ref 23). Earlier in Section 3.0, Criticality requirements were established on the basis of a 10^{-4} probability of exceeding one-half hour delay. It seems reasonable then to use one-half hour as the standard acceptable delay, in which case the delay factor becomes

$$e^{-k_i/d_i} = e^{-0.5/d_i}$$

where k_i = 0.5 acceptable delay

d_i = mean down time in the Critical State

The Critcality equation is then,

$$C_i = P_i Q_i e^{-k_i/d_i}$$

C_i = PROBABILITY OF BEING IN A CRITICAL STATE

P_i = PROBABLITY OF A FUNCTIONAL FAILURE

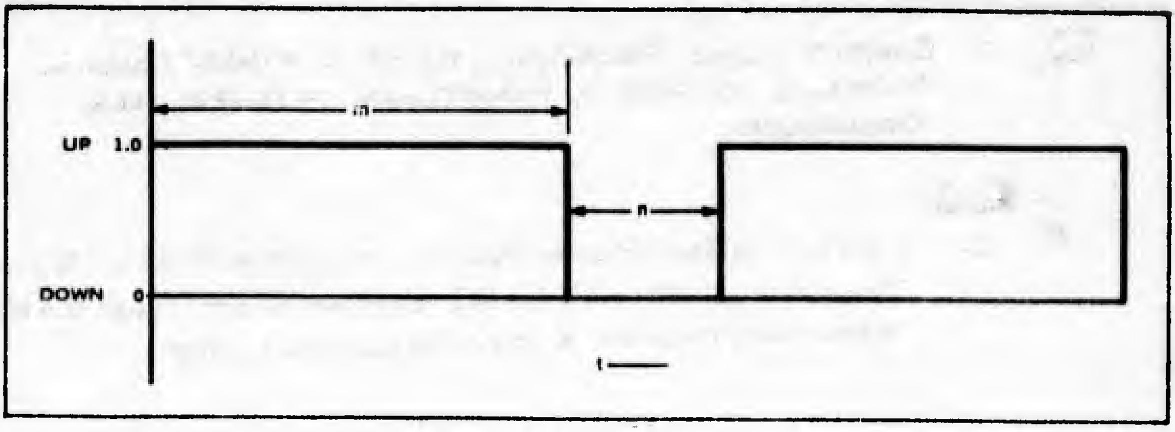


Figure 3.5.1 Demand Model

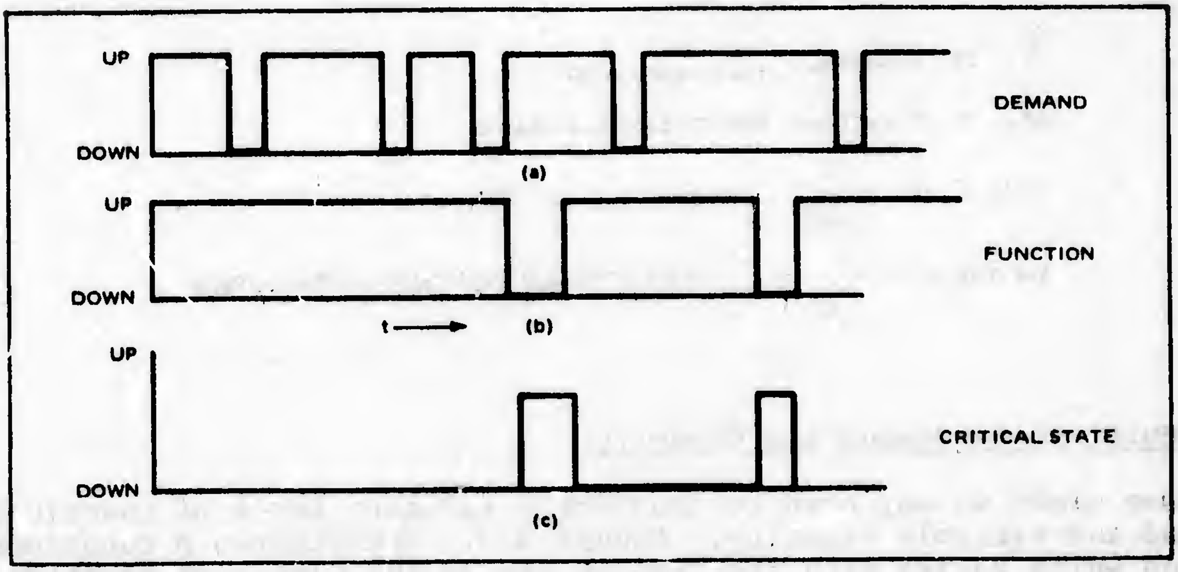


Figure 3.5.2 Superstate Model

Q_i = CONDITIONAL PROBABILITY OF A FUNCTIONAL DEMAND, GIVEN A FUNCTIONAL FAILURE HAS OCCURRED.

e^{-k_i/d_i} = CONDITIONAL PROBABILITY THE CRITICAL DOWN TIME WILL EXCEED k_i GIVEN THAT THE SYSTEM HAS SUSTAINED A CRITICAL FAILURE.

The acceptable delay time can be set at any value, depending upon the particular application of the Criticality Analysis. However, for most FAA NAS applications following the methodology of this Handbook, one-half hour is a reasonable level. For worst case analysis the demand is assumed continuous, with no delay allowed. Criticality is then simply outage (unavailability) probability.

$$C_i = P_i = \frac{\lambda_i}{\lambda_i + \mu_i} \text{ OR } = \frac{MDT}{MDT + MTBF}$$

λ_i = FUNCTION FAILURE RATE

μ_i = FUNCTION RESTORATION RATE

$MDT = -\frac{1}{\mu_i}$, MEAN DOWN TIME

$MTBF = \frac{1}{\lambda_i}$, MEAN TIME BETWEEN FAILURES

B. Multi-State Demand and Capacity

In some cases we may have to consider a variable level of functional demand and variable capacity. Figure 3.5.3 illustrates a functional demand which varies with the time of day in the number of functional units required.

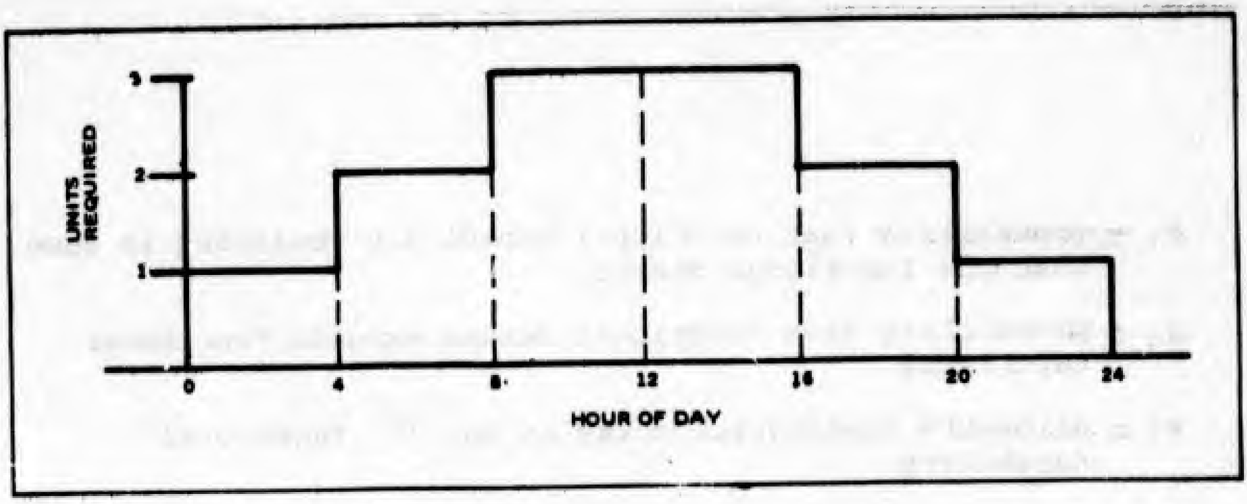


Figure 3.5.3 Typical Daily Demand

This can be decomposed into a set of binary demands as in Figure 3.5.4.

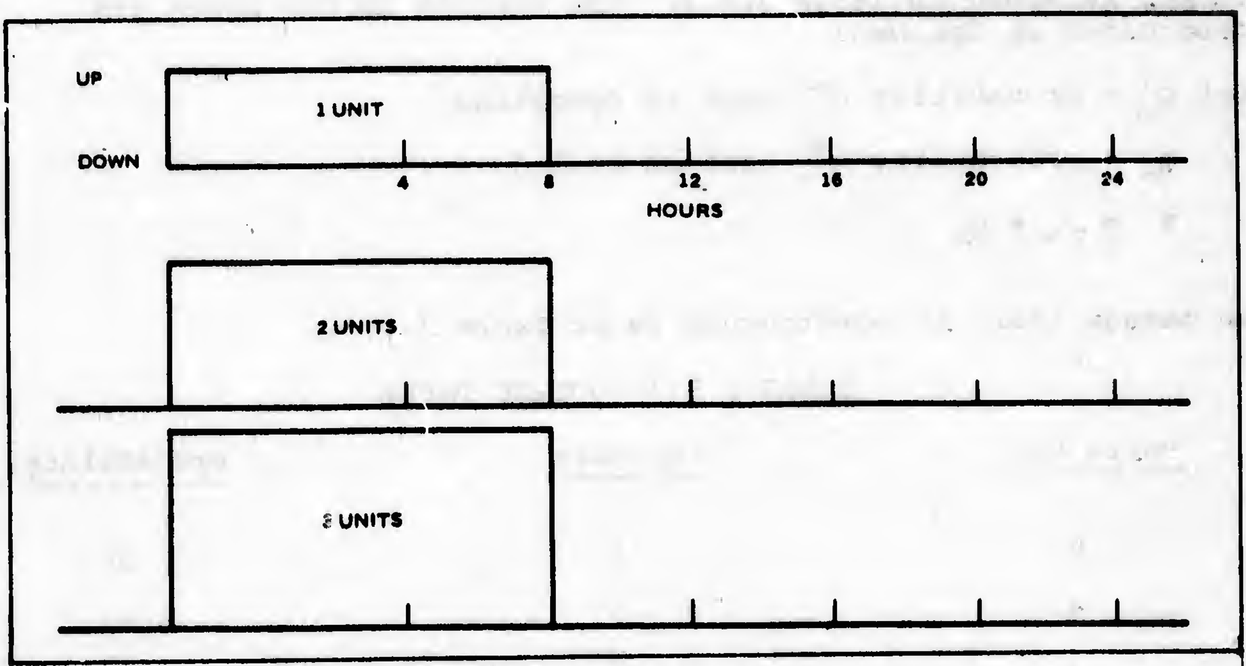


Figure 3.5.4 Binary Demand Model

The probability of each demand at any random time in the future is

P (1) = 8/24 = 1/3 demand for 1 unit

P (2) = 8/24 = 1/3 demand for 2 units

P (3) = 8/24 = 1/3 demand for 3 units

Consider a random capacity of one, two, or three units, then the Criticality of each of the functional levels may be calculated

P_i = probability that functional capability remaining is less than the functional demand

Q_i = probability that functional demand exceeds functional capability

k_i = allowable restoration delay in the i^{TH} functional capability

d_i = duration of i^{TH} functional outage

The C_i's in this case are summations since there may be many ways in which a particular level of functional demand cannot be met. The calculations are best carried out (manually) with the aid of a table, as shown in Table 3.5.3. The entries in the boxes are determined as follows:

Let p_n = probability n^{TH} unit is operating

q_n = probability n^{TH} unit is failed

$1 = p_n + q_n$

an outage table is constructed as in Table 3.5.1.

TABLE 3.5.1 OUTAGE TABLE

Units Out	Capacity	Probability, P_n
0	3	p^3
1	2	$3p^2q$
2	1	$3pq^2$
3	0	q^3

The joint probabilities, P , in each box are determined as follows:

$P_{ij} = P_D P_N$, i.e., the probability of demand times the probability of of functional failure.

In each box is also entered the difference of capacity and demand, S-D, where S is the system capacity and D is the demand on the system.

Criticality is the probability that the demand will not be met, thus it is the sum of the boxes containing negative entries, i.e., (assuming no allowable delay in restoration for simplicity).

TABLE 3.5.2

JOINT PROBABILITY

$p_{10} = 1/6\ q^3$	$p_{11} = 1/6\ 3pq^2$
$p_{20} = 1/6\ q^3$	$p_{21} = 1/6\ 3pq^2$
$p_{30} = 1/6\ q^3$	$p_{31} = 1/6\ 3pq^2$
$p_{12} = 1/6\ 3p^2q$	$p_{13} = 1/6\ p^3$
$p_{22} = 1/6\ 3p^2q$	$p_{23} = 1/6\ p^3$
$p_{32} = 1/6\ 3p^2q$	$p_{33} = 1/6\ p^3$

		Units Capacity/Pn			
Time-of-Day	Units Demand P_D	$\frac{0}{P_0}$	$\frac{1}{P_1}$	$\frac{2}{P_2}$	$\frac{3}{P_3}$
0000-0400	$\frac{1}{1/6}$	P_{10} -1 *■	P_{11} 0	P_{12} +1	P_{13} +2
0400-0800	$\frac{2}{1/6}$	P_{20} - 2 ■	P_{21} -1 ■	P_{22} 0	P_{23} +1
0800-1200	$\frac{3}{1/6}$	P_{30} -3 ■	P_{31} -2 ■	P_{32} -1 ■	P_{33} 0
1200-1600	$\frac{3}{1/6}$	P_{30} -3 ■	P_{31} -2 ■	P_{32} -1 ■	P_{33} 0
1600-2000	$\frac{2}{1/6}$	P_{20} -2 ■	P_{21} -1 ■	P_{22} 0	P_{23} +1
2000-2400	$\frac{1}{1/6}$	P_{10} -1 ■	P_{11} 0	P_{12} +1	P_{13} +2

*■ indicates deficiency

TABLE 3.5.3

ANALYSIS TABLE

$$C = P_{10} + P_{20} + P_{21} + P_{30} + P_{31} + P_{32} + P_{30} + P_{31} +$$

$$P_{32} + P_{20} + P_{21} + P_{10}$$

$$C = 2P_{10} + 2P_{20} + 2P_{21} + 2P_{30} + 2P_{31} + 2P_{32}$$

$$C = 2\left[\frac{1}{6}/q^3 + \frac{1}{6}/q^3 + \frac{1}{2}/3pq^2 + \frac{1}{6}/q^3 + \frac{1}{6}/3pq^2 + \frac{1}{6}/3p^2q\right]$$

$$C = 2\left[\frac{3}{6}q^3 + 3pq^2 + \frac{1}{2}p^2q\right]$$

$$C = q^3 + 6pq^2 + p^2q$$

The table defines the 12 possible states of the supersystem (demand-capacity), the steady state probabilities of various capacity states are obtained from the elementary binary formulas

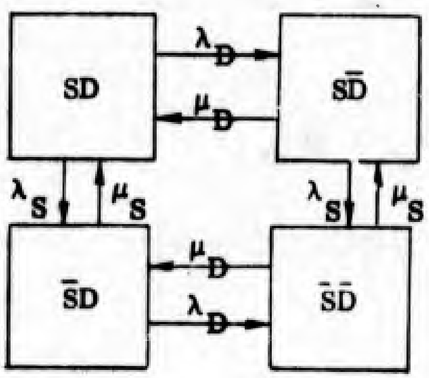
$$P = \frac{\mu}{\lambda+\mu} \quad \& \quad Q = \frac{\lambda}{\lambda+\mu}.$$

The frequency and duration of the Critical States can be determined as follows:

Each Critical State, that is one showing negative capacity, has a frequency given by

$f_i = P_i(\mu_i + \lambda_{D_i})$, λ_{D_i} IS THE RATE OF DEPARTURE OF FUNCTIONAL DEMAND $(\lambda_{D_i+} + \lambda_{D_i-})^*$ AND μ_i IS THE RATE OF RESTORATION OF FUNCTIONAL CAPABILITY $(\mu_{i+} + \mu_{i-})^*$

This is illustrated in Figure 3.5.5 for a single element, single function, single demand level system. *Note: The rate of departure may be composed of two rates, that is, rate of departure to a higher or lower demand state, or higher or lower capacity state. This is true for example, of States 1 and 2, and Demand Levels 1 and 2. Detailed state diagrams should be drawn to assist in determining the proper rates of departure.



S - System

D - Demand

The Critical State is $\bar{S}$ D, system down, demand up

Figure 3.5.5 System/Demand Transitional States

The rate of departure from the Critical State, is the sum of departing via restoration, or via termination of demand. i.e., $\mu_s + \lambda_D$.

The total frequency is approximated by,

$$f = \sum f_i$$

The expected time in the Critical State is then given by

$$d = C/f = \frac{1}{\mu_s + \lambda_D}$$

These equations are the same as those in Section 3.0 where systems with binary demands and capability were considered.

C. <u>Demand Duty Cycles and Probabilities</u>

The functional demand duty cycles and probabilities are most easily obtained from the Functional Analysis results. For existing systems, observation of the function demand over a period of time can produce the required data.

The data may also be deduced from facility operating procedures, or traffic pattersn. Some facilities simply shut down a functional capability for some period of the day. An average traffic pattern, as in Figure 3.5.6 may be correlated with functional demand. The probability of demand from recorded data is given by :

$$P_D \text{ Probability of demand} = \frac{\sum L_i d_i}{\text{time base}} = \frac{m}{m + n}$$

L_i = number of times demand appears

d_i = duration of demand

$$\text{Probability of no demand} = 1 - P_D = \frac{n}{m + n}$$

$\lambda_D = \frac{1}{m}$, $\mu_D = \frac{1}{n}$ $\quad$ m = expected duration of demand

n = expected duration of no demand

Peak Activity: 8-12 hours, maximum functional utilization

Moderate Activity: 4-8, 16-18 hours, medium functional utilization

Low Activity: 0-4, 18-24 hours, low functional utilization

For single functions the traffic pattern can also be used to estimate units of functional capability required.

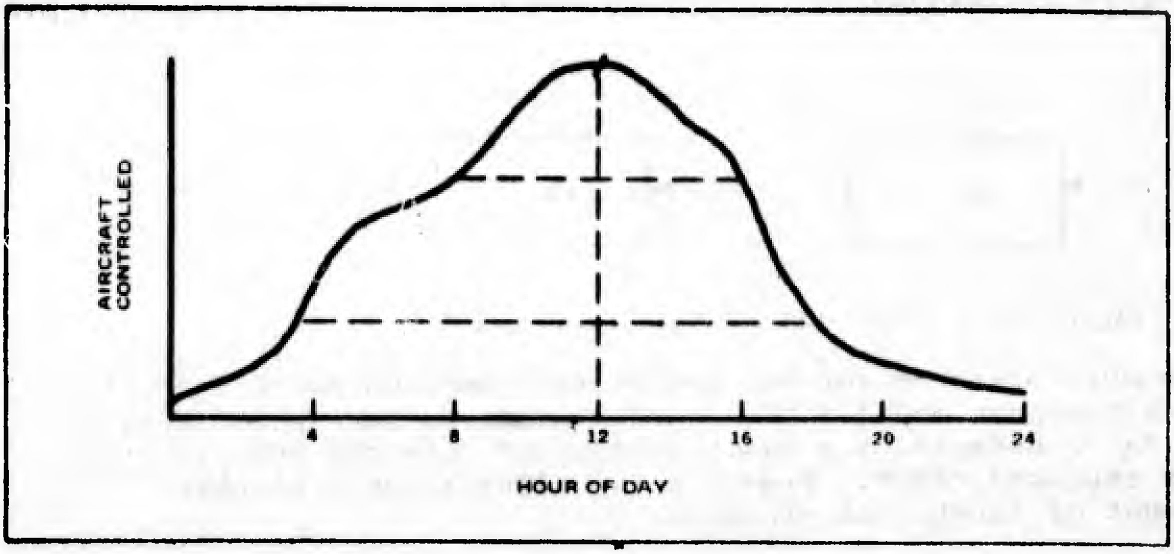


Figure 3.5.6 Typical Daily Demand Pattern

Weather statistics at the facility can also be used to deduce duty cycles on functions designed for poor weather operation, for example ILS.

Traffic altitude distributions can be used to deduce use of functions which may be sensitive to altitude, for example, clutter rejection functions. Any or all of these methods may be used to obtain a reasonable estimate of the frequency and duration of the various functional demands.

3.6 Criticality Block Diagrams

A. Logic Concepts

Upon completion of the foregoing 5 basic analyses, all the data is available for the Criticality Analysis. The two remaining tasks are a system model, and a suitable means of evaluation. For relatively simple, non-complex systems, or as a preliminary step, the Criticality Block Diagram is an adequate system model. It graphically depicts the functional relationships existing in the system. It is easily constructed using basic logical principles. For complex systems, or detailed analysis, the Fault Tree is a much more effective system model (see subparagraph 3.5.2.1). Both models are variants of logic diagrams, and some familiarity with logical propositions is required for understanding Logic symbology is covered in paragraph 3.5.2.1. In this section we need only to review the basic "AND," and "OR" logical concepts for an understanding of the CBD.

Criticality Analysis is a study of failure, which is complementary to success. A function either fails or succeeds. If degraded operation is permitted, we can still dichotomize the result into failed states and success states. Figure 3.6.1 shows two elements in a "series" configuration. Postulating that "A AND B must operate" for the associated function to succeed, then this is a "success model." The complimentary failure model states that if "A or B fails, the function fails." Note the complimentary "OR" has replaced "AND". Figure 3.6.2 illustrates a parallel arrangement of functional elements.

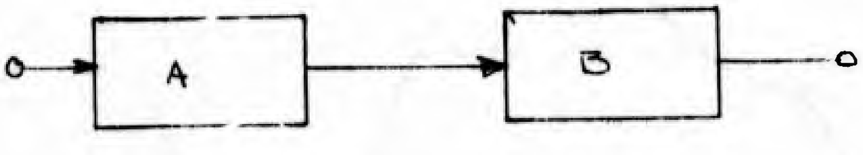


Figure 3.6.1 Criticality Logic of "A" and "B"

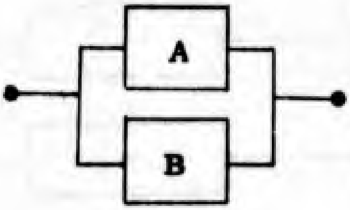


Figure 3.6.2 Criticality Logic of "A" or "B"

Now postulating that "A OR B must operate for system success," this is again a "success model." The complementary failure model states that if "A ANC B fail, the system faile." Again we have exchanged the "OR" for an "AND." Now we could represent failure models as in Figures 3.6.3 and 3.6.4, rather than the complementary representation which derived from considering success models. This would be more in keeping with our conditioning which tends to look at "parallel" configurations as redundant success models. However, less confusion appears to result by maintaining our reliability success model concepts and merely change the logical statement. It is important to standardize the symbology, and logical statements to avoid confusion when other factors, such as functional demand, and restoration delay, are added to the diagram. Some of this confusion is avoided in the Fault Tree by the use of additional symbology. Figure 3.6.5 summarizes the foregoing discussion, showing the relation of success and failure models in the parallel and series structures, where the reliability success model logic is retained.

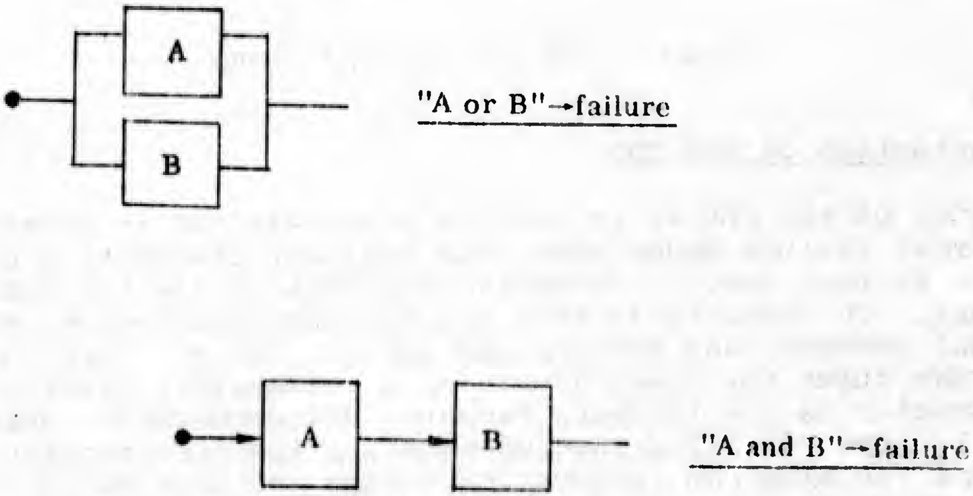


Figure 3.6.3 Summary of Previous Criticality Logic States

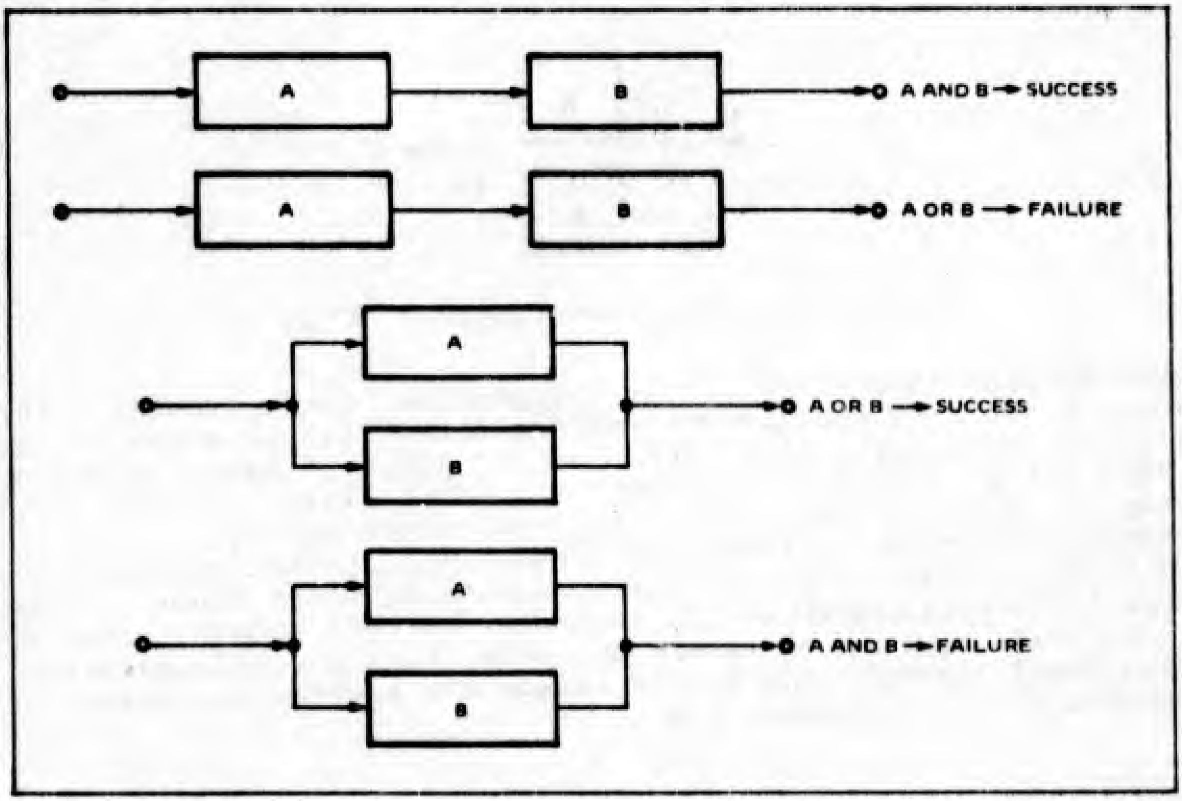


Figure 3.6.5 Logical Equivalents

B. Construction of the CBD

The purpose of the CBD is to provide a graphic aid in identifying the Critical Failure Modes (CFM) and Critical States of a system. This data is then used to determine Criticality and its associated parameters. In order to do this the CBD must incorporate the functional demands, and restoration delays. Construction of the CBD follows the rules for construction of a Reliability Block Diagram (RBD), insofar as the hardware elements are concerned. Reference 9, Chapter 7, gives detailed instructions for the construction of RBDs. The demand function and restoration delays are then added to the model as "AND"elements in accordance with the logic of Figure 3.6.5. Figure 3.6.6 illustrates a CBD for a single function system.

Logically the diagram states that $A \cup (B \cap C) \cap (\text{DEMAND} \cap \text{DELAY})$ failure. In words, A or (B and C) must fail, AND (demand must exist, AND restoration delay be exceeded), in order for failure to occur. This in turn is simply a statement of the Criticality equation

$C_i = P_i Q_i e^{-k_i/d_i}$

P_i = probability of the i^{TH} a Critical Failure Mode

Q_i = probability of the i^{TH} Functional Demand

k_i = allowable restoration delay in i^{TH} function

d_i = duration of the i^{TH} Critical State

In this simple system there is only a single function, and a single associated restoration delay. However, it is obvious from the diagram that there are two Critical Failure Modes (CFM) viz: loss of A, or the loss of B and C. The joint failure mode, i.e., loss of A and B, or A and C, are usually ignored because of their low probability of occurrence. Only the "minimal cut-sets" are considered, where a "cut-set" is equivalent to a Critical Failure Mode. A "minimal cut-set" is defined as the "minimum number of elements, which when failed, the function (or system) is failed." There are also two Critical States, C , one associated with each CFM, and

$$C_1 = P_A Q_A e^{-k_A/d_A} \quad \text{and} \quad C_2 = P_{BC} Q_{BC} e^{-k_{BC}/d_{BC}}$$

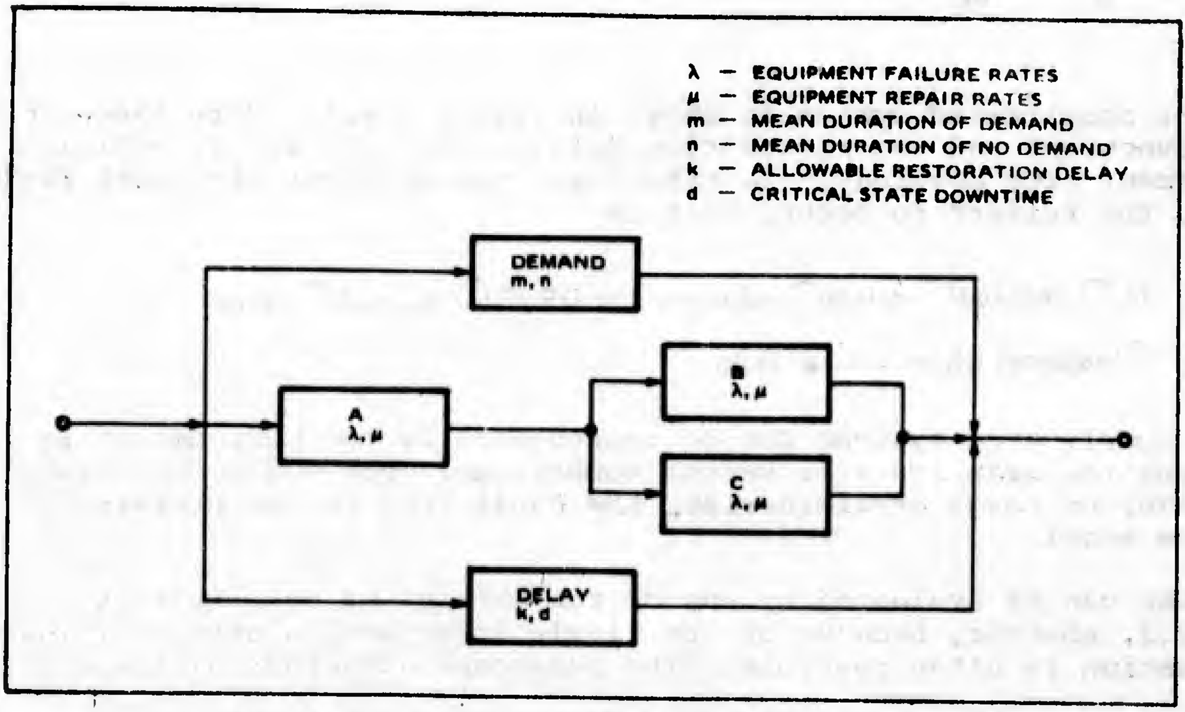

λ — EQUIPMENT FAILURE RATES
μ — EQUIPMENT REPAIR RATES
m — MEAN DURATION OF DEMAND
n — MEAN DURATION OF NO DEMAND
k — ALLOWABLE RESTORATION DELAY
d — CRITICAL STATE DOWNTIME
DEMAND
m, n
A
λ, μ
B
λ, μ
C
λ, μ
DELAY
k, d

Figure 3.6.6 Criticality Block Diagram

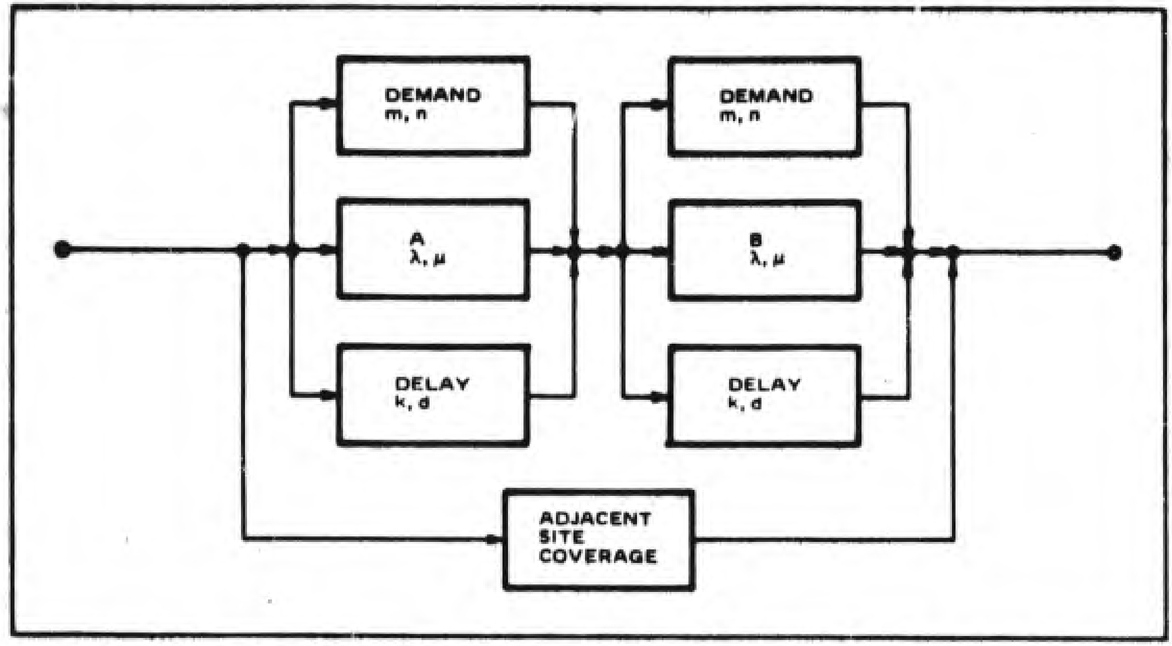


Figure 3.6.7 Multi-Function CBD with A$_{d}$jacent Site Coverage

Since there is only a single function involved,

$$Q_A = Q_{BC} \text{ and } e^{-k_A/d_A} = e^{-k_{BC}/d_{BC}}$$

A more complicated system is shown in Figure 3.6.7. Here there are two functions and two restoration delays involved, and in addition "adjacent site coverage." In this case, the adjacent site must fail also, for failure to occur, that is

$$(A \cap \text{demand} \cap \text{delay}) \cap \text{adjacent site OR } (B \cap \text{demand} \cap \text{delay} \cap \text{adjacent site}) \longrightarrow \text{failure}$$

More complicated systems can be represented by the CBD, but it is obvious the graphics will become combersome. For other than simple systems, or rough preliminaries, the Fault Tree is the preferred system model.

The CBD can be evaluated by any of the methods of subparagraph 3.5.2.2, however, because of its simple structure, a straightforward evaluation is often possible. The paramount advantage of the CBD is that the Critical Failure Modes are usually explicit, and can often be determined by inspection. Any failure that breaks the flow from input to output ("cuts the set") is a CFM. This simple visibility tends to be obscurred in the Fault Tree, often resulting in the need for more complex methods of determining the CFM.

A straightforward evaluation of the CBD is carried out in the following paragraphs using manual methods.

3.7 Evaluation of Criticality Block Diagrams

Evaluation of the CBD. The final task of the PCA is to evaluate the CBD to determine the following data:

1. The Critical Failure Modes and Critical States.

2. The probabilities of occurrence of the Critical Failure Modes, and the Critical States

3. The expected frequency and expected duration of the Critical Failure Modes, and the Critical States.

4. A ranking of the Critical States by probability of occurrence, that is, Criticality.

5. A ranking of the equipments by the magnitude of their contribution to the occurrence of the Critical States.

6. The overall system Criticality and the expected frequency-duration of the Critical States.

7. The expected occurrences per year of the Critical States, and the total expected downtime in the Critical States, that is, the expected loss of service.

For a system of even moderate complexity computer aid is required in the evaluation. As an example of the manual computations required, a single function, three element system Figure 3.24 will be analyzed.

A. Example of Analysis

The probability of occurrence of a Critical State (Criticality) C , is given by,

$$C_i = P_i Q_i e^{-k_i/d_i}$$

where

C_i = the probability of the i^{th} Critical State

P_i = the probability of the i^{th} Critical Failure Mode

Q_i = The Conditional probability of a demand on the i System function, given the function has failed.

e^{-k_i/d_i} = the probability that the mean time in the i^{th} Critical State d_i, will exceed the allowable downtime,k

Each failure mode, also called a "cut set" in graph theory, is composed of one or more elements. A "minimum cut set" is the smallest number of elements which, when failed, will fail the system.

In Figure 3.7.1 "A" is a minimum cut set of one element (single point failure) and BC is a minimum cut set of 2 elements. Neither AB, AC, or ABC are minimum cut set, since they include "A" which is a minimum cut set itself.

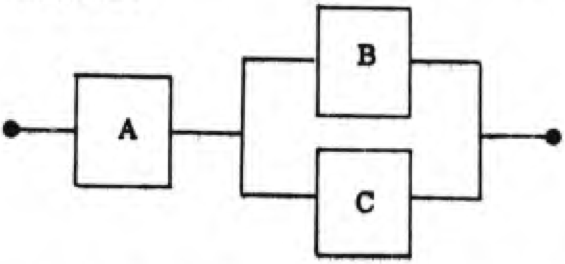


Figure 3.7.1 Criticality Logic for "A" Must Fail or "B and C" Must Fail

The probability of failure of the multiple element minimum cut sets, with 1/m required, is

$$P_i = \prod_{j=1}^{m} p_j$$

That is, all elements of the Critical Failure Mode must fail.

This assumes independent failures.

The total probability of a Critical Failure Mode is, approximately, the sum of the P_i,

$$P = \sum_{i=1}^{n} P_i$$

P_i = FAILURE OF THE i^{TH} CUT SET

n = NUMBER OF CRITICAL FAILURE MODES

This neglects the joint probability of the Critical Failure Modes. Methods for bounding this approximation are given in reference 10.

This approximation is an upper bound, i.e. worst case.

Assume a single functional demand on the system represented in Figure 3.6.7. A criticality Block Diagram is constructed by including the demand, and allowable delay as AND elements as in Figure 3.7.2. This representation follows the conventional reliability block diagram method such that delay and demand are shown as parallel elements. Logically, the figure says that:

"A" must fail or "B" AND "C" must fail.

AND demand must exist AND allowable delay must be exceeded for A Critical State to occur. In logical notation

$$C = P\,[\bar{A} \cup (\bar{B} \cap \bar{C}) \cap \text{demand} \cap \text{delay}]$$

Note: $\bar{A}$ = NOT A, that is, A has failed.

$\cup$ = union (OR)

$\cap$ = intersection (AND)

that is

$$C \underline{=} P\ Q\ e\ -t/d$$

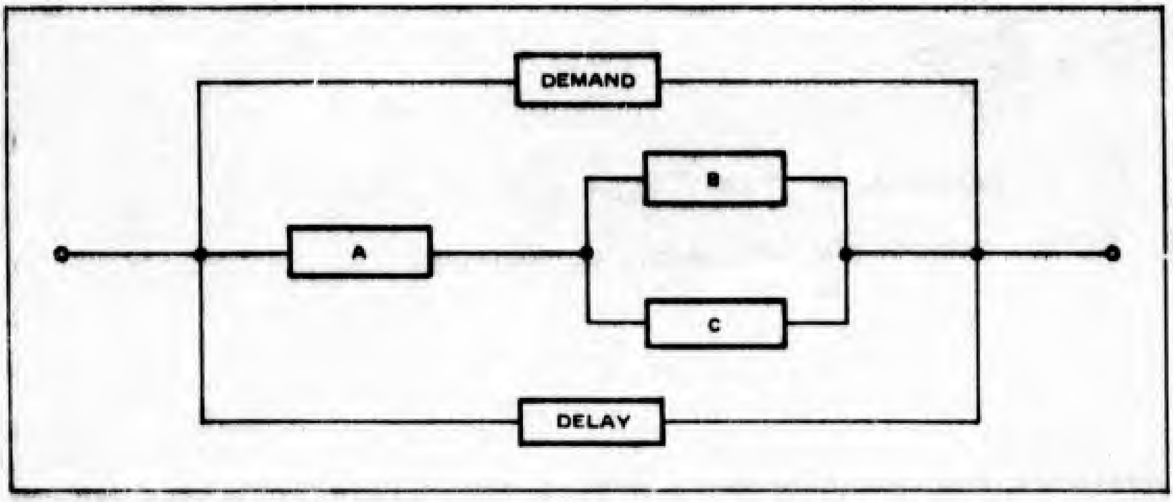


Figure 3.7.2 Criticality Block Diagram

where,

C = Criticality

P = the probability $A \cup (B \cap C)$

Q = The probability a demand exists

$e^{-k/d}$ = the probability that the downtime in the Critical State, d, exceeds the allowable k hours

The Criticality Analysis for this simple system can be carried out in a straightforward manner either manually or with the aid of a computer. Using the CBD as a graphic aid, the first step is to identify the Critical Failure Modes (minimum cut sets) of the system. From Figure 3.6.7 these are obviously failure of element A, or failure of elements B and C.

Thus A, and BC are the Critical Failure Modes.

Determining the Critical States requires incorporating the demand probability and allowable delay. Assuming that the System demand, System failure and restoration time are independent, then for the Critical Failure Mode involving A of Figure 3.6.7

$$C_A = P_A Q_A e^{-k_A/d_A}$$

WHERE,

P_A = PROBABILITY ELEMENT "A" FAILS

Q_A = PROBABILITY OF FUNCTION DEMAND GIVEN A FUNCTIONAL FAILURE

K_A = ALLOWABLE DELAY

d_A = CRITICAL STATE MEAN DOWN TIME

The Criticality of the BC Failure Mode is determined in a similar manner. In order to illustrate the method assume some numbers for the characteristics of the system. Table 3.7.1 shows the failure and repair rates. The allowable delay in restoration, k, is assumed to be one hour for both failure modes. This means that if repair or resotration is effected in less than an hour the system is not considered down.

TABLE 3.7.1

Element	Failure Rate/hr, λ_S	Repair Rate/hr, μ_S
A	$1 \times 10^{-4} = \lambda_1$	$0.2 = \mu_1$
B	1×10^{-2} $\Big\} = \lambda_2$	0.3 $\Big\} = \mu_2$
C	1×10^{-2}	0.3

λ_S = System failure rate

μ_S = System repair rate

The demand function is assumed to be on a daily basis, as in Figure 3.7.3.

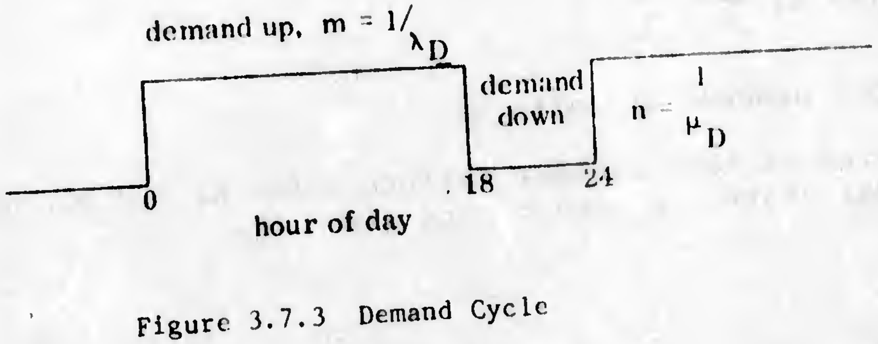


Figure 3.7.3 Demand Cycle

The probability of a demand at any random time in the future is given by,

$$Q = \frac{\mu_D}{\lambda_D + \mu_D} = \frac{18}{24} = 0.75$$

Note: $\lambda_D = \frac{1}{18}$; $m = 1/\lambda_D$ = mean duration of a demand, assuming an exponential density of time between demands.

$\mu_D = \frac{1}{6}$; $n = 1/\mu_D$ = mean duration of "no demand" assuming an exponential density of times between no demand.

Table 3.7.2 summarizes the failure modes, effects, and significant parameters.

TABLE 3.7.2

FAILURE MODE	FAILURE PROBABILITY	EFFECT	DEMAND PROBABILITY	DELAY $e^{-K/d}$
A	5×10^{-4}	Loss of all capability	0.75	0.775
BC	11.1×10^{-4}	Loss of all capability	0.75	0.520

where d is given by $\frac{1}{\mu_S + \lambda_D}$

The calculations proceed as follows:

The probabilities of the Critical Failure modes A, and BC, and the related Critical States, C and C are given by,

$$P_1 \approx \frac{\lambda_1}{\mu_1} = 10^{-4} \frac{1}{0.2} = 5 \times 10^{-4}, \text{ and}$$

$$C_1 = P_1 Q_1 e^{-k/d_1} = 2.9 \times 10^{-4}$$

$$P_2 \approx \lambda_2^2 \mu_2^2 = 10^{-4} \left(\frac{1}{0.3}\right)^2 = 11.1 \times 10^{-4}, \text{ and}$$

$$C_2 = P_2 Q_2 e^{-k/d_2} = 4.33 \times 10^{-4}$$

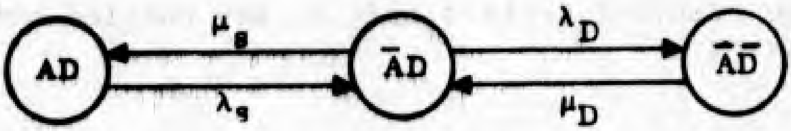
The expected time in the Critical State, d_1, is

$$d_1 = \frac{1}{\mu_1 + \lambda_D} = \frac{1}{0.2 + 0.056} = 3.9 \text{ hours}$$

The frequency of the Critical State is determined as follows

f_1 = C_1 x (rate of departure from Critical State)

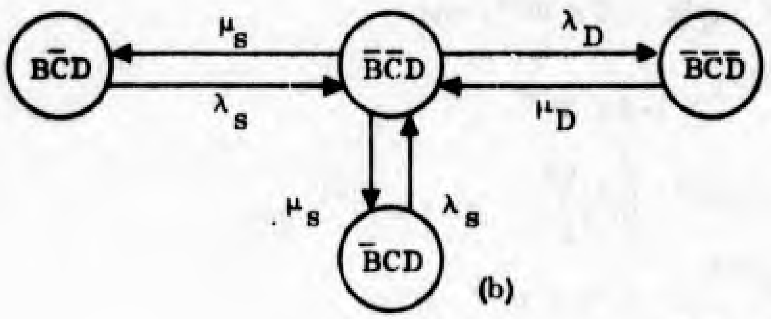
Figure 3.7.4 is a Critical State diagram, showing the Critical States and the rates of entry and departure to adjacent states.



CRITICAL STATE 1, element A down and D, demand, up

(a)

FIGURE 3.7.4 (PART 1)



(PART 2)

CRITICAL STATE 2, elements B and C down and D, demand, up

Figure 3.7.4 Critical States

Thus the frequency of Critical State 1, f_1 is

f_1 = C_1 x (rate of departure)=2.9 x 10^{-4} $(\mu_s + \mu_D)$

f = 2.9 x 10^{-4} (0.256) = 0.742 x 10^{-4} cycles per hour

Calculations for the Critical Failure mode BC are carried out in a similar fashion, giving

$$d_2 = \frac{1}{2\mu_s + \lambda_D} = \frac{1}{0.6 + 0.056} = \frac{1}{0.656} = 1.5 \text{ hours}$$

The frequency of the Critical State, f_2, is

$$f_2 = C_2\ (2\mu_s + \lambda_D) = 4.33 \times 10^{-4} \times 0.656 = 2.84 \times 10^{-4} \text{ cycles per hour}$$

TABLE 3.7.3

System Summary

Critical Failure Mode	Rank	Failure Description	Effect	10^{-4} Probability of Occurrence	10^{-4} Expected Frequency (events/hr)	Expected Duration (hours)	Annual Occurrences (Events)	Annual Lost Service (hours)	Weighting			10^{-4} Criticality	
									Demand	Delay	Other	C	Percent Total
1	2	Loss of element A	Total loss of function	5.0	0.742	3.96	0.65	2.54	0.75	0.775	–	2.0	40
2	1	Loss of elements B and C	Total loss of function	11.1	2.84	1.5	2.48	3.78	0.75	0.520	–	4.33	60
Totals					3.582	2.02	3.13	6.32				7.23	100

Table 3.18 (System Summary Sheet) summarizes the results of these calculations, and includes the system totals, where

$$C_T \simeq \sum_{i=1}^{2} C_i = (2.9+4.33)10^{-4}$$

$$= 7.23 \times 10^{-4}$$

$$f_T \simeq \sum_{i=1}^{2} f_i = (0.732+2.84)10^{-4}$$

$$= 3.572 \times 10^{-4}$$

$$d_T = \frac{C_T}{f_T} = \frac{7.23 \times 10^{-4}}{3.572 \times 10^{-4}}$$

$$= 2.02 \text{ HOURS}$$

Also the total expected hours of Critical downtime per year $D = (C_T) \times 8760 = 6.32$ hours

The Expected number of Critical events per year,

$N = f_T \times 8760 = 3.12$

The Critical States, can now be ranked by Criticality, percentage contribution to the total and possible reduction methods. Table 3.7.4 illustrates this. The cost of each possible reduction method can be computed, then along with the Criticality reduction obtained, will produce a Cost Effectiveness measure. For example, triple redundancy in cut set BC, will reduce the Criticality of that mode from

$C = 4.33 \times 10^{-4}$ and $d_2 = 1.5$ hours to

$C_2 \approx \lambda^3 \tau^3 \times 0.75 \times e^{-0.956} = 10^{-6} \times \frac{1}{0.027} \times 0.75 \times e^{-0.956}$

$\approx 0.1065 \times 10^{-4}$ and $d_2 = \frac{1}{0.9+0.056} = 1.05$ hours

TABLE 3.7.4

Critical State	(Criticality) Probability	Total %	Total Reduction Methods*
1	2.9×10^{-4}	40	1) Improve failure or repair rates
			2) Redundancy
2	3.33×10^{-4}	60	1) Triple redundance
			2) Improve failure, repair rates

*There are many more possible methods than shown.

3.8 Program Management

3.8.1 Management. The contractors organization is responsible for performing the Criticality Analysis in accordance with the requirements of the prime equipment specification, and the Criticality Analysis Methodology Specification (CAS). The responsibilities and functions of those directly associated with system Criticality Analysis must be clearly identified. Lines of communications engineering, safety and logistics must be established and maintained in order to insure propser feedback and implementation of recommended Criticality reduction techniques. Figure 3.8.1 illustrates the interfacing organizations, the data they supply, and the major outputs of the Criticality Analysis. Depending upon the Contractor's organization , the varioud disciplines may or may not be encompassed under the same organizational structure. Figure 3.8.2 depicts a typical organization which includes all of the disciplines under "Systems Analysis." In this diagram most of the support requirement groups are also under the same sub-organization of "Effectiveness." In the usual structure, the Criticality Analysis task would be included under the Reliability/Maintainability Branch, and/or the Operations Analysis Branch. It is an identifiable task which requires organizational structure for proper implementation. There must be an identifiable organizational element which is responsible for the management and control of the Criticality Analysis Program within the Contractor's organization.

3.8.2 Program Monitoring and Control. The Criticality Analysis manager is responsible for planning, implementing, controlling and reporting on all Criticality Analysis tasks. Reviews, audits, and milestones must be regularly scheduled and at intervals sufficient to provide proper lead time for corrective actions when necessary. A typical program, identifying the tasks, milestones, and program

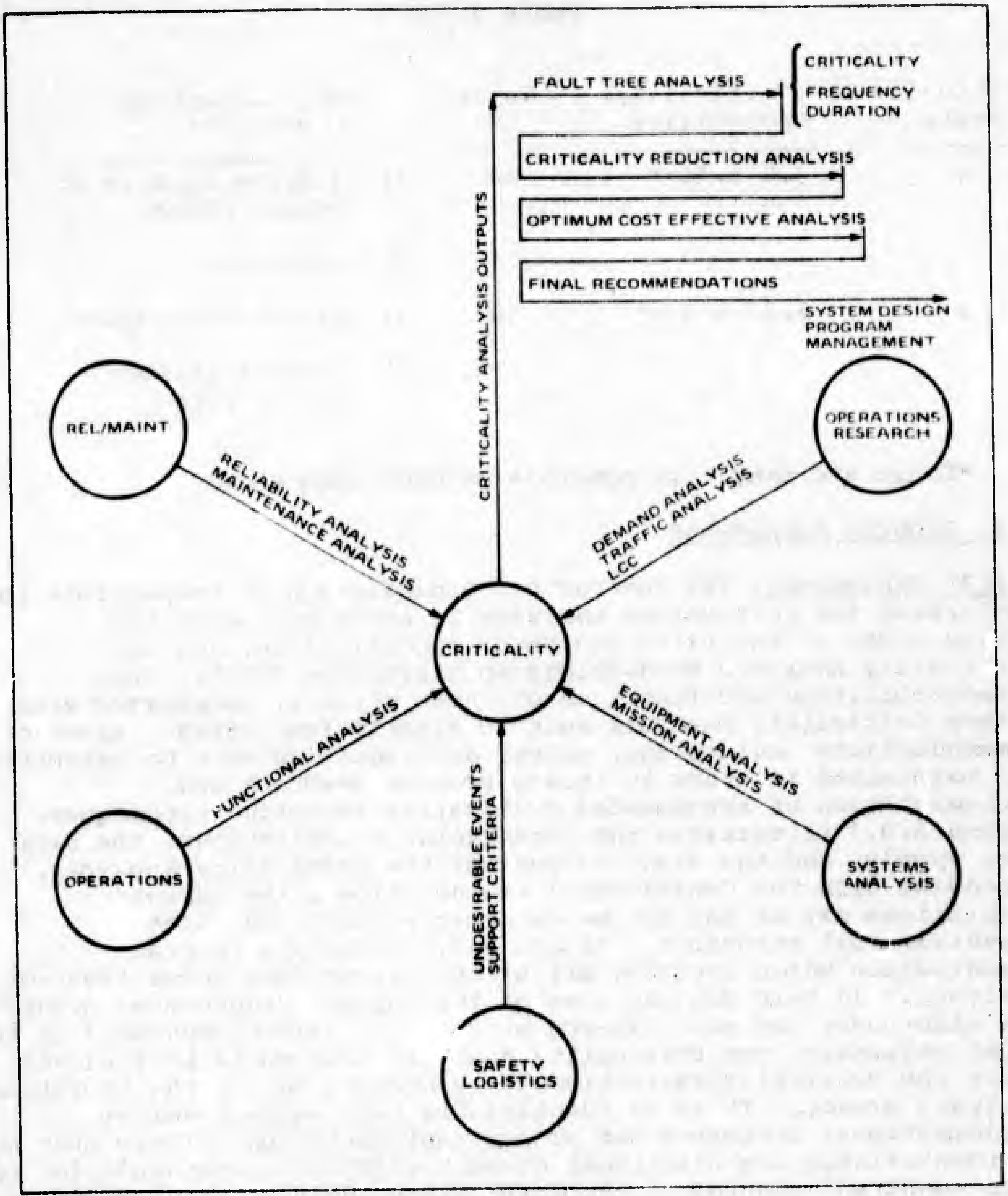


Figure 3.8.1 Criticality Interfaces

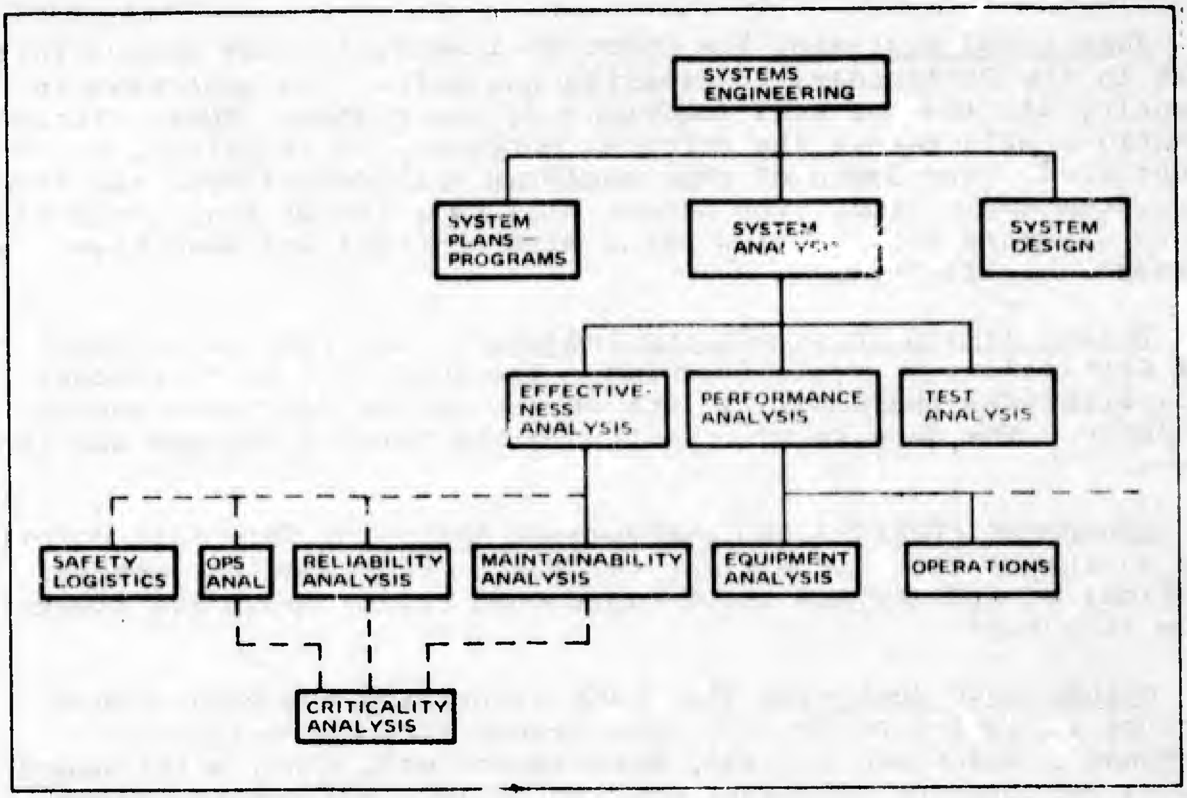


Figure 3.8.2 Organizational Structure

review intervals is shown in Figure 3.8.3 and described in the following paragraphs.

A. Typical Program Tasks:

1. Functional Analysis. The Functional Analysis task is the initial task in the Preliminary Criticality Analysis. Its objective is to identify all the Critical functions of the system. These Critical Functions will permit the critical hardware, if it exists, to be identified. The depth of this analysis will depend upon the level of system definition. The output will be a set of functional flow block diagrams showing flow paths with critical and sensitive elements highlighted.

2. Reliability/Maintainability Analysis. This task is an input to the Criticality Analysis function. The objective is to produce reliability/maintainability data on the system functions and/or hardware. The data is principally in the form of failure and repair rates.

3. Equipment physical and performance Analysis. This task compiles the equipment list and all the relevant performance parameters. Critical equipments and their functional relationship are identified from this task.

4. Maintenance Analysis. This task identifies the Maintenance Concept including preventive maintenance actions, maintenance personnel, maintenance tasks, maintenance equipment, maintenance costs, restoration policies, sparing policy, maintenance manual, documentation, reporting procedures, - that is, all aspects of maintenance. Its basic objective is to determine why and how a systems fails, and how it is restored or repaired. It is a key study in Criticality Analysis, when the level of system definition permits it to be accomplished.

5. Functional Demand Analysis. The objectives of this analysis is to determine the distribution(s) of the demand(s) on the various system functions(s). In addition it should also determine if there is a permissable delay in restoration of the function after it has failed. Guidance in this task is contained in paragraph 3.5.

6. Construct the Fault Tree. The Fault Tree is the detailed system model for the study of Criticality. It provides the principal graphic aid for the identification and quantitative evaluation of the Critical States of the system. Detailed guidance in construction of the tree is contained in paragraph.

7. Evaluate the Fault Tree. The Fault Tree is normally evaluated using special computer programs which have been developed and are available for contractor use.

8. Corrective Action Analysis. This task results from a failure to meet quantitative Criticality requirements. A more detailed study may be required to determine if corrective action is feasible.

9. Integrated Solutions and Life Cycle Cost Analysis. This task combined with corrective action analysis undertakes the search for integrated system solutions, i.e., elimination of Critical Failure Modes, and Life Cycle costing of these solutions. The objective is to keep all aspects of the study at the system level, including costing. The methodology of LCC must be fairly standardized to permit comparison of various solutions.

10. Analysis of Results. The results of the Criticality study, is in terms of Criticality levels, frequency/duration of Critical states, annual occurrences and lost service. The parameters which are chosen as most important vary with the NAS element being analyzed. For some Criticality may be paramount, for others frequency of occurrence, or duration of downtime, or total lost service. Each element must be studied in light of its prime function and relation to the overall NAS. When the results have been properly ranked and tabulated, the selection of the appropriate method of reduction is simplified.

11. Documentation. The documentation for the study consists in periodic reports, a final report, and specifically formatted tables summarizing the study findings. In support of the study, data must also be collected, and be available for inspection.

B. Milestones. Twelve significant milestones are identified in Figure 3.8.3. They represent typical program points at which important information is made available for study. These twelve milestones and their significance are briefly reviewed in the following paragraphs.

1. Significant functional failures identified. This is the fundamental data that drives the study. These identified functional failures or derivatives of them ultimately become the events in the Fault Tree. Careful study and evaluation at this point can reduce the complexity of later analyses.

2. Failure/Repair rates available. This is a basic data input which permits quantitative evaluation of Critical Failure Modes. When hardware is defined, this milestone is concurrent with the following milestone, relating function to hardware.

3. Function/Hardware Correlation. This is the step, when hardware is defined that correlates the failure/repair rate predictions into Critical Failure Mode identification.

4. Functional Demand Duty Cycles and Restoration Delays Established. This important milestone should be used to review the data which will be used to determine the Q of the Criticality equation. It is

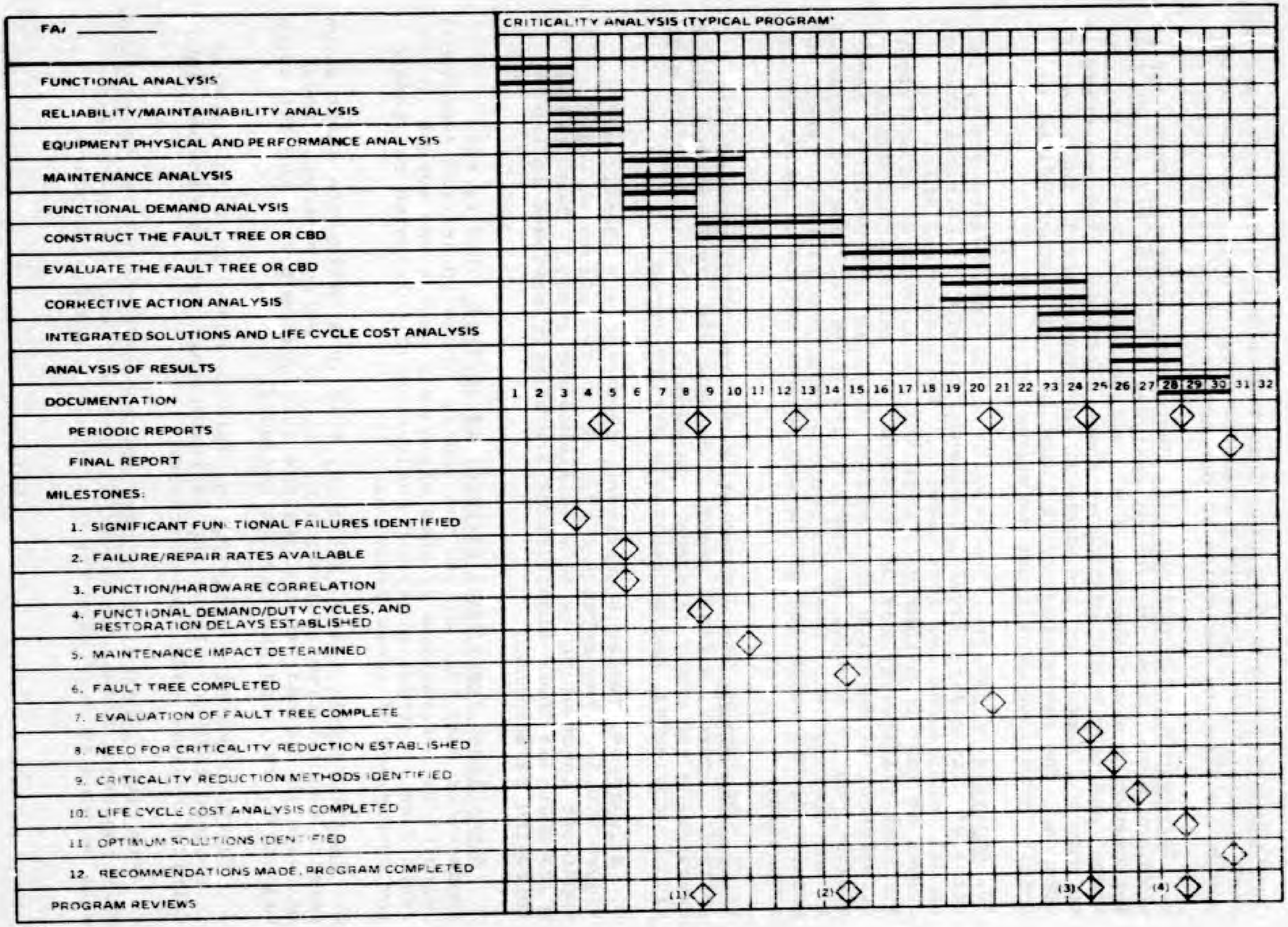


Figure 3.8.3 Typical Program Schedule/Milestones

probably the most variable characteristic in the NAS and differs for identical facilities located in different parts of the country. The tendency to impose 100% duty cycle, and zero restoration delay should be avoided to maintain the realistic nature of the Criticality result.

5. Maintenance Impact Determined. For well defined systems Criticality contributions may emanate from Maintenance related activities. A well designed maintenance concept has minimum impact in this area, but the possibilities must be examined - both to assist in the best estimate of Criticality and to provide possible means of reduction. The far reaching and sometimes subtle influence of maintenance on the system should be as thoroughly explored as time and money permit, to insure any effects are factored into the study.

6. Fault Tree Completed. This milestone marks the conclusion of the data gathering, analyzing, and processing phase. All the acquired knowledge of the system to date is incorporated into the Fault Tree. Significantly it cocurs about midway in the program. Since the results from this point on will depend entirely on the data and structure of the tree, it must be thoroughly reviewed and critiqued.

7. Evaluation of Fault Tree Complete. At this point assurance should be obtained that all events contributing to Criticality have been accounted for, and their impact identified and quantified. The data at this milestone constitutes the material from which all decisions are made.

8. Need for Criticality Reduction Established. If no reduction is required, the program may end at this point, except for documentation. All possible inputs should be examined at this time to insure that the program is not terminated prematurely.

9. Criticaltiy Reduction Methods Identified. A checklist review of all possible reduction methods should be diligently reviewed to insure that no significant method has been neglected.

10. Life Cycle Cost Analysis Completed. This is the final data producing task in the Criticality Analysis, and the results shoudl be carefully reviewed to insure a degree of standardization in costing with related programs, both Criticality Analysis, and other planning programs.

11. Optimum Solutions Identified. At this point the analysis is essentially completed. The effectiveness measures, whether Criticality, frequency, duration, lost service, etc., should be reviewed to insure they reflect what is significant to the NAS.

12. Recommendations Made, Program Completed. This is the final step in the program, and ought to take the form of a presentation of results and recommendations.

3.8.3 Program Reviews. Periodic reviews are essential for program control. They should be conducted at significant points in the program to insure the program is proceeding in the proper direction, that its outputs are being utilized, and that its completion is a recognizable event. The CAS call for a minimum of two program reviews, with proper notification provided the FAA program office. Figure 3.6 shows four possible Program Reviews scheduled for a program. Reviews 1 and 3, are the minimum required. 2 and 4 are added as time and budget permit.

Review #1 Takes place when all the essential quantitative data has been collected for the calculation of Criticality. The Critical Failure Modes have been identified, failure/repair rates predicted, hardware and functions correlated, and the functional demands established. A comprehensive review of all this data is necessary to obtain confidence in the program results. For simple, non-complex systems it only remains to compute the Criticality characteristics. For more complex systems it signals the start of the Fault Tree construction, or CBD. Thus it is a key point in the program, and warrants a substantial review.

Review #2 This review is scheduled upon completion of the Fault Tree, and its importance is obvious. However, for non-complex programs, or programs using the CBD it can be deleted.

Review #3 This review occurs when the Fault Tree or CBD has been evaluated, and the possible need for corrective Action established. Some possible solutions and costing data will also be available to aid in the review. If the need for reduction is rejected, the program may be terminated at this point. Solution methods must be carefully reviewed to insure that reasonable methods only are considered for Criticaly reduction.

Review #4 This is the final review when all the results have been obtained. It can be used to filter out extraneous material for the final report, or to require/request further effort on the part of the contractor. The program is essentially complete, requiring only the final documentation.

3.9 Criticality Requirements

3.9.1 Criticality Analysis Program Requirements. The required Criticality Analysis Program is specified in the applicable procurement documentation. The particular paragraphs of the Criticality Analysis Specification are specified as required, or one of the four standard programs from the specification is specified. The contractor is required to implement a program in accordance with these requirements. This Handbook gives guidance in the performance of each task. The particular program to impose on a contractor is determined by such considerations as state of development, inherent criticality, budgetary limitations, and FAA needs. General guidelines as to applicability are given in the following paragraphs, but it must be emphasized that each contract must be individually assessed in the light of the foregoing considerations.

3.9.1.1 Study Contracts. A study contract is not usually concerned with the delivery of a hardware end item, but is concerned with conceptual design, detail design, or possible modifications to existing systems. Budget constraints may also be a factor As a minimum the Critical States should be identified, and quantified to the extent possible, and documented. For studies related to highly critical functions it is essential that Criticality be injected early in the program so that it can impact on the design process. For studies related to modifications of existing hardware, a full quantitative program is highly desirable and quite possible. The outputs should be in a form so as to materially assist the planning function.

3.9.1.2 Equipment and Facilities Contracts. The Criticality Analysis programs required for equipment contracts will depend, to some extent, on the state of equipment development Systems in the development, prototype, or production phases will presumably have different qualities of data available to support the analysis. In general the depth of the analysis should increase with increasing levels of development. The following paragraphs provide some general guidelines.

3.9.1.2.1 Development Models. In a developmental model contract, a primary objective of the Criticality Analysis effort is to assist in the evaluation of the system concept and design approaches. This is generally the last opportunity to impact the design in its developmental stage.

3.9.1.2.2 Prototype/Preproduction Models. At this stage the system designs are essentially in final form. Criticality Analysis are normally concerned with the effects of environmental and dynamic tests on the functional integrity of the system and the validation of previously established indices.

3.9.1.2.3 Production Models and Existing Equipments. In the production model contract the primary task of Criticality Analysis is to insure that the Criticality level is not degraded by the production process, and the overall Criticality level of the NAS will not be significantly effected by the introduction of the new equipments. Existing equipments should be analyzed to quantify their contribution to the existing Criticality level in the NAS and cost effective modifications identified.

3.9.2 Criticality Analysis Requirements. Sections 1.0 to paragraph 3.3.2 of the Criticality Analysis Methodology Specification are imposed as a function of the level of system definition. In order to understand the reasoning behind the paragraph imposition, the following formatted sheets covering each significant paragraph are provided. They discuss the purpose of the specification paragraph, and its applicability to various contracts.

3.10 Analysis results

3.10.1 Analysisof Results. At the point that all the quantitative results from studies are available, recommendations are then made. Alternate solutions arising from the analyses should be carefully reviewed to insure that the selected alternative(s) meets the specific requirements of the facility under study and the general requirements of the FAA. The impact of the proposed solution on other NAS operations should be considered within the time and information constraints existing. The additional side benefits accruing may be very significant, even if only of a qualitative nature. The following paragraphs provide guidance for various conditions.

A. Qauntitative Criticality Requirement Specified. When quantitative Criticality requirements are specified in the prime equipment specification then the alternative solutions must at least meet this requirement. There may be many ways in which the requirement can be met. For example, since

$$C=\sum c_i = \sum P_i Q_i e^{-k_i/d_i}$$

one can reduce P_i, Q_i, or d_i to reduce Criticality. At thenext level, more reduction means are available.

$$C=\sum\left(\frac{\lambda_i}{\lambda_i+\mu_i}\right)\left(\frac{m_i}{m_i+n_i}\right)e^{-k/(\tau_i+m_i)}$$

λ_i = CFM FAILURERATE

μ_i = CFM REPAIR RATE

m_i = MEANDURATION OF FUNCTIONDEMAND

n_i = MEAN DURATION OF FUNCTION NODEMAND

k_i = ALLOWABLE RESTORATION DELAY

d_i = MEAN TIME INCRITICAL STATE

τ_i = MEAN TIME IN CFM

i = i^{TH} ELEMENT OR FUNCTION

Operating on any or all of these factors may provide the required decreases in Criticality. Plainly, though, the effect of some changes will be more significant to the total NAS than others. For example, if the reduction was obtained by adjusting Q, say reducing the functional demand by reducing the traffic, then this solution would be felt in other areas of the NAS that had to pick up the diverted traffic. Of course solutions by adjusting Q are generally considered beyond the scope of NAS activity.

More realistically if downtime is reduced at the expense of frequency of occurrence, the increased maintenance activity may place a severe drain on maintenance personnel, and spares supply activities.

On the other hand if the requirement is achieved by reducing the frequency of occurrence, at the expense of expected downtime, then the spectre of catastrophic failures is raised. That is, faulres which are very infrequent, but when they occur the downtime is so long their effects are catastrophic.

For this reason a Criticality requirement should be bounded with a maximum downtime constraint suitable to each particular facility.

The Critcality requirement may be totally bounded by also specifying the frequency of Critical State occurrence. This would reflect the maintenance resources available for the facility.

To assist in Analyzing the study results a series of tables should be constructed which do the following:

1. Rank all the proposed alternates by Cost-Effectiveness, that is the cost per unit of Criticality Reduction.

2. Ranked by the maximum reduction in Criticality achievable by each alternate.

3. Ranked by the reduction in frequency of occurrence of the Critical State.

4. Ranked by reduction in Critical State downtime.

Study of these rankings as they apply to the particular facility will facilitate identification of a global optimum, i.e., the alternate which benefits the overall NAS most.

3.10.2 No Criticality Specified. When no Criticality requirement has been specified, the analysis results may be reviewed in the light of possible reductions in air carrier delays. Section 3.0 provided guidance in establishing and allocating a Criticality requirement based on a delay probability greater than 1/2 hour to be less than or equal to 10^{-4}. We may also consider the possible savings in dollars due to reduced delay. Using an average savings of $20 a minute (Giant Airport Category), compute the total savings and compare this against the cost of reducing Criticality. This would proceed in the following manner.

Given a facility Criticality level of 10^{-3} and a related conditional probability of delay P (UE/C) = 10^{-1}, then the probability of a delay exceeding 1/2 hour

$$P\ (UE,C) = 10^{-4}$$

The expected hours delay per year

$$D_{ELAY} = 10^{-4} \times 8760 \simeq 1.0 \text{ hour/year}$$

If the facility, on the average, handles 100 aircraft per hour, then this translates into 100 hours of aircraft delay. The cost of this delay,

$$\text{Cost} = 100 \text{ hours} \times 60 \text{ minutes/hr} \times \$20/\text{min}$$

$$= \$120{,}000 \text{ cost of delay per year}$$

On a ten year basis, this would translate into

$$C_{10YRS} = \$1{,}200{,}000$$

This should then be compared against, for instance, the ten year life cycle cost of the proposed Criticality reduction on Life Cycle Costing.

3.10.3 Sensitivity Considerations. The probabilistic nature of Criticality Analysis, and the wide variance that may exist, dictates a consideration of the sensitivity aspects of each solution. Of concern is the adverse effect that may occur if a particular solution does not achieve the parameter improvement required. For this reason proposed solutions should be varied about their nominal values to observe any significant effects on the other Criticality parameters of the system. Solutions which show extreme sensitivity in the related paramters should be viewed skeptically, and discarded if more stable solutions are available. The sensitivity equations are defined as follows:

Sensitivity to frequency, f_i, of the Critical State to changes in the duration of the Critical State, d_i:

$$S^{f_i}_{d_i} = \frac{\frac{\Delta f_i}{f_i}}{\frac{\Delta d_i}{d_i}} = \frac{\Delta f_i}{\Delta d_i} \cdot \frac{d_i}{f_i}$$

Sensitivity of the duration of the Critical State, to changes in the frequency of the Critical State.

$$S^{d_i}_{f_i} = \frac{\Delta d_i}{\Delta f_1} \cdot \frac{f_i}{d_i} \quad , \quad S_{f_i}$$

In addition to the inter-parameter sensitivity, the overall Criticality sensitivity to parameter variation should be studied. These equations are

$$S^{C_i}_{d_i} = \frac{\Delta C_i}{\Delta d_i} \cdot \frac{d_i}{C_i} \quad , \quad S^{C_i}_{f_i} = \frac{\Delta C_i}{\Delta f_i} \cdot \frac{f_i}{C_i}$$

These equations can be very easily implemented as part of the Fault Tree evaluation computer program.

Solutions should be selected which meet the criteria of the specific site, and are relatively stable under parameter variation.

The effect of the Criticality parameters on various possible figures of merit (FOM) for FAA facilities can be used as a guide in judging relative stability. Table 3.10.1 illustrates some FOMs and the related Criticality parameter. Each Critical function is assumed to provide some essential service to the NAS. In summary each particular solution has to be examined in the light of the service being provided to the NAS, the effect of service interruption, the effect of protracted downtime, and the cost-effectiveness of the solution.

TABLE 3.10.1 CRITICALITY PARAMETERS AND FOMs

FOM	Criticality Parameter
Average number of service interruptions per year	Frequency, f
Average service restoration time	Duration, d
Average total service lost time	Criticality, C
Maximum expected number of service interruptions	Frequency, f
Maximum expected restoration time	Duration, d
Probability that service will be lost at any time for a periof of time exceeding some minimum	Criticality, C

3.11 Data Requirements

3.11.1 Data Collection. Criticality estimation depends on data collection, reduction and aanalysis. Without data, no estimates can be made. With poor data, poor estimates are made. For good estimates, good data is needed. Table 3.11.1 lists nine types of essential data. Each data type contributes to the estimation of one or more elements in the Criticality equation as shown in the matrix. Note that if some elements of Criticality are to be ignored, then less data collection is required. For example assume no delays allowable, and continuous demand, then only six classes of data are required. Eliminating C/E considerations only five classes are required. For the full-blown study all nine classes of data are necessary to generate the required estimates.

For the four standard programs the types of data normally required are indicated. This is not a hard and fast rule, and may be altered to require any mix of data for any of the programs. Of course, the important thing to recognize is that the required data must exist in some form or other prior to inception of the Criticality study. With proper coordination most of the data should be available in usable form. The usual sources for the data are shown in Table 3.11.2. Program costs can be kept to a minimum by insuring that the data sources exist, and are active during the program. The Criticality Analysis task is not expected to undertake those tasks associated with generating the data. Its task is essentially to reduce and modify existing data for use in the Criticality model. In pursuit of this objective, it should interface strongly with the data sources to insure that the form and extent of the data is adequate for its needs. Initial Criticality estimates can be made with only this data, and refined as more detailed data becomes available. The use of an iterative procedure such as this is preferable to waiting for all data inputs before any estimates are attempted. This procedure also speeds up computer program checkout and instlls confidence in the results. The modular nature of the Fault Tree is ideal for this approach.

Systematic data collection, and reduction insures traceability in the final Criticality estimates. Traceability which is concerned with the genesis of the Criticality parameters, is a necessary ingredient in any system engineering project.

TABLE 3.11.2

DATA REQUIREMENTS

Criticality Element	P_i		Q_i		e^{-k_i/d_i}		C/E		Criticality Programs			
Data	λ_i	μ_i	m_i	n_i	k_i	d_i	C	E	1	2	3	4
Failure Rates	x							x	x	x	x	x
Repair Rates		x				x		x	x	x	x	x
Allowable Delays					x			x	x	x	x	x
Maintenance Practices	x	x					x	x			x	x
Operating Practices			x	x	x		x	x				x
Demand Patterns			x	x				x	x	x	x	x
Interfaces	x	x						x			x	x
Equipment Characteristics	x	x			x	x		x		x	x	x
Cost Data							x				x	x

DATA/USE MATRIX

P_i - Probability of ith Critical Failure Mode

Q_i - Probability of ith Function Demand

k_i - Allowable delay in restoring ith Function

d_i - Expected duration of ith Function Outage

C - Cost of Criticality Reduction

E - Effectiveness in reducing Criticality

APPENDIX A

DEPARTMENT OF TRANSPORTATION

FEDERAL AVIATION ADMINISTRATION SPECIFICATION

FOR THE

DEVELOPMENT OF CRITICALITY ANALYSIS

1. SCOPE

1.1 Scope. This specification sets forth the requirements for system Criticality Analysis Methodology. Its intended purpose is to provide uniform requirements and criteria for establishing and implementing a system Criticality Analysis Program. It is applicable to existing systems in the National Airspace System and to all phases of new procurement.

1.2 Classification. Three types of contracts and three types of equipment are covered by this specification:

1.2.1 Contract Type. Contracts covered by this specification are for one of the following:

(a) Studies (with or without experimental hardware)

(b) Equipment

(c) Facilities

1.2.2 Equipment Types. The following types of equipment are covered by this specification:

(a) Development

(b) Prototype and Preproduction

(c) Production

1.3 Standard Programs. Table I lists applicable paragraphs of this specification for three Criticality Analysis programs one of which is specified in the applicable procurement documentation. The general applicability of each program is listed below.

(a) Criticality Analysis Program (1) - Design Study

(b) Criticality Analysis Program (2) - Developmental Model Equipment

(c) Criticality Analysis Program (3) - Production Model

2 APPLICABLE DOCUMENTS

2.1 Precedence of Documents. - This specification will have precedence over all specifications, standards, documents, etc., listed or referenced herein. In the event of conflict between the requirements of the equipment specification and this specification, the equipment specification shall have precedence.

2.2 Documents. The following documents, of the issue in effect on the date of invitation for bids or request for proposal, form a part of this specification to the extent specified herein.

3. REQUIREMENTS

3.1 General Requirements

3.1.1 Summary of Services to be Furnished. Services and documentation required are stipulated in the applicable procurement documentation.

3.1.2 General Guidelines.

3.1.2.1 Criticality Requirements. Quantitative Criticality performance and test requirements are specified in the FAA detail equipment specification. These requirements shall be included in appropriate sections of the contractors specification for the system.

3.1.2.2 Criticality Analysis Program Objectives. The objectives of a Criticality Analysis program are to insure that:

(a) Unacceptable modes of failure are identified, and eliminated, or reduced to an acceptable level.

(b) The safety of the National Airspace System is not degraded below established levels by the introduction of new equipments, or the continued use of existing equipments.

TABLE 1 REQUIRED CRITICALITY ANALYSIS PROGRAM

FAA SPECIFICATION	CRITICALITY ANALYSIS METHODOLOGY	CRITICALITY ANALYSIS METHODOLOGY PROGRAM		
PARAGRAPH NUMBER	PARAGRAPH HEADING	1	2	3
1.0 – 3.1	SCOPE APPLICABLE DOCUMENTS GENERAL REQUIREMENTS	*	*	
3.2.6(a) TO (e)	DATA COLLECTION	*	*	
3.2.7(a), (b)	CRITICALITY ANALYSIS DOCUMENTATION REQUIREMENTS	*	*	
1.0 TO 4	SCOPE APPLICABLE DOCUMENTS GENERAL REQUIREMENTS QUALITY ASSURANCE PROVISIONS			*

(c) Unacceptable delays are not introduced.

3.1.2.3 Criticality Analysis Program Requirements. The required Criticality Analysis Program shall be as specified in the applicable procurement specification. Specification shall be by reference to one of the specific Criticality Analysis Programs identified in paragraph 1.3 and specified in Table 1. Each of these programs stipulates the paragraph-by-paragraph applicability of this specification to a particular procurement.

3.1.2.4 Program Implementation. The contractor shall implement a Criticality Analysis Program in accordance with this specification to the extent specified to be applicable. The Criticality Analysis Program and tasks shall be performed in accordance with the applicable procedures contained in the FAA Criticality Analysis Methodology Handbook. The program shall be performed in cocsonance with the other design, development, and production functions to permit the most cost-effective achievement of program aims.

3.1.3 Definitions.

System. A composite, at any level of complexity, of operational and support equipment, personnel, facilities, and software which are used together as an entity and capable of performing and supporting an operational role.

Critical. This modifier applies to functions, facilities or equipments necessary to provide a service, the loss of which would cause derogation of safety to, and/or unacceptable delays in, expedient and efficient control of air traffic either enroute or at terminal locations.

Undesirable Event. The loss of a function, facility or equipment, which results in derogation of safety, to and, or unacceptable delays in, expedient and efficient control of air traffic either enroute or at terminal locations. Sometimes called a "Critical Event."

Criticality. A characteristic of a system, or element of a system, which quantifies its contribution to the probability of occurrence of an undesirable event, as defined above.

3.1.4 Program Activities and Sequences. The application of this specification to a specific contract requires a review of the candidate program and this specification to determine the degree of applicability of the various sections. Criticality Analysis should be initiated as soon as reasonable failure and repair rate data is available. The early identification of critical modes of failure is essential to timely and economical correction.

3.1.4.1 Study Contracts. To the extent possible, critical failure modes shall be identified, and their impact factored into the system design process. At the very least a functional failure analysis shall be performed to identify single point critical failures, and means taken to correct them.

3.1.4.2 Equipment Contracts. The Criticality Analysis Program requirements for equipment contracts will depend on the level or degree to which the equipment has been integrated into the National Airspace System (NAS).

3.1.4.2.1 Develcpment Equipment. During the development, both a functional and hardware failure analysis should be possible using reliability/maintainability prediction data. Quantitative tradeoffs shall be performed and optimum, economic solutions obtained, to assist system planning.

3.1.4.2.2 Integrated Equipment. Production equipments, or equipments already in the NAS shall be quantitatively, and systematically analyzed for their Criticality impact on the NAS. A complete economic analysis, using the techniques of Life Cycle Costing shall be performed on the resulting critical failure modes, and alternate fixes proposed to determine the most effective policy.

3.1.5 Organizational Requirements. The contractors organization shall be responsible for managing and performing a Criticality Analysis Program. The responsibilities and functions of those directly associated with system criticality and implementation shall be clearly defined. The lines of communications with interfacing organization, e.g. reliability, maintainability, systems engineering, safety and logistics shall be established and maintained, to insure proper feedback and implementation of criticality reduction techniques.

The contractor shall have one clearly identified organizational element which shall be responsible for the management and control of the Criticality Analysis Program, within the contractors facility.

3.1.6 Program Monitoring and Control. The Criticality/Analysis manager shall be responsible for planning, implementing, controlling and reporting all Criticality Analysis tasks. Reviews, audits, and milestones shall be scheduled at intervals sufficient to provide lead time for corrective action when necessary. Methods shall be implemented for assuring Criticality Analysis efforts of suppliers and subcontractors are consistent with overall Criticality Analysis requirements.

3.1.7 Program Evaluation and Validation. The Criticality Analysis Program shall be periodically evaluated to insure that it is effectively achieving its objectives.

3.2 Detailed Requirements. System Criticality Analysis Methodology is a formalized approach designed to identify and quantify critical system failures, and to provide techniques for economical elimination or reduction of the criticality level. The steps set forth below, or those selected steps specified by paragraph in Table 1 , shall be followed in performing the Criticality Analysis.

3.2.1 Preliminary Criticality Analysis (PCA). A PCA shall be conducted to determine whether a detailed criticality analysis is needed. The PCA will involve the following steps:

(a) A functional analysis to identify those functions critical to system operation.

(b) A physical and performance analysis of the system hardware and software to determine the function-hardware/software relationships.

(c) A detailed analysis of the maintenance concept and practice to assess its impact on Criticality.

(d) An analysis of the demands on the various system functions to determine the probability distribution of the demand.

(e) Construction of a top level Criticality Block Diagram (CBD) as per figures and instructions in the FAA Criticality Methodology Handbook contained herein.

(f) Evaluation of the CBD to qualify.

1. Joint probability of cuntional outage, and functional demand.

2. Expected duration of the outage.

3. Frequency of the outage.

The results of the PCA shall be evaluated against Criticality requirements as specified in the prime equipment specification to determine if further analysis and corrective action is required.

3.2.2 Detailed Criticality Analysis. If the results of the PCA indicate that the Criticality requirement is not being met, then a detailed Criticality Analysis shall be conducted. The objective of the detailed analysis is to idwntify all modes of system failure leading to the undesirable events and to determine economic fixes. The following paragraphs describe the steps in a detailed analysis.

3.2.2.1 System Model. A detailed model of the system will be constructed to aid in the Criticality Analysis. This model will be in the form of a Fault Tree (see figures and instructions in the FAA Criticality Handbook) in which all events in the casual chain leading to the undesirable event are identified and quantified. The events shall include, but not be limited to:

a. Equipment failures or malfunctions.

b. Operating personnel errors.

c. Maintenance personnel errors.

d. Maintenance actions capable of causing failures.

e. Software errors.

f. Support system errors.

g. Natural and manmade environmental effects.

3.2.2.2 Evaluation of Fault Tree. The fault tree shall be evaluated using methods detailed in the FAA Criticality Handbook. The outputs of the evaluation shall be:

a. The weighted joint probability of system functional failure mode and functional demand (Criticality).

b. Expected duration of the failure mode outage.

c. Frequency of the outage.

d. A ranking of the modes of failure by Criticality, by frequency, and by duration of outage.

3.2.3 Requirements for Corrective Action. Each failure path shall be analyzed for possible corrective actions to reduce the Criticality. The sensitivity of the Criticality to the corrective action shall be determined.

3.2.4 Integration and Life Cycle Costing of Fixes. Fixes for the various failure paths shall be studied to determine if integrated solutions are possible. Alternate solutions shall be costed out in a Life Cycle (10 years) manner, and the cost-effectiveness of each solution determined.

3.2.5 Analysis of Results. The overall results shall be analyzed to determine those solutions which provide the improvement required, and the cost-effectiveness of each one. Selected solutions shall be recommended for implementation.

3.2.6 Data Collection. In support of the criticality analysis the following data will be collected and reduced:

(a) Equipment failure rates.

(b) Equipment repari rates.

(c) Functional weighting data.

(d) Preventive maintenance practices.

(e) Operating regulations.

(f) Traffic patterns.

(g) Functional interfaces.

(h) Equipment physical/performance characteristics.

(i) Cost data on criticality reduction methods.

3.2.7 Criticality Analysis Documentation Requirements. The PCA and Detailed Criticality Analysis documentation shall include, but not be limited to the following:

(a) Criticality Block Diagrams

(b) PCA Summary Sheet

(c) Detailed Criticality Analysis logic diagrams (fault trees)

(d) Failure mode summary sheets.

(e) Criticality analysis sheets.

(f) Cost/Effective Reduction Summary Sheets.

These forms and instructions for their cimpletion are contained in the FAA Criticality Handbook.

4 QUALITY ASSURANCE PROVISIONS

When appropriate, tests may be specified to insure compliance with this specification. If the equipment is in existence, non-damaging faults should be induced to verify that the proposed methods of reduction are effective. When equipment is not available, standardized computer programs shall be used to simulate the system, and deterine effectiveness of fixes.