AD 299561

BOEING

MICROFILMED 5-1

AD-299561

THE BOEING COMPANY

CODE IDENT NO. 81205

NUMBER D2-30207-1

TITLE WS-133B Fault Tree Analysis Program Plan (U)

MODEL NO. WS-133B CONTRACT NO. AF04(694)-266

ISSUE NO. ________ ISSUED TO ________________

SPECIAL LIMITATIONS ON ASTIA DISTRIBUTION

ASTIA may distribute this report to requesting agencies subject to their security agreement, approved fields of interest, and the following:

☒ UNLIMITED—To all agencies of the Department of Defense and their contractors.

□ LIMITED—To U. S. Military organizations only.

This report may be distributed to nonmilitary agencies not approved above subject to Boeing approval of each request.

NOTE: the LIMITED category may be checked only because of actual or potential patent, proprietary, ethical, or similar implications.

PREPARED BY	C. R. Eckberg	3/8/63
SUPERVISED BY	N. R. Payne	3/11/63
APPROVED BY	N. B. Classon / H. K. Hebeler	3/11/3
APPROVED BY	O. C. Boileau	3/16/3
CLASS & DISTR APPROVED BY		3/11/3
		(DATE)

94

REV SYM B

VOL. NO. 1 OF 3

SECT. 1 PAGE 1 of 17

AD 299561

BOEING

NUMBER D2-30207-1

TITLE WS-133B Fault Tree Analysis Program Plan (U)

MODEL NO. WS-133B CONTRACT NO. AF04(694)-266

ACTIVE PAGE RECORD

SECTION	ORIG REL PAGE NO.	REV SYM	ADDED PAGES					
			PAGE NO.	REV SYM	PAGE NO.	REV SYM	PAGE NO.	REV SYM
1	1	B			28	B		
	2	B			29	B		
	3	B			30	B		
	4	B	4.1	B	31	B		
	5	B	5.1 6.1	B B	32	B		
	6	B	6.2	B	33	B		
	7	B	7.1 8.1	B B	34	B		
	8	B	18.1	B	35	B		
	9	B	19	B	36	B		
	10	B	20	B	37	B		
	11	B	21	B	38	B		
	12	B	22	B	39	B		
	13	B	23	B	40	B		
	14	B	24	B	41	B		
	15	B	25	B	42	B		
	16	B	26	B	43	B		
	17	B	27	B	44	B		
2	1	B						
	2	B						
	~~3~~	B						
	~~4~~	A						
	~~5~~	A						
3	1	B						
	2	A						
	3	B						
4	1	B						
	2	B						
	3	B						
	4	B						
	5	B						
	6	B						
	7	B						
	8	B						
	9	B						
	10	B						
	11	B						
	12	B						
	13	B						
	14	B						
	15	B						
	16	B						
	17	B						
	18	B						
	19	B						
	20	B						

SECTION	ORIG REL PAGE NO.	REV SYM	ADDED PAGES					
			PAGE NO.	REV SYM	PAGE NO.	REV SYM	PAGE NO.	REV SYM
5	1	B						
	2	B						
	3	B						
	4	B						
	5	B						
	6	B						
	7	B						
	8	B						
	9	B						
	10	B						
	11	B						
	12	B						
	13	B						
	14	B						
	15	B						
	16	B						
	17	B						
	18	B						
~~[illegible]~~	~~1~~	B						
	~~2~~	B						

REV SYM B

REVISIONS

SYM	DESCRIPTION	DATE	APPROVED
A	**SECTION A** Page 6 - Revised to clarify Fault Tree documentation. Page 7 - Revised to identify IA&T as Integrating Contractor. Page 7.1 - Added to provide for Technical Interchange Meetings Page 8 - Revised to identify the Fault Trees. **SECTION B** Page 2 and 3 - Revised to correct scheduling to reflect associate contractors commitments A/N Letter 63AN/MM 3820 dated 11 June 1963, Subject: Fault Tree Analysis Program, and Sylvania Letter MPOL-2-4-860 dated 14 June 1963, Subject: Fault Tree Coordination. Pages 4 and 5 deleted. **SECTION C** Pages 2 - Revised to clarify definitions	7/16	7/2/3 7/2/3
B	SECTION 1 Pages 5 through 6.2 revised to redefine composition of the -2 and -3 volumes. All pages are revised to reflect change in section identification. Pages 18 through 44, Section 1, added to provide additional mathematical methods. Section F "References" is deleted. The references are included in introductory pages of Section 1.	11 May 64	DAR 5/11/64

TABLE OF CONTENTS

D2-30207-1

D2-30207-2

D2-30207-3

REFERENCES

1 Launch Control Safety Study; Vol. I and II; Bell Telephone Laboratories - September 15, 1962

2 D2-14134 Minuteman Electronic Part Failure Rates - WS-133-2

3 D2-10744 Minuteman Reliability Engineering Directives #5, 6, 7 and 8

4 BAC Standards - D590 - Book No. 30 Section 500

5 Air Force Report
A65-E-62-123 WS-133B Weapon System Design Criteria R

1 INTRODUCTION

1.1 Letter Contract AF04(694)-266 requires that a Fault Tree Analyses be prepared to determine the probabilities of Inadvertent and Faulty Launches in the WS-133B Weapon System. This type of analysis provides a graphic display of fault sequences which can cause an unwanted event and a measure of the system safety.

1.2 The determination of the ability of a complex system to provide safety against an undesirable event is exceedingly involved. An orderly analysis has been prepared by the Bell Telephone Laboratories, entitled Launch Control Safety Study Report, dated September 15, 1962 (ref. 1). They introduced a concept of Fault Trees which, with equivalent Boolean equations, provides a technique particularly adaptable to this effort. The trees graphically illustrate, in a logical form, the faults which might occur to permit an undesirable event. Boolean equations, which express the fault relationships, offer mathematical simplifications for calculating the Safety Constant.

2 PURPOSE

2.1 The purpose of the Fault Tree Analysis Program is to:

(a) Determine the probabilities of inadvertent and faulty launches.

(b) Identify those failures which make excessive contribution to (a).

(c) Recommend corrective measures.

3 ORGANIZATION AND SCOPE

3.1. The WS-133B Fault Tree analysis program is organized into three categories, each in a volume of this document as follows: R

D2-30207-1	Program Plan
D2-30207-2	Inadvertent and Faulty Launch Summary
D2-30207-3	Associate Contractor's Detail Analyses

3.1.1 The scope of the analysis is divided into 5 divisions. R

R

3.1.1.1 The Alert System

This is the analysis of the probability of I.L. during the system life. It includes the operational system during the Strategic Alert, Strategic Standby, Launch Commanded, and Launch in Process modes, the exercise of preparatory launch commands, and also includes the probabilities of those events which can be caused by commanded programmed tests or calibration of the system, and by maintenance equipment and procedures.

3.1.1.2 The System Under Commanded Tests, Calibration and Interrogations:

This is the detail analysis of the probabilities contributing to I.L. during the periods of commanded tests and calibration. It also includes the interactions of commanded tests and interrogation of a specific LF upon the overall system. It excludes the effects of MGE connected to the system, paragraph 3.1.2.4.

3.1.1.3 Assembly and Checkout Equipment

This is the analysis of the A&CO equipment to determine what unsafe residual or post test effects can be left in the system by failures of the test equipment.

3.1.1.4 Maintenance Ground Equipment

This is the analysis of maintenance equipment effects at the LCF, LF and OCCP.

1. Analyze the maintenance conditions which contribute to those events indicated in the analysis of the alert system paragraph 3.1.2.1.

2. Determine what unsafe residual or post maintenance effects can be left in the system by failure of the maintenance equipment.

3. Determine maintenance equipment failure rates for the modes of failure which are needed for (1) and (2) above.

3.1.1.5 Faulty Launch Analysis - The Alert System

It includes equipment malfunctions and improper flight instructions under operational and maintenance conditions.

3.2 D2-30207-1 WS-133B Fault Tree Analysis Program Plan

This volume defines the Fault Tree Analysis Program requirements and responsibilities of all contractors and establishes ground rules, formats, definitions and instructions for preparing fault tree analyses.

R

3.3 D2-30207-2 WS-133B FAULT TREE ANALYSIS - INADVERTENT AND FAULTY LAUNCH SUMMARY

This volume contains the Weapon System Summary Fault Trees and Analyses prepared by the Analysis Integration Contractor. The contents of this volume are shown below:

SECTION 1. GENERAL

- Title Page
- Active Page Record Page
- Revision Page
- Table of Contents
- References
- Introduction
- Summary

SECTION 2. INADVERTENT LAUNCH ANALYSES

1.0 The Alert System

- 1.1 Functional Flow and Block Diagrams
- 1.2 Fault Tree
- 1.3 Mathematical Solution
- 1.4. Recommendations for Change

2.0 The System Under Tests, Calibration and Interrogations

- 2.1 Functional Flow and Block Diagrams
- 2.2 Fault Tree
- 2.3 Mathematical Solution
- 2.4 Recommendations for Change

3.0 Assembly and Checkout Equipment

- 3.1 Functional Flow and Block Diagrams
- 3.2 Fault Tree
- 3.3 Mathematical Solution
- 3.4 Recommendations for Change

4.0 Maintenance Ground Equipment

- 4.1 Functional Flow and Block Diagrams
- 4.2 Fault Tree
- 4.3 Mathematical Solution
- 4.4 Recommendations for Change

SECTION 3. FAULTY LAUNCH ANALYSIS

1.0 The Alert System

- 1.1 Functional Flow and Block Diagrams
- 1.2 Fault Tree
- 1.3 Mathematical Solution
- 1.4 Recommendations for change

3.4 D2-30207-3 WS-133B FAULT TREE ANALYSIS - ASSOCIATE CONTRACTOR'S DETAIL ANALYSES

This volume contains the detailed Fault Tree Analyses of each Associate Contractor as received by the Integration Assembly and Test Contractor in support of preparation of the System Fault Trees contained in volume 2 of this document. The contents of this volume are organized as follows:

SECTION 1. GENERAL

Title Page
Active Page Record Page
Revision Page
Table of Contents
References
Introduction
Summary

SECTION X* ASSOCIATE CONTRACTOR*

1.0 Inadvertent Launch Analyses

1.1 The Alert System

1.1.1 Functional Flow and Block Diagrams
1.1.2 Fault Trees
1.1.3 Mathematical Calculations

1.2 The System Under Tests, Calibration and Interrogation

1.2.1 Functional Flow and Block Diagrams
1.2.2 Fault Trees
1.2.3 Mathematical Calculations

1.3 Assembly and Checkout Equipment

1.3.1 Functional Flow and Block Diagrams
1.3.2 Fault Trees
1.3.3 Mathematical Calculations

1.4 Maintenance Ground Equipment

1.4.1 Functional Flow and Block Diagrams
1.4.2 Fault Trees
1.4.3 Mathematical Calculations

2.0 Faulty Launch Analysis

2.1 The Alert System

2.1.1 Functional Flow and Block Diagrams
2.1.2 Fault Trees
2.1.3 Mathematical Calculations

R

3.0 Recommendations for Change

4.0 Supporting Data

4.1 Failure Mode Analysis
4.2 Reliability Data

*Associate Contractor section numbers have been assigned as follows:

SECTION 2. AEROJET GENERAL

SECTION 3. AUTONETICS

SECTION 4. AVCO

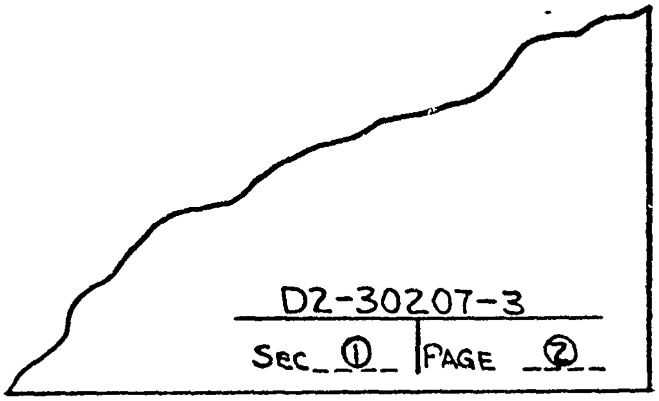
SECTION 5. BOEING

SECTION 6. HERCULES

SECTION 7. SYLVANIA

SECTION 8. THIOKOL

All Associate Contractors shall submit their inputs on their own stationary (8½" x 11" to 11" x 34½"). Document, section and page numbers shall be included in the lower right-hand corner of each page in accordance with the following sample:



1 Each Associate Contractor shall use the section number assigned as shown in the organization of contents above.

2 Page numbering shall start with Page No. 2. The Analysis Integration Contractor shall add the Section Title Page to facilitate handling and incorporation of individual sections into D2-30207-3.

R

4 CONTRACTORS' RESPONSIBILITIES

The responsibilities of the contractors are described as follows:

4.1 The Integrating Contractor

4.1.1 It is the prime responsibility of the Integrating Contractor to prepare and submit the final Weapon System Fault Tree Analysis to AFBSD.

4.1.2 Based on the Weapon System Fault Tree Analyses, the Integrating Contractor shall provide guidance to other contractors and generate requirements for specific inputs from them.

4.1.3 The Integrating Contractor shall evaluate all detail Fault Tree inputs from other Contractors for compatibility and coordinate interface problems in the analyses.

4.1.4 The Integrating Contractor shall develop and maintain detailed schedules for preparation and submittal of Weapon System Fault Tree Analyses.

4.1.5 The Integrating Contractor shall also fulfill the requirements of paragraph 4.2 below.

4.1.6 The Integrating Contractor shall honor the proprietary rights of the Associate Contractors' submitted proprietary data and shall delete this material from the published submittals and reports.

R
I
R

4.2 All Associate Contractors

4.2.1 It is the prime responsibility of each contractor to prepare detailed Fault Tree Analyses of the equipments he provides.

4.2.2 All contractors shall submit their detail Fault Tree Analyses, together with other substantiating data (failure mode probability, worst case analyses, etc.), to the Integrating Contractor for incorporation into the Weapon System Fault Tree Analyses as outlined in Section 1 Subsection 3.3 and scheduled in Section 2.

4.2.3 Each Contractor may initiate recommendations for changes, shall coordinate them with other Contractors and prepare submittals to AFBSD for decision.

4.2.4 All contractors shall coordinate their Fault Tree Analysis Schedules with the Integrating Contractor for compatibility with the master Weapon System Fault Tree Schedules of. Section 2.

4.2.5 All contractors shall submit their inputs to Integrating Contractor, in accordance with approved schedules, for incorporation into quarterly submittals of the Weapon System Fault Tree Analysis documentation.

4.2.6 Material of proprietary nature submitted to the Integrating Contractor shall be so indicated. This data must be submitted as a separate attachment of the submittal to permit its extraction without rework of the remaining material. R

4.3 Technical Interchange (TI) Meetings

4.3.1 TI Meeting will be held on a monthly basis, the third Tuesday of the month, except as indicated in paragraph 4.3.2. Additional meetings may be scheduled on an individual basis at the request of any Associate.

4.3.2 The TI Meetings, to be held during the months quarterly submittals are made to BSD/STL, are to be scheduled on the day preceding the quarterly submittal meeting date.

4.3.3 Announcement of the TI Meeting time and place is the responsibility of the Integrating Contractor with the concurrence of the other Associate Contractors and shall be such that travel is apportioned on an equitable basis.

4.3.4 An action item log will be maintained by the Integrating Contractor, as an instrument of coordination, to assure the timely flow of data among the Associated.

4.3.5 Each action item will be prepared by the representative responsible for the provisions of the data and will include a date for the completion of the action item.

4.3.6 Each Associate will be represented by personnel who are knowledgeable in the fault tree effort and who are prepared to commit a date for the completion of an action item. R

5. GROUND RULES

These ground rules are supplementary to Contractor's Responsibilities and define a common approach for the development of Fault Trees.

5.1 The Safety Constant objectives for the fault trees will be tabulated and the values specified in the appropriate volumes as shown typically below.

5.1 Continued R

Fault Tree	Safety Constant Objective	Unit Time	Results
I.L. - Alert System, including effects of:	$1X10^{-x}$	System Life of Squadron	-
System Under Test, Calibration and Interrogation -			
Maintenance Equipment -			
Faulty Launch	$1X10^{-x}$	Per Launch	-

5.2 Terms and symbols defined in Section 3 will apply throughout these analyses.

5.3 Fault Tree Analysis will be conducted similar to the outline in Paragraph 6 and Section 4 and 5. R

5.4 The transmission constant of the cable system will be applied as furnished by the GFS Contractor. These will include noise and crosstalk values in the 100 to 5000 cycles band for normal and abnormal conditions caused by cable system failures.

5.5 Failures will be assumed to occur in a random manner.

5.6 Those functions which are required to operatenormally to transmit a fault will be assumed to be operating properly. The probability of their failure, which in these instances could block another failure function, is disregarded.

5.7 Failure-Rates and Mean-Time-Between-Failures shall be based upon Document D2-14134 (reference 2) and Boeing Standards (reference 4) or other Contractors' equivalent.

5.8 The time during which a failure contributes to inadvertent launch is evaluated as follows,

5.8.1 Failures which are detected and repaired by the normal system maintenance shall be considered to be effective for forty-eight (48) hours.

5.8.2 Failures which upon detection cause a subsystem shutdown shall be considered to be effective until shutdown.

5.8.3 Failures which are detectable by the system periodic testing shall be considered to be effective for the period between these tests plus either the period to shut down or 48 hours, whichever applies.

5.8.4 Failures which are not subject to monitored system detection shall be considered to be effective for ½ the maintenance period specified in the Forms C and C1, 5.9 For the critical circuits which contribute to the evaluation of the Safety Constants, The Boeing Company shall prepare circuit analyses per Document D2-10744 - Minuteman Reliability Directives 5, 6, 7, and 8 (Ref 3). Other Contractors' shall prepare their analyses per these or equivalent procedures.

5.10 Functional flow and fault tree drawings shall be reduced to 11" high by a maximum of 34½" long (page edges; 6½" folds) for inclusion in documents.

5.11 The base line for starting this analysis is the system as designed, properly connected and properly operated.

5.12 The fault tree development shall be pursued to that level where the probability of failure can be readily substantiated at the lowest significant level of interface with other branches (equipment).

6 FAULT TREE CONSTRUCTION

6.1 The purpose of a Fault Tree Analysis is to identify events leading to a hazardous condition and organize these events in a logical form which lends itself to a clear determination of sequence and order of events leading to a hazard and to simple mathematical analysis.

6.2 The basic principles for setting up and preparing Fault Tree Analyses are given in Section VII of the BTL Report: Minuteman Launch Control System Safety Study Report, Vol. I, included as Sect. 4 of this document. R

6.3 A Fault Tree Analysis shall be divided into three distinct parts,

1. Functional Flow Diagram,
2. Fault Tree,
3. Mathematical Analysis,

which are finally summed up in the Safety Constant. This safety constant is a numerical evaluation of Safety for a given Fault Tree Analysis.

6.4 The following sequence of steps may be used as a guideline in accomplishing Fault Tree Analyses:

1. Determine methods of operation
2. Prepare functional flow diagrams
3. Develop appropriate Fault Trees
4. Determine circuit and equipment reliability
5. Perform other mathematical analyses as necessary and calculate Safety Constant.
6. Analyze and investigate phenomena that would affect the sensitive elements and show effect on Safety Constant.

15

6.3 EXAMPLE OF FAULT TREE

6.3.1 Inadvertent launch, defined for this example as at least silo cover removal and first stage ignition, can be considered to be caused by three separate branches of a fault tree as shown in Figure 1. Improper initiation of the proper terminal launch sequence (1) can be caused by faults at almost any point in the command flow; the terminal sequence, once initiated, is irreversible and will certainly result in inadvertent launch (sequence cancelling faults being ground ruled out). Inadvertent launch can also result from random critical failures (3); that is, launch events occur not as ordered by an improperly initiated sequence, but as caused by random failures (the command flow upstream from the DCU is not involved in this branch). Finally, improper entry into the terminal launch sequence at other than its initial point could cause an inadvertent launch if random failures have effectively completed the necessary steps in skipped portion of the sequence (2) - i.e., inadvertent launch due to interaction of (1) and (2).

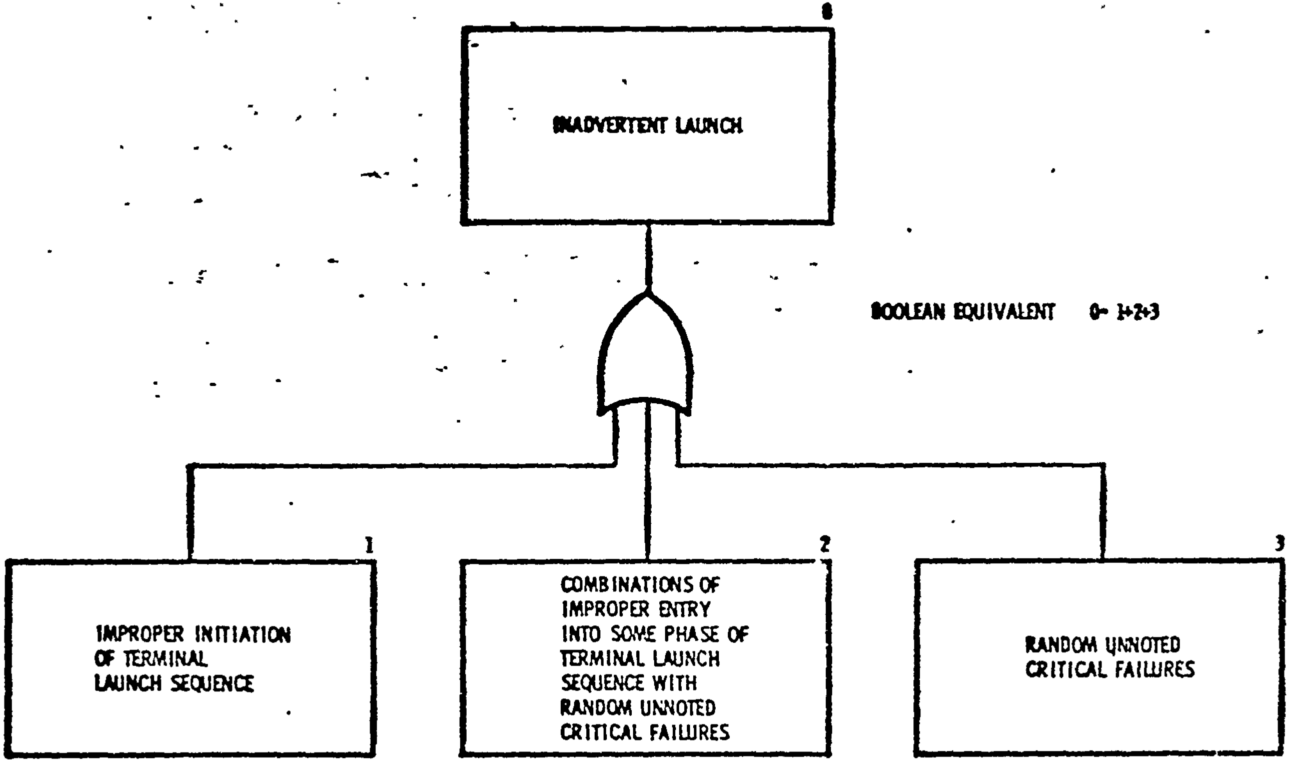
6.3.2 A breakdown of the (1) branch of the sample fault tree is shown in Figure 2. Since the DCU controls (or is involved in) all events that must precede terminal sequence initiation as well as controlling the terminal sequence itself, it is advantageous to separate (by branches) faults upstream from the DCU (11) from DCU faults (13), either of which can cause an inadvertent launch. The third (12) branch is needed to account for interaction between the (11) and (13) branches.

6.3.3 The branching philosophy shown in Figures 1 and 2 is obviously not the only philosophy that could be used; however, it appears useful from a bookkeeping point of view in that it permits complete, independent investigation of portions of the total prior to tangling with the maze of total interactions.

6.3.4 A breakdown of the (115) branch is shown in Figure 3. This subbranch is based on the sample functional flow shown in Figure 4. Note that DCU faults do not appear in Figure 3 since the (115) branch deals only with non-DCU faults. Again, the system is apportioned by branch, with a "combination" branch to handle interactions. At this point in the fault tree it is possible to associate faults with specific equipments. Status system or remedial action failure, shown generally in Figure 3, is brought in at this point of the tree since it is at this level that specific fault status items will usually be defined.

6.3.5 The Boolean equation describing each tree branch is shown on the figures depicting each sample branch.

MAIN BRANCHES OF INADVERTENT LAUNCH FAULT TREE


0
INADVERTENT LAUNCH
BOOLEAN EQUIVALENT 0- 1+2+3
1
IMPROPER INITIATION OF TERMINAL LAUNCH SEQUENCE
2
COMBINATIONS OF IMPROPER ENTRY INTO SOME PHASE OF TERMINAL LAUNCH SEQUENCE WITH RANDOM UNNOTED CRITICAL FAILURES
3
RANDOM UNNOTED CRITICAL FAILURES

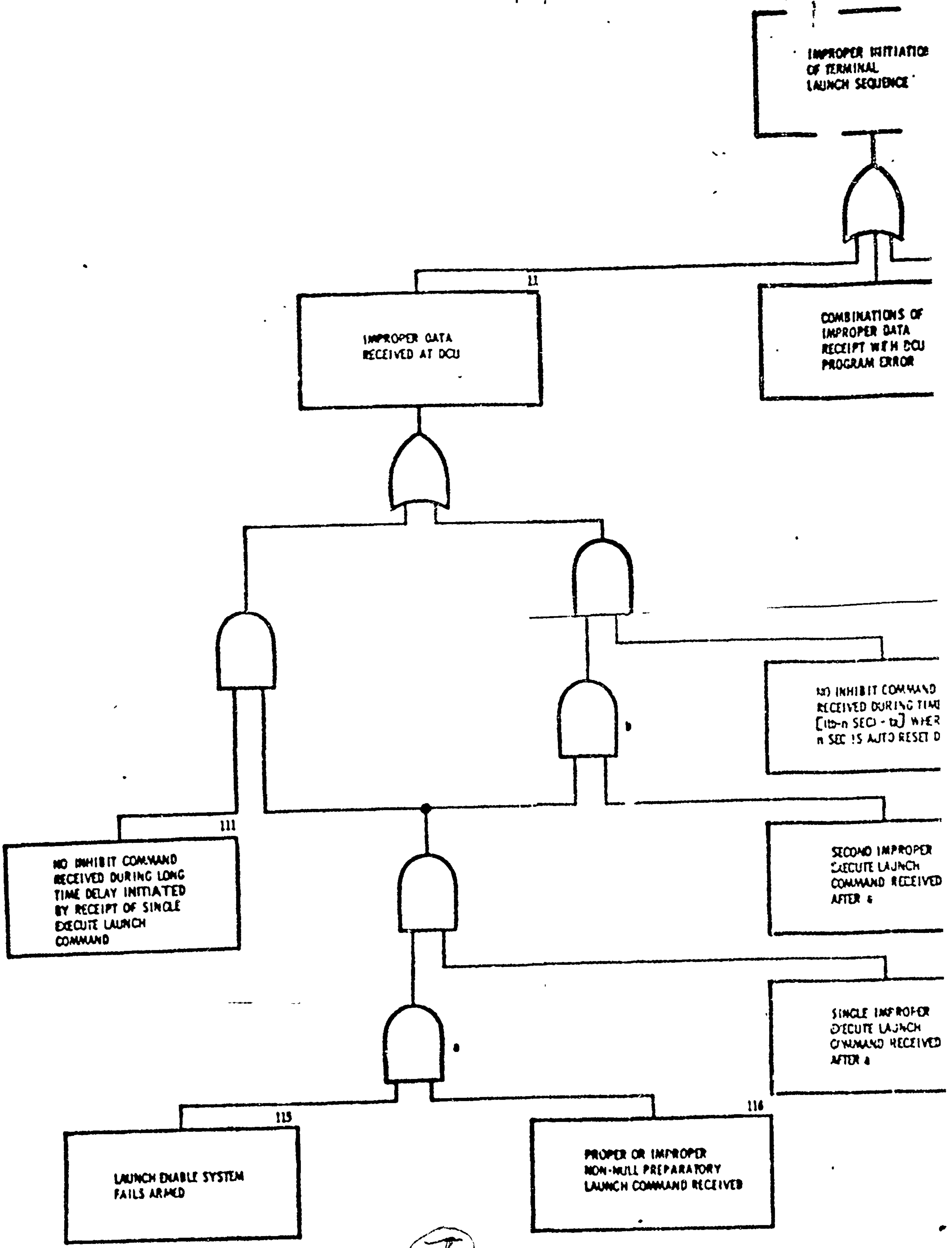
NOTE:

EACH FAILURE EVENT EITHER MUST BE UNNOTED BY FLCF'S OR INADVERTENT LAUNCH MUST OCCUR BEFORE CORRECTIVE (PREVENTIVE) ACTION CAN BE TAKEN OR CORRECTIVE ACTION MUST FAIL

-17

REV B

FIGURE 1


IMPROPER INITIATIO
OF TERMINAL
LAUNCH SEQUENCE
11
IMPROPER DATA
RECEIVED AT DCU
COMBINATIONS OF
IMPROPER DATA
RECEIPT WITH DCU
PROGRAM ERROR
NO INHIBIT COMMAND
RECEIVED DURING TIME
[tb-n SEC) - t2] WHER
n SEC IS AUTO RESET D
b
111
NO INHIBIT COMMAND
RECEIVED DURING LONG
TIME DELAY INITIATED
BY RECEIPT OF SINGLE
EXECUTE LAUNCH
COMMAND
SECOND IMPROPER
EXECUTE LAUNCH
COMMAND RECEIVED
AFTER b
SINGLE IMPROPER
EXECUTE LAUNCH
COMMAND RECEIVED
AFTER a
a
115
LAUNCH ENABLE SYSTEM
FAILS ARMED
116
PROPER OR IMPROPER
NON-NULL PREPARATORY
LAUNCH COMMAND RECEIVED

I

PAGE-18

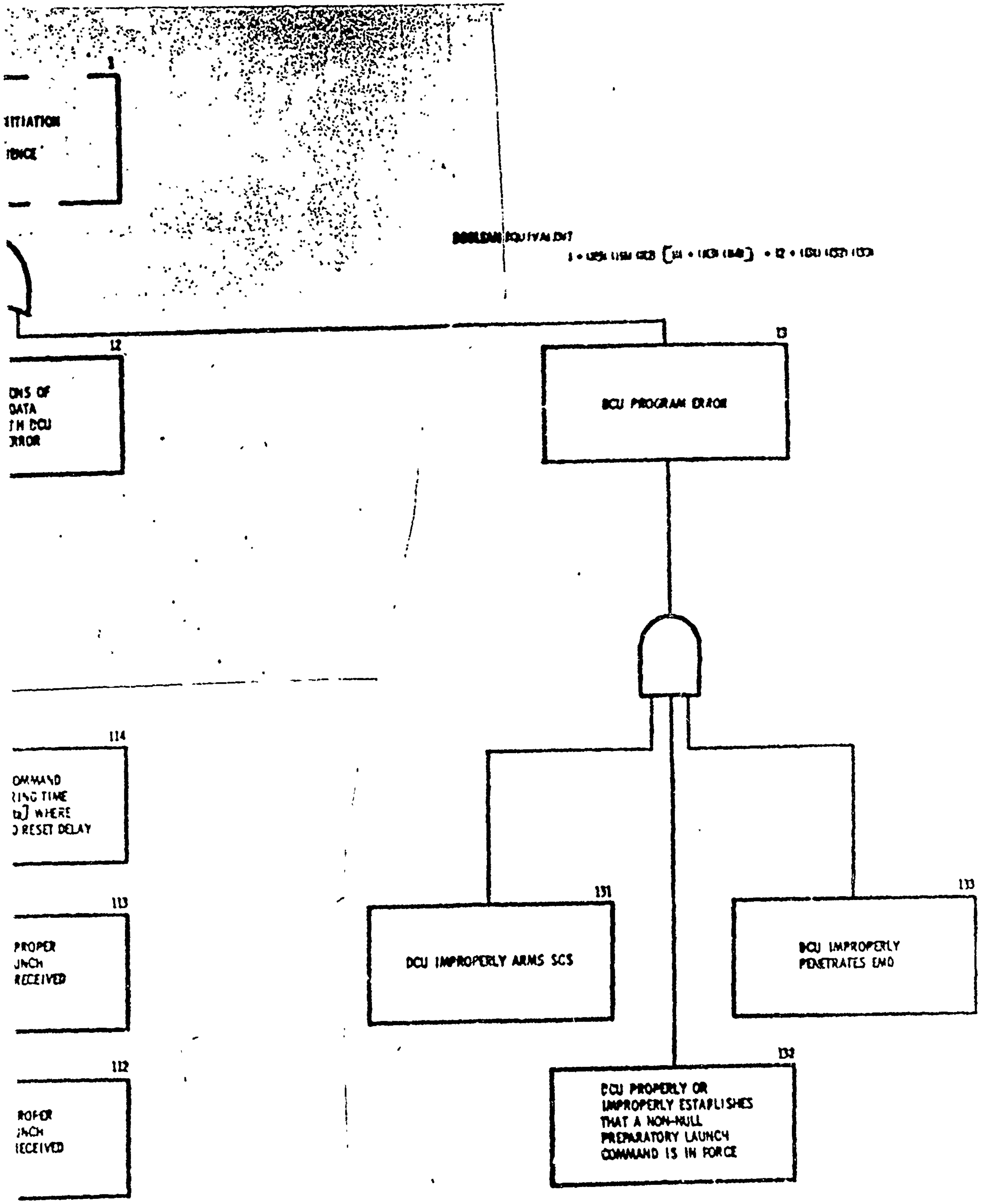
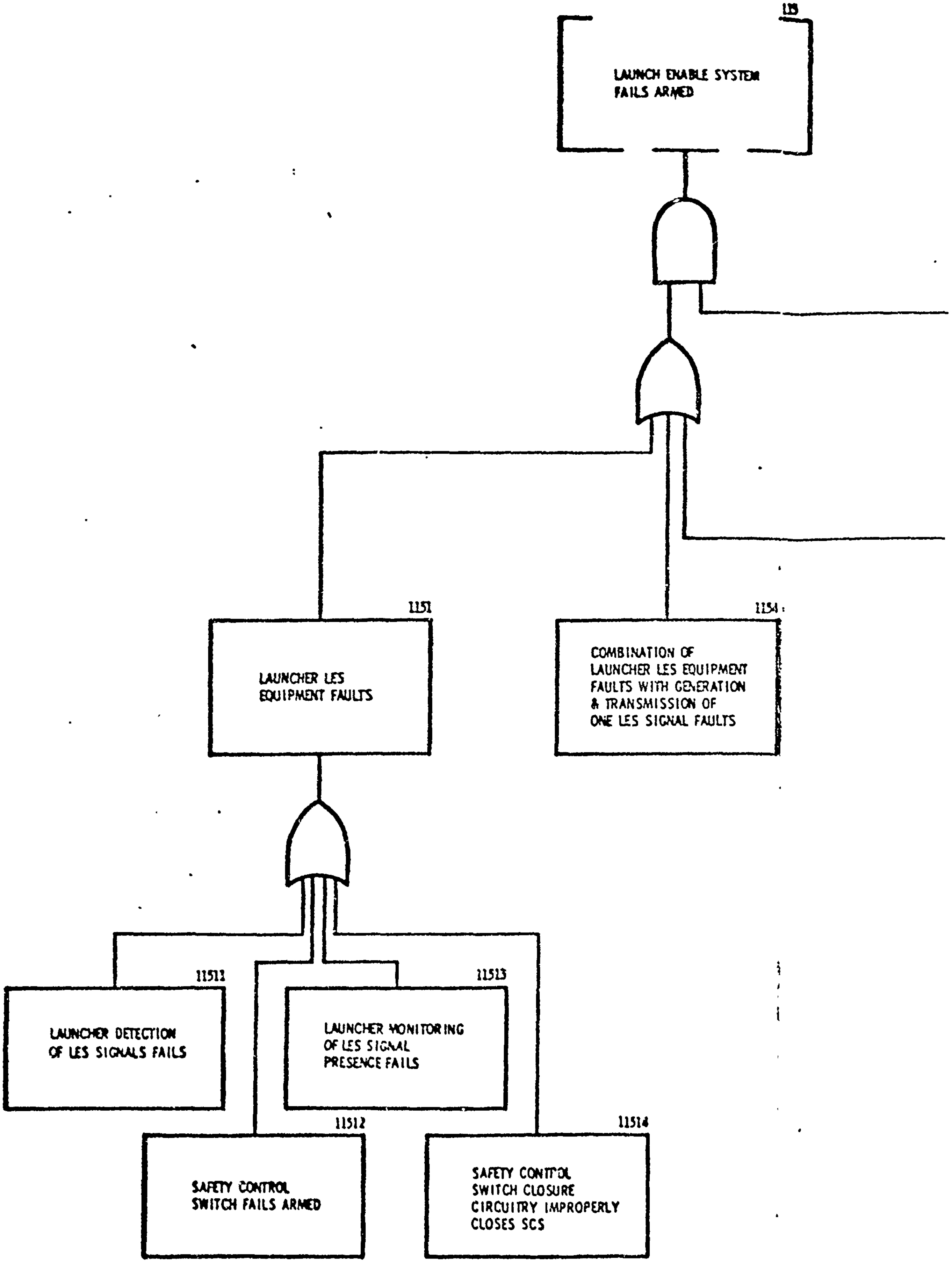


FIGURE 2

Page-18 ② Rev B PG


115
LAUNCH ENABLE SYSTEM FAILS ARMED
1151
LAUNCHER LES EQUIPMENT FAULTS
1154
COMBINATION OF LAUNCHER LES EQUIPMENT FAULTS WITH GENERATION & TRANSMISSION OF ONE LES SIGNAL FAULTS
11511
LAUNCHER DETECTION OF LES SIGNALS FAILS
11513
LAUNCHER MONITORING OF LES SIGNAL PRESENCE FAILS
11512
SAFETY CONTROL SWITCH FAILS ARMED
11514
SAFETY CONTROL SWITCH CLOSURE CIRCUITRY IMPROPERLY CLOSES SCS

BOOLEAN EQUIVALENT

$$115 = [1151 + 1152 + 1153 + 11514 + 11521 + 11522 + 11523 + 1154] (1155)$$

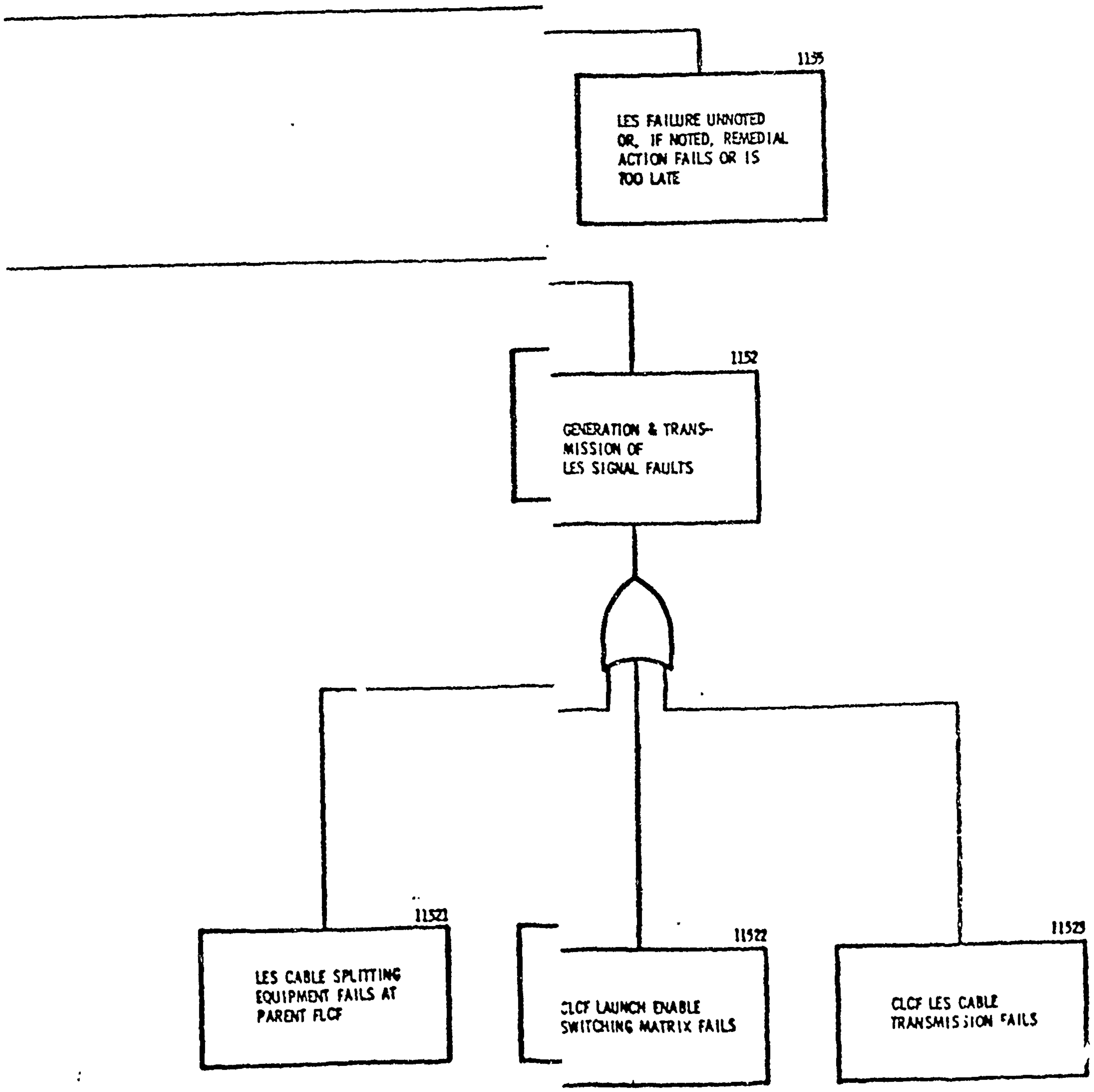

1155
LES FAILURE UNNOTED OR, IF NOTED, REMEDIAL ACTION FAILS OR IS TOO LATE
1152
GENERATION & TRANSMISSION OF LES SIGNAL FAULTS
11521
LES CABLE SPLITTING EQUIPMENT FAILS AT PARENT FLCF
11522
CLCF LAUNCH ENABLE SWITCHING MATRIX FAILS
11523
CLCF LES CABLE TRANSMISSION FAILS

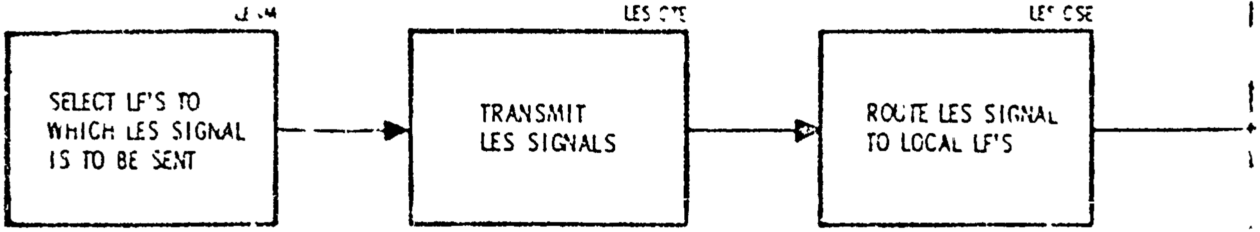
FIGURE 3

PG 19

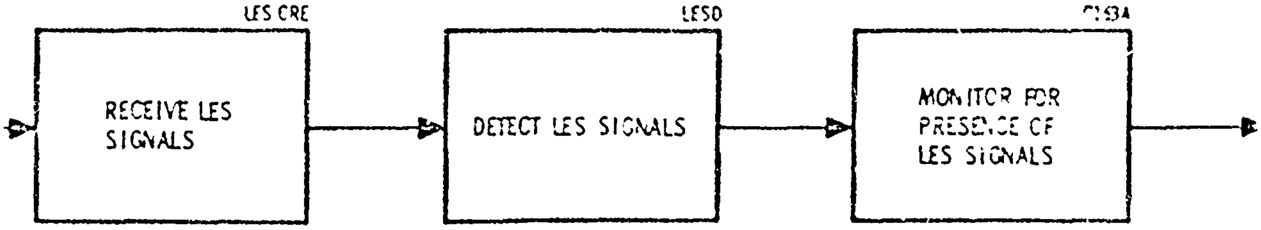
2

Page-19R

FLCF

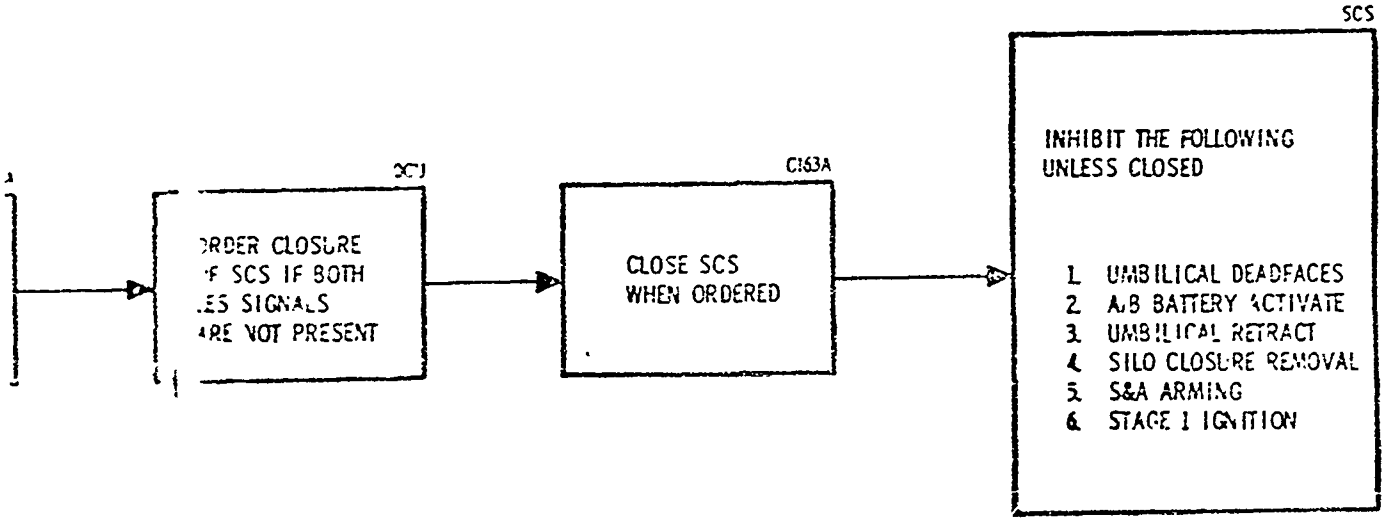

LES CTE
LES CSE
SELECT LF'S TO WHICH LES SIGNAL IS TO BE SENT
TRANSMIT LES SIGNALS
ROUTE LES SIGNAL TO LOCAL LF'S

LF



LESM-	LAUNCH ENABLE SWITCHING MATRIX
LES-	LAUNCH ENABLE SYSTEM
CTE-	CABLE TRANSMITTING EQUIPMENT
CSE-	CABLE SPLITTING EQUIPMENT
CRE-	CABLE RECEIVING EQUIPMENT
LESD-	LAUNCH ENABLE SIGNAL DETECTOR
C163A-	SIGNAL CONVERTER
DCU-	DIGITAL COMPUTER UNIT
SCS-	SAFETY CONTROL SWITCH

UF



OCU
ORDER CLOSURE
OF SCS IF BOTH
LES SIGNALS
ARE NOT PRESENT
C153A
CLOSE SCS
WHEN ORDERED
SCS
INHIBIT THE FOLLOWING
UNLESS CLOSED
1. UMBILICAL DEADFACES
2. A/B BATTERY ACTIVATE
3. UMBILICAL RETRACT
4. SILO CLOSURE REMOVAL
5. S&A ARMING
6. STAGE 1 IGNITION

③

FIGURE 4

7. APPLICABLE MATHEMATICS

R

Fault Tree analysis requires careful mathematical treatment. Logic gates for combining faults, Boolean simplification to properly compute the effects of interacting branches, and the calculation of probability of failure in a periodically tested system have been developed by the Bell Telephone Laboratories. In addition to the preceding, the development of failure rate expression in the constantly monitored system with allowance for repair periods has been added by Boeing.

Also included in this section are some approximations which are useful to reduce undue complications in the Boolean simplification; qualification applying to failure rate data; the method for performing the final squadron calculations; and some notes on the application of probability to the non-repairable system or short time system modes.

R

7 APPLICABLE MATHEMATICS - Contd.

7.1 General

The quantitative conclusion of a fault tree analysis is numerically expressed as the safety constant. The calculations necessary to obtain it require:

(a) The development of the Boolean equations (Paragraph 7.2) R

(b) Reliability and failure rate data (Paragraph 7.3)

(c) Determination of failure rates and effective duration times at logic gate outputs. (Paragraph 7.4)

(d) Effect of interacting branches (Paragraph 7.5)

(e) Nonrepairable and short-time system mode analysis (Paragraph 7.6)

(f) Squadron and final calculations (Paragraph 7.7) R

7.2 Boolean Equations

Section VII of Vol. 1 and Section II of Vol. 2 of the Bell Telephone Laboratory inadvertent launch study describe the generation and simplification of Boolean equations applicable to the fault trees. These sections are included as part of this document in Sections 6 and 7.

7.3 Failure Rates R

In determining failure rates for parts and circuits, certain assumptions have been defined. They are as follows:

7.3.1 Assumption 1

For electronic parts, assume a constant three (3) year failure rate to apply for the ten (10) year period except in the cases where information to the contrary is available.

7.3.2 Assumption 2

For parts and components whose failure distribution is Gaussian. convert to the appropriate constant failure rate distribution and specify assumed maintenance intervals. The steps involved in converting a Gaussian distribution to an approximate equivalent constant failure rate distribution are as follows:

(a) Determine, by prediction or estimation, the mean, $(\bar{X})$, and standard deviation, (s) of the Gaussian (normal) failure distribution.

(b) Determine the number of standard deviations between t = o (where t is time) and the mean. R

(c) If $\bar{X}$ is large as related to s, the shape of the normal curve from t = o to t = x - 3s is relatively flat. The failure rate over the range t = o to t = $\bar{X}$ - 3s can be calculated by dividing the probability of failure (area under normal curve) over this range by the time interval of the range. Since the curve is essentially flat, the failure rate is approximately constant.

(d) The approximation to a constant failure rate is appropriate for only the duration of the interval used in the calculation. However, if an equipment can be restored to its original operating condition by performing maintenance at intervals equal to, or less than, the ones used in calculating a constant failure rate, this failure rate can be applied to extended periods of time.

7.3.3 Assumption 3

The density function of inadvertent launch is uniform with time when Assumptions I and II above are utilized in calculations.

7.4 Logic Gate Formulas

These Logic Gate formulas are applicable to the inadvertent launch calculations because they account for failure duration times. They will not apply, except for rare instances, in the faulty launch calculations.

7.4.1 Coexistence of Failures at AND Gates.

Given n repairable items. Let event A_1 represent the failure of item 1, event A_2 the failure of item 2, and in general A_i the failure item i. Suppose each item i fails randomly with constant failure rate λ_i and duration time τ_i for i = 1, 2, . . . n where λ_i and τ_i are in consistent units. Duration time is defined as the time from the occurrence of a failure to the time at which it is rendered ineffective. The expression $1 - e^{-\lambda T}$ is the probability that an item, with constant failure rate λ, will fail in an interval of time T, given that the item was working at the beginning of the interval.

Consider an interval of time 0 to T as shown in Fig. 7.4.1-1.

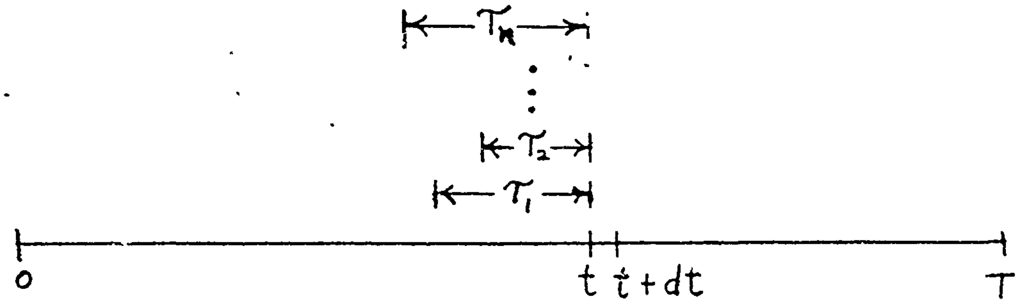


Fig. 7.4.1-1

If $\frac{\tau_i}{T}$ and $\lambda_i \tau_i$ are small for i = 1, 2, . . . n, then the probability that $A_1, A_2, \ldots A_n$ coexist in the interval (t, t + dt) given that they have not coexisted up to time t is given by the following expression.

$$\begin{aligned}
&\lambda_1\, dt\, (1 - e^{-\lambda_2 \tau_2})(1 - e^{-\lambda_3 \tau_3}) \ldots (1 - e^{-\lambda_n \tau_n}) \\
&+ \lambda_2\, dt\, (1 - e^{-\lambda_1 \tau_1})(1 - e^{-\lambda_3 \tau_3}) \ldots (1 - e^{-\lambda_n \tau_n}) \\
&+ \lambda_3\, dt\, (1 - e^{-\lambda_1 \tau_1})(1 - e^{-\lambda_2 \tau_2})(1 - e^{-\lambda_4 \tau_4}) \ldots (1 - e^{-\lambda_n \tau_n} \\
&\vdots \\
&+ \lambda_n\, dt\, (1 - e^{-\lambda_1 \tau_1})(1 - e^{-\lambda_2 \tau_2}) \ldots (1 - e^{-\lambda_{n-1} \tau_{n-1}}) \\
&= H\, dt
\end{aligned}$$

This expression is obtained by adding together the probabilities of each way in which n events can coexist for the first time in the dt interval. For example: A_1 can happen in the dt interval with a probability of λ_1 dt. If A_2 is to coexist with A_1 in the dt interval, it must occur some time in a τ_2 time period prior to t; the probability of this is $(1 - e^{-\lambda 2 \tau 2})$. If A_2 occurs before t - τ_2, it will be repaired before it can coexist with A_1 in the dt interval. If A_2 occurs after t, it will not coexist with A_1 in the particular dt interval under consideration. Similarly, A_3 must occur in a τ_3 interval before t with a probability of $(1 - e^{-\lambda 3 \tau 3})$ in order to coexist with A_1 for the first time in the dt interval, etc. The product of these probabilities expresses their joint occurrence and gives the first term of the above expression.

Now let f(t) be the probability that $A_1, A_2, \ldots A_n$ have not coexisted up to time t. Then f(t + dt) is the probability that $A_1, A_2, \ldots A_n$ have not coexisted during the time period from o to t + dt; this can also be expressed as

$$f(t + dt) = f(t)\,(1 - H\,dt)$$

where (1 - H dt) is the probability that $A_1, A_2, \ldots A_n$ do not coexist in the dt interval.

Now by definition, the differential of f(t) is f(t + dt) - f(t); therefore, $d\,f(t) = f(t)\,(1 - H\,dt) - f(t)$

$$d\,f(t) = f(t)\,(- H\,dt)$$

and

$$\frac{df(t)}{f(t)} = - H\,dt$$

Solving this differential equation by integration we have $\ln f(t) = - Ht + c$.

But when t = o, f(t) = 1, ln f(t) = o and therefore c = o so that

$$f(t) = e^{-Ht}$$

The probability (P_A) that $A_1, A_2 \ldots A_n$ coexist at some time during the interval T is then given by the following:

$$P(A) = 1 - f(T) = 1 - e^{-HT} \quad \ldots$$

By comparing this equation with the standard equation for probability of failure $(1 - e^{-\lambda T})$ one can easily see that H is the failure rate for the coexistence of n events or, in other words, it is the failure rate appearing at the output of an AND gate. From this point on, therefore, H will be replaced by λ_n (i.e., the failure rate for the intersection of n failures.) If $\lambda_i \tau_i$ is small for all i from 1 to n then H reduces to the following expression.

$$\lambda_\cap = \lambda_1\lambda_2 \cdots \lambda_n (\tau_2\tau_3 \cdots \tau_n + \tau_1\tau_3 \cdots \tau_n + \cdots + \tau_1\tau_2 \cdots \tau_{n-1})$$

If duration times are all equal, $\lambda_\cap$ reduces to

$$\lambda_\cap = n \lambda_1 \lambda_2 \cdots \lambda_n \tau^{n-1}$$

7.4.2 Effective Duration Time ($\tau_\cap$) at the Output of an AND Gate

Consider the logic configuration shown in Fig. 7.4.2-1.

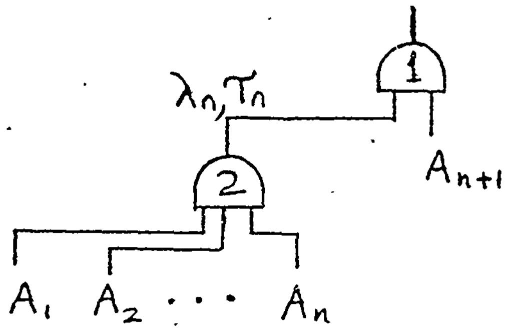


Fig. 7.4.2-1

By Boolean algebra it is evident that the output of gate (1) is $A_1 A_2 \ldots A_{n+1}$. According to the general expression obtained in paragraph 7.4.1, the failure rate at the output of gate (1) is, therefore,

$$\lambda_1 \lambda_2 \cdots \lambda_{n+1} (\tau_2\tau_3 \cdots \tau_{n+1} + \tau_1\tau_3 \cdots \tau_{n+1} + \tau_1\tau_2 \cdots \tau_n)$$

This must be equal to the failure rate obtained by combining the output of gate (2), having failure rate $\lambda_\cap$ and duration time $\tau_\cap$, with the failure rate and duration time of event A_{n+1}. This is expressed as follows:

$$\lambda_\cap \lambda_{n+1} (\tau_\cap + \tau_{n+1})$$

$$= \lambda_1 \lambda_2 \cdots \lambda_{n+1} (\tau_2\tau_3 \cdots \tau_{n+1} + \tau_1\tau_3 \cdots \tau_{n+1} + \cdots + \tau_1\tau_2 \cdots \tau_n)$$

Substituting in the general expression for $\lambda_\cap$ we get

$$\lambda_1\lambda_2 \cdots \lambda_n (\tau_2\tau_3 \cdots \tau_n + \tau_1\tau_3 \cdots \tau_n + \cdots + \tau_1\tau_2 \cdots \tau_{n-1}) \lambda_{n+1} (\tau_\cap + \tau_{n+1})$$

$$= \lambda_1\lambda_2 \cdots \lambda_{n+1} (\tau_2\tau_3 \cdots \tau_{n+1} + \tau_1\tau_3 \cdots \tau_{n+1} + \cdots + \tau_1\tau_2 \cdots \tau_n)$$

Therefore,

$$\tau_\cap = \frac{\tau_1 \tau_2 \cdots \tau_n}{\tau_2 \tau_3 \cdots \tau_n + \tau_1 \tau_3 \cdots \tau_n + \cdots + \tau_1 \tau_2 \cdots \tau_{n-1}}$$

or

$$\tau_\cap = \frac{1}{\frac{1}{\tau_1} + \frac{1}{\tau_2} + \cdots + \frac{1}{\tau_n}}$$

If $\tau_1 = \tau_2 = \cdots = \tau_n = \tau$ then $\tau_\cap$ reduces to

$$\tau_\cap = \frac{\tau}{n}.$$

It can be observed that $\tau_\cap$ is an essential factor which enables the transfer of failure rates through succeeding logic gates.

7.4.3 Failure Rate ($\lambda_\cup$) at the Output of an OR Gate

Given an interval of time T, the probability ($\overline{P}_o$) that none of the events $A_1, A_2, \cdots A_n$ occur in the interval of time is

$$\overline{P}_o = e^{-\lambda_1 T} e^{-\lambda_2 T} \cdots e^{-\lambda_n T}$$

$$= e^{-(\lambda_1 + \lambda_2 + \cdots + \lambda_n) T}$$

The probability (P_o) that any one of the events $A_1, A_2, \cdots A_n$ occurs is

$$P_o = 1 - \overline{P}_o = 1 - e^{-(\lambda_1 + \lambda_2 + \cdots + \lambda_n)T}.$$

This shows that the failure rate at the output of an OR gate (i.e., the failure rate for the union of failures) is the sum of the input failure rates or

$$\lambda_\cup = \lambda_1 + \lambda_2 + \cdots + \lambda_n$$

7.4.4 Effective Duration Time ($\tau_\cup$) at the Output of an OR Gate.

Consider the logic configuration shown in Fig. 7.4.4-1.

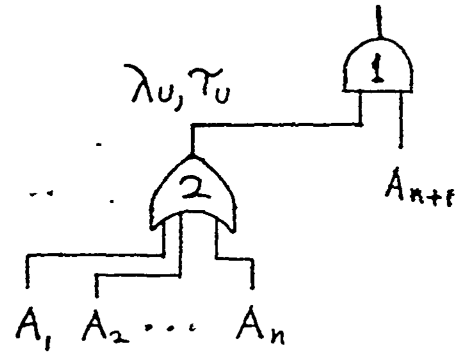


Fig. 7.4.4-1

By Boolean algebra the output of gate (1) is

$A_1 A_{n+1} + A_2 A_{n+1} + \cdots + A_n A_{n+1}$.

The failure rate for the output of gate (1) is, therefore,

$$\lambda_1\lambda_{n+1}(\tau_1+\tau_{n+1})+\lambda_2\lambda_{n+1}(\tau_2+\tau_{n+1})+\cdots+\lambda_n\lambda_{n+1}(\tau_n+\tau_{n+1})$$

This must be equal to the failure rate obtained by combining the output of gate (2), having failure rate λ_U and effectivity time τ_U with the failure rate and effectivity time of event A_{n+1}. This is expressed as follows:

$$\lambda_U\lambda_{n+1}(\tau_U+\tau_{n+1}) =$$
$$\lambda_1\lambda_{n+1}(\tau_1+\tau_{n+1})+\lambda_2\lambda_{n+1}(\tau_2+\tau_{n+1})+\cdots+\lambda_n\lambda_{n+1}(\tau_n+\tau_{n+1})$$

Substituting in the expression for λ_U we get

$$(\lambda_1+\lambda_2+\cdots+\lambda_n)\lambda_{n+1}(\tau_U+\tau_{n+1})$$
$$=\lambda_1\lambda_{n+1}(\tau_1+\tau_{n+1})+\lambda_2\lambda_{n+1}(\tau_2+\tau_{n+1})+\cdots+\lambda_n\lambda_{n+1}(\tau_n+\tau_{n+1})$$

Therefore, $\tau_U = \dfrac{\lambda_1\tau_1+\lambda_2\tau_2+\cdots+\lambda_n\tau_n}{\lambda_1+\lambda_2+\cdots+\lambda_n}$

If $\tau_1 = \tau_2 = \dots = \tau_n = \tau$ then $\tau_\cup$ reduces to

$$\tau_\cup = \tau$$

As with $\tau_\cap$, $\tau_\cup$ is an essential factor which enables the transfer of failure rates through succeeding logic gates.

7.4.5 The foregoing results are summarized in Table 1. A general proof of the validity of these results is given in paragraph 7.4.7. The logic gate formulas are directly applicable to Boolean expressions as well as to logic gates.

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

TABLE 1. LOGIC GATE FORMULAS

7.4.6 Combining Probabilities with Failure Rates at Logic Gates

In evaluating the fault trees, the need will arise to combine failure rates with probabilities. An example of this are shown below.

7.4.6.1 Random Generation of ELC

7.4.6.1.1 Conditions:

(a) Let λ_1, λ_2, τ_1 and τ_2 be equipment failure rates and corresponding fault durations of equipment failures which result in the generation, transmission, or receipt of random bits.

(b) Let P represent the probability that 1 word length of random bits have the correct ELC format.

(c) Let C represent the period between radio or cable slots at a particular Launch facility, i.e., the time for one cycle. C is smaller than both τ_1 and τ_2.

(d) Assume that only one valid ELC can be transmitted in a time slot. Assume also that P, $\lambda_1 \tau_1$ and $\lambda_2 \tau_2$ are small.

7.4.6.1.2 Conclusion:

The failure rate for the random generation of an ELC under the above conditions is.

$$\lambda_{ELC} = \frac{P \lambda_1 \lambda_2 \tau_1 \tau_2}{C}$$

If only one equipment failure is required, then the failure rate is

$$\lambda_{ELC} = \frac{P \lambda_1 \tau_1}{C}$$

The effective duration of an ELC failure (τ_{ELC}) is zero.

7.4.6.1.3 **Derivation:**

Consider the interval of time shown in Fig. 7.4.6.1.3-1.

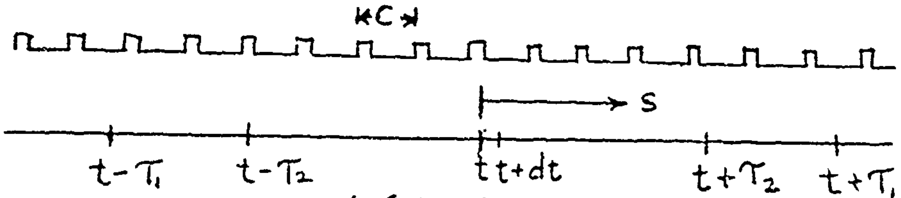


Fig. 7.4.6.1.3-1

By reasoning similar to that given in Paragraph 7.4.1, the probability (P_c) that A_1 and A_2 coexist with a time slot in which a valid ELC is generated is

$$P_c = \lambda_1 dt \int_0^{\tau_2} \frac{PS}{C} \lambda_2 ds + \lambda_2 dt \left[\int_0^{\tau_2} \frac{PS}{C} \lambda_1 ds + + \frac{P\tau_2}{C} \lambda_1 (\tau_1 - \tau_2) \right]$$

Where $\frac{S}{C}$ is the number of slots available for ELC generation as a function of position S.

From this it can be shown that the failure rate is

$$\lambda_{ELC} = \frac{P\lambda_1 \lambda_2 \tau_1 \tau_2}{C}$$

7.4.7 Proof of Logic Gate Formulas

Suppose we are given a fault tree where only coexistance of events is of concern at each AND gate (i.e., the order in which events occur in time is not important). Suppose further the bottom elements of the fault tree consist of items which can be assigned constant failure rates and fixed duration times from the advent of the failure to the correction of the failure (i.e., fixed repair times). We proceed up the fault tree obtaining new λ's and τ's by use of the following formulas. Suppose we have n events, $A_1, A_2 \ldots A_n$ to be ANDed and suppose we have associated with them the failure rates $\lambda_1, \lambda_2 \ldots \lambda_n$ and "effective duration times" $\tau_1, \tau_2 \ldots, \tau_n$. The λ, output of the gate is given by

$$\lambda_1 \cdots \lambda_n (\tau_1 \tau_2 \cdots \tau_{n-1} + \tau_1 \tau_2 \cdots \tau_{n-2} \tau_n + \cdots + \tau_2 \cdots \tau_n). \qquad (1)$$

The τ output (effective duration time output) is given by

$$\frac{1}{\frac{1}{\tau_1} + \frac{1}{\tau_2} + \cdots + \frac{1}{\tau_n}}. \qquad (2)$$

If the n events are to be ORed, the λ output is

$$\lambda_1 + \lambda_2 + \cdots + \lambda_n \qquad (3)$$

and the τ output is

$$\frac{\lambda_1 \tau_1 + \cdots + \lambda_n \tau_n}{\lambda_1 + \cdots + \lambda_n} \qquad (4)$$

we will prove that the failure rate output at any gate in the fault tree is correct when the above formulas are used. Write the output from any logic gate as the union of n chains, $E_1, E_2, \ldots E_n$, (A chain is a series of ANDed events.) where

$$E_1 = F_1^1 \cap F_2^1 \cap \cdots \cap F_{k_1}^1$$
$$\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots$$
$$E_n = F_1^n \cap F_2^n \cap \cdots \cap F_{k_n}^n.$$

We will prove that in every case the τ output of any logic gate will be of the form

$$\frac{\lambda_{F_1^1}\cdots\lambda_{F_{k_1}^1}\tau_{F_1^1}\cdots\tau_{F_{k_1}^1}+\cdots+\lambda_{F_1^n}\cdots\lambda_{F_{k_n}^n}\tau_{F_1^n}\cdots\tau_{F_{k_n}^n}}{\lambda_{\Gamma_1^1}\cdots\lambda_{F_{k_1}^1}\left(\tau_{F_1^1}\cdots\tau_{F_{k_1-1}^1}+\cdots+\tau_{F_2^1}\cdots\tau_{F_{k_1}^1}\right)+\cdots+\lambda_{F_1^n}\cdots\lambda_{F_{k_n}^n}\left(\tau_{F_1^n}\cdots\tau_{F_{k_r-1}^n}+\cdots+\tau_{F_2^n}\cdots\tau_{F_{k_n}^n}\right)} \quad (5)$$

and the output will be of the form

$$\lambda_{F_1^1}\cdots\lambda_{F_{k_1}^1}\left(\tau_{F_1^1}\cdots\tau_{F_{k_1-1}^1}+\cdots+\tau_{F_2^1}\cdots\tau_{F_{k_1}^1}\right)+\cdots$$
$$+\lambda_{F_1^n}\cdots\lambda_{F_{k_n}^n}\left(\tau_{F_1^n}\cdots\tau_{F_{k_r-1}^r}+\cdots+\tau_{F_2^n}\cdots\tau_{F_{k_n}^n}\right) \quad (6)$$

We proceed by induction. We will assume that the above is true for two inputs into an AND or an OR gate. This will later by generalized for any number of inputs into an AND or an OR gate.

7.4.7.1 Proof of OR Gate Formulas

Suppose at step n we take the union of two branches, branch 1 (β_1) and branch 2 (β_2).

Suppose branch 1 is the union of n chains, $C_1, C_2 \cdots C_n$ where

$$C_1 = A_1^1 \cap A_2^1 \cap \cdots \cap A_{k_1}^1$$
$$\cdots\cdots$$
$$C_n = A_1^n \cap A_2^n \cap \cdots \cap A_{k_n}^n$$

Suppose branch 2 is the union of m chains

$$D_1 = B_1^1 \cap B_2^1 \cap \cdots \cap B_{\ell_1}^1$$
$$\cdots\cdots$$
$$D_m = B_1^m \cap \cdots \cap B_{\ell_m}^m$$

then by the induction assumption (Equations 5 and 6) the τ's we have at this point are

$$\tau_{\beta_1} = \frac{\lambda_{A_1^1}\cdots\lambda_{A_{k_1}^1}\tau_{A_1^1}\cdots\tau_{A_{k_1}^1}+\cdots+\lambda_{A_1^n}\cdots\lambda_{A_{k_n}^r}\tau_{A_1^n}\cdots\tau_{A_{k_n}^n}}{\lambda_{A_1^1}\cdots\lambda_{A_{k_1}^1}\left(\tau_{A_1^1}\cdots\tau_{A_{k_1-1}^1}+\cdots+\tau_{A_2^1}\cdots\tau_{A_{k_1}^1}\right)+\cdots+\lambda_{A_1^n}\cdots\lambda_{A_{k_n}^n}\left(\tau_{A_1^n}\cdots\tau_{A_{k_n-1}^n}+\cdots+\tau_{A_2^n}\cdots\tau_{A_{k_n}^n}\right)}$$

and

$$\tau_{\beta_2} = \frac{\lambda_{B_1^1}\cdots\lambda_{B_{\ell_1}^1}\tau_{B_1^1}\cdots\tau_{B_{\ell_1}^1}+\cdots+\lambda_{B_1^m}\cdots\lambda_{B_{\ell_m}^m}\tau_{B_1^m}\cdots\tau_{B_{\ell_m}^m}}{\lambda_{B_1^1}\cdots\lambda_{B_{\ell_1}^1}\left(\tau_{B_1^1}\cdots\tau_{B_{\ell_1-1}^1}+\cdots+\tau_{B_2^1}\cdots\tau_{B_{\ell_1}^1}+\cdots+\lambda_{B_1^m}\cdots\lambda_{B_{\ell_m}^m}\left(\tau_{B_1^m}\cdots\tau_{B_{\ell_m-1}^m}+\cdots+\tau_{B_2^m}\cdots\tau_{B_{\ell_m}^m}\right)}$$

The λ's are

$$\lambda_{\beta_1} = \lambda_{A_1^1} \cdots \lambda_{A_{k_1}^1}\left(\tau_{A_1^1} \cdots \tau_{A_{k_1-1}^1} + \cdots + \tau_{A_2^1} \cdots \tau_{A_{k_1}^1}\right) + \cdots$$
$$+ \lambda_{A_1^n} \cdots \lambda_{A_{k_n}^n}\left(\tau_{A_1^n} \cdots \tau_{A_{k_n-1}^n} + \cdots + \tau_{A_2^n} \cdots \tau_{A_{k_n}^n}\right)$$

$$\lambda_{\beta_2} = \lambda_{B_1^1} \cdots \lambda_{B_{\ell_1}^1}\left(\tau_{B_1^1} \cdots \tau_{B_{\ell_1-1}^1} + \cdots + \tau_{B_2^1} \cdots \tau_{B_\ell^1}\right) + \cdots$$
$$+ \lambda_{B_1^m} \cdots \lambda_{B_{\ell_m}^m}\left(\tau_{B_1^m} \cdots \tau_{B_{\ell_m-1}^m} + \cdots + \tau_{B_2^m} \cdots \tau_{B_{\ell_m}^m}\right)$$

$\beta_1 \cup \beta_2$ consists of the m + n chains $C_1, \cdots C_n, D_1 \cdots D_m$.

From paragraph 7.4.3, $\lambda_{\beta_1 \cup \beta_2} = \lambda_{\beta_1} + \lambda_{\beta_2}$

Write $\tau_{\beta_1} = \dfrac{A}{\lambda_{\beta_1}}$

where $A = \lambda_{A_1^1} \cdots \lambda_{A_{k_1}^1} \tau_{A_1^1} \cdots \tau_{A_{k_1}^1} + \cdots + \lambda_{A_1^n} \cdots \lambda_{A_{k_n}^n} \tau_{A_1^n} \cdots \tau_{A_{k_n}^n}$

Similarly, write $\tau_{\beta_2} = \dfrac{B}{\lambda_{\beta_2}}$

where $B = \lambda_{B_1^1} \cdots \lambda_{B_{\ell_1}^1} \tau_{B_1^1} \cdots \tau_{B_{\ell_1}^1} + \cdots + \lambda_{B_1^m} \cdots \lambda_{B_{\ell_m}^m} \tau_{B_1^m} \cdots \tau_{B_{\ell_m}^m}$

Now the τ output should be $\dfrac{A+B}{\lambda_{\beta_1} + \lambda_{\beta_2}}$. This is seen by by examining Equation 5 where the chains are $C_1, \cdots C_n, D_1, \cdots D_m$.

By equation 4,

$$\tau_{\beta_1 \cup \beta_2} = \frac{\lambda_{\beta_1}\tau_{\beta_1} + \lambda_{\beta_2}\tau_{\beta_2}}{\lambda_{\beta_1} + \lambda_{\beta_2}} = \frac{\lambda_{\beta_1}\dfrac{A}{\lambda_{\beta_1}} + \lambda_{\beta_2}\dfrac{B}{\lambda_{\beta_2}}}{\lambda_{\beta_1} + \lambda_{\beta_2}}$$
$$= \frac{A+B}{\lambda_{\beta_1} + \lambda_{\beta_2}}$$

This proves the τ output of an OR gate maintains the correct form (as given by Equation 5) when Equation 4 is applied.

7.4.7.2 Proof of AND Gate Formulas

It will now be shown that the τ output of an AND gate is of the correct form and that the output of the AND gate is correct given (by induction) that the λ inputs are correct and the τ's are of the form indicated by Equation 5. We are now interested in $\tau_{\beta_1 \cap \beta_2}$.

We first ascertain what the correct τ is.

$$\beta_1 \cap \beta_2 = (C_1 \cup C_2 \cup \cdots \cup C_n) \cap (D_1 \cup D_2 \cup \cdots \cup D_m)$$

$$= C_1 \cap D_1 \cup C_1 \cap D_2 \cup \cdots \cup C_1 \cap D_m \cup C_2 \cap D_m \cup \cdots \cup C_n \cap D_1 \cup \cdots \cup C_n \cap D_m$$

$$= A_1^1 \cap A_2^1 \cap \cdots \cap A_{k_1}^1 \cap B_1^1 \cap B_2^1 \cap \cdots \cap B_{l_1}^1 \cup A_1^1 \cap \cdots \cap A_{k_1}^1 \cap B_1^2 \cap \cdots \cap B_{l_2}^2 \cup \cdots \cup A_1^n \cap \cdots \cap A_{k_n}^n \cap B_1^m \cap \cdots \cap B_{l_m}^m$$

The correct τ by Equation 5 is seen to be

$$\frac{\lambda_{A_1^1} \cdots \lambda_{A_{k_1}^1} \lambda_{B_1^1} \cdots \lambda_{B_{l_1}^1} \tau_{A_1^1} \cdots \tau_{A_{k_1}^1} \tau_{B_1^1} \cdots \tau_{B_{l_1}^1} + \cdots + \lambda_{A_1^n} \cdots \lambda_{A_{k_n}^n} \lambda_{B_1^m} \cdots \lambda_{B_{l_m}^m} \tau_{A_1^n} \cdots \tau_{A_{k_n}^n} \tau_{B_1^m} \cdots \tau_{B_{l_m}^m}}{C} \quad (7)$$

where

$$C = \lambda_{\beta_1 \cap \beta_2}$$
$$= \lambda_{A_1^1} \cdots \lambda_{A_{k_1}^1} \lambda_{B_1^1} \cdots \lambda_{B_{l_1}^1} (\tau_{A_1^1} \cdots \tau_{A_{k_1}^1} \tau_{B_1^1} \cdots \tau_{B_{l_1 - 1}^1} + \cdots + \tau_{A_2^1} \cdots \tau_{A_{k_1}^1} \tau_{B_1^1} \cdots \tau_{B_{l_1}^1}) + \cdots + \lambda_{A_1^n} \cdots \lambda_{A_{k_n}^n} \lambda_{B_1^m} \cdots \times \lambda_{B_{l_m}^m} (\tau_{A_1^n} \cdots \tau_{A_{k_n}^n} \tau_{B_1^m} \cdots \tau_{B_{l_m - 1}^m} + \cdots + \tau_{A_2^n} \cdots \tau_{B_{l_m}^m})$$

We have

$$\frac{1}{\frac{1}{\tau_{\beta_1}} + \frac{1}{\tau_{\beta_2}}} = \frac{\tau_{\beta_1} \tau_{\beta_2}}{\tau_{\beta_1} + \tau_{\beta_2}}$$

$$= \frac{\frac{AB}{\lambda_{\beta_1} \lambda_{\beta_2}}}{\frac{A}{\lambda_{\beta_1}} + \frac{B}{\lambda_{\beta_2}}}$$

$$= \frac{AB}{A\lambda_{\beta_2} + B\lambda_{\beta_1}}$$

Now

$$AB = \lambda_{A_1^1}\cdots\lambda_{A_{k_1}^1}\lambda_{B_1^1}\cdots\lambda_{B_{\ell_1}^1}\tau_{A_1^1}\cdots\tau_{A_{k_1}^1}\tau_{B_1^1}\cdots\tau_{B_{\ell_1}^1}+\cdots$$
$$+\lambda_{A_1^n}\cdots\lambda_{A_{k_n}^n}\lambda_{B_1^m}\cdots\lambda_{B_{\ell_m}^m}\tau_{A_1^n}\cdots\tau_{B_{\ell_m}^m}$$

AB is therefore identical with the numerator of Equation 7. It follows that we must now only show that $A\lambda_{\beta_2}+B\lambda_{\beta_1}=C$.

$$A\lambda_{\beta_2}+B\lambda_{\beta_1}$$
$$=\lambda_{A_1^1}\cdots\lambda_{A_{k_1}^1}\lambda_{B_1^1}\cdots\lambda_{B_{\ell_1}^1}\left(\tau_{A_1^1}\cdots\tau_{A_{k_1}^1}\tau_{B_1^1}\cdots\tau_{B_{\ell_1-1}^1}+\cdots+\tau_{A_1^1}\cdots\tau_{A_{k_1}^1}\tau_{B_2^1}\cdots\tau_{B_{L_1}^1}\right)$$
$$+\cdots+\lambda_{A_1^h}\cdots\lambda_{A_{k_n}^n}\lambda_{B_1^m}\cdots\lambda_{B_{\ell_m}^m}\left(\tau_{A_1^n}\cdots\tau_{A_{k_n}^n}\tau_{B_1^m}\cdots\tau_{B_{\ell_m-1}^m}+\cdots+\tau_{A_1^n}\cdots\tau_{A_{k_n}^n}\tau_{B_2^m}\cdots\tau_{B_{\ell_m}^m}\right)$$
$$+\lambda_{B_1^1}\cdots\lambda_{B_{\ell_1}^1}\lambda_{A_1^1}\cdots\lambda_{A_{k_1}^1}\left(\tau_{B_1^1}\cdots\tau_{B_{\ell_1}^1}\tau_{A_1^1}\cdots\tau_{A_{k_1-1}^1}+\cdots+\tau_{B_1^1}\cdots\tau_{B_{\ell_1}^1}\tau_{A_2^1}\cdots\tau_{A_{k_1}^1}\right)$$
$$+\cdots+\lambda_{B_1^m}\cdots\lambda_{B_{\ell_m}^m}\lambda_{A_1^n}\cdots\lambda_{A_{k_n}^n}\left(\tau_{B_1^m}\cdots\tau_{B_{\ell_m}^m}\tau_{A_1^n}\cdots\tau_{A_{k_n-1}^n}+\cdots+\tau_{B_1^m}\cdots\tau_{B_{\ell_m}^m}\tau_{A_2^n}\cdots\tau_{A_{k_n}^n}\right)$$

Regrouping the above by adding line one of the above to line 3 and line 2 to line 4 (In general line y would be added to line $m+n+y$ for $y=1,2\cdots m+n$), it is easily seen that the result is C. It remains to show that the failure rate from the output of the AND gate is correct. This means we must show that

$$\lambda_{\beta_1}\lambda_{\beta_2}(\tau_{\beta_1}+\tau_{\beta_2}) = C$$
$$= \lambda_{\beta_1\cap\beta_2}$$

But

$$\lambda_{\beta_1}\lambda_{\beta_2}\left(\frac{A}{\lambda_{\beta_1}}+\frac{B}{\lambda_{\beta_2}}\right) = A\lambda_{\beta_2}+B\lambda_{\beta_1}$$
$$= C$$

by what we just proved.

7.4.7.3 Generalization

We have shown that $\dfrac{1}{\frac{1}{\tau_1}+\frac{1}{\tau_2}}$ is the correct τ formula for 2 items.

Assume $\dfrac{1}{\frac{1}{\tau_1}+\cdots+\frac{1}{\tau_n}}$ is the correct τ formula for n items, then

$$\frac{1}{\dfrac{1}{\dfrac{1}{\frac{1}{\tau_1}+\cdots+\frac{1}{\tau_n}}}+\dfrac{1}{\tau_{n+1}}}$$

is the correct τ formula for n+1 items ANDed together.

But

$$\frac{1}{\dfrac{1}{\dfrac{1}{\frac{1}{\tau_1}+\cdots+\frac{1}{\tau_n}}}+\dfrac{1}{\tau_n+1}} = \frac{1}{\frac{1}{\tau_1}+\frac{1}{\tau_2}+\cdots+\frac{1}{\tau_{n+1}}}$$

This proves the τ formula for n items ANDed together. A similar argument proves the OR formula for n items and the λ formula for n items ANDed together.

7.5 Interacting Branches

When two or more branches interact or, in other words, when a failure is common to two or more branches of a fault tree, error is induced into the final probability number unless the Boolean expression is simplified. This fact is noted in Section 5 Page 6. When combining failure rates through AND and OR gates from the bottom of the fault tree to the top, careful inspection must be employed to insure that no unconservative error is induced into the probability calculation. A conservative error is defined as an error which makes the final probability number larger than it should be. A discussion of errors and remedies follows.

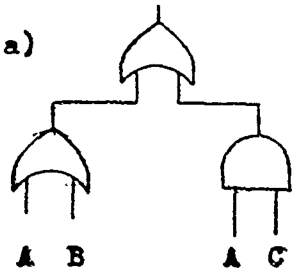
7.5.1 OR Gate Interaction Error

If two or more branches with common terms unite at an OR gate, the induced error is conservative and often insignificant. The general proof of this is found in paragraph 7.5.4.2. The conservative error induced by common branches at an OR gate is not a serious condition; however, if further refinement is desirable, the Boolean expression may be obtained and simplified up to the point at which the branches unite.

7.5.1.1 Examples:

In both cases shown below, the probability expression on the left of the inequality sign (the probability which would be obtained by combining probabilities directly through logic gates) is seen to be conservative.

(a)

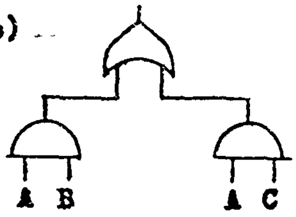


Unsimplified - Simplified

$$A + B + AC = A + B$$

$$P(A) + P(B) + P(A)\,P(C) > P(A) + P(B) - P(A)\,P(B)$$

(b)



Unsimplified - Simplified

$$AB + AC = A(B + C)$$

$$P(A)\,P(B) + P(A)P(C) > P(A)\left[P(B) + P(C) - P(B)\,P(C)\right]$$

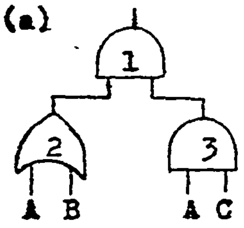
7.5.2 AND Gate Interaction Error

If two or more branches with common terms unite at an AND gate, an unconservative error is always induced. This is proved in general in paragraph 7.5.4.3.

7.5.2.1 Examples:

In both cases shown below, the probability expression on the left of the inequality sign (the probability which would be obtained by combining probabilities directly through logic gates) is seen to be unconservative.

(a)

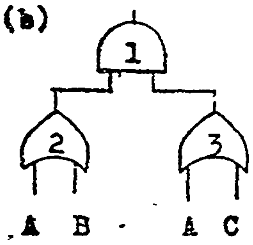


Unsimplified – Simplified

$$(A + B)\ AC = AC$$

$$\left[P(A) + P(B)\right] P(A)P(C) < P(A)P(C)$$

(b)



Unsimplified - Simplified

$$(A + B)\ (A + C) = A + BC$$

$$\left[P(A)\right]^2 + P(A)P(C) + P(A)P(B) + P(B)P(C) < P(A) + P(B)P(C) - P(A)P(B)P(C)$$

Since this condition results in a final probability number which is smaller than it should be, a remedy must be applied to eliminate its effect.

7.5.2.2 Remedies:

7.5.2.2.1 The AND gate interaction error can be removed entirely by expressing the terms of the interacting branches in Boolean form and by simplifying the expression. The logic gate formulas can then be applied directly to the expression without restoring it to fault tree form. The Boolean expression need only be obtained up to the logic gate at which the interacting branches unite.

7.5.2.2.2 A conservative estimate of the final probability number may be obtained by substituting a probability of unity into all but one of the common terms. The unity probability should be assigned first to common terms at OR gates when a choice exists. If this remedy is applied to the probability expression of Example (a) of Paragraph 7.5.2.1, the following results are obtained.

$$\left[P(A) + P(B)\right] P(A)\ P(C) < P(A)\ P(C)$$

$$\left[1 + P(B)\right] P(A)\ P(C) > P(A)\ P(C)$$

$$P(A)\ P(C) + P(A)\ P(B)\ P(C) > P(A)\ P(C)$$

~~26~~ 40

Similarly, applying this remedy to Example (b) of Paragraph 7.5.2.1, we obtain the following.

$$\left[P(A) + P(B)\right] \left[P(A) + P(C)\right] < P(A) + P(B)\ P(C) - P(A)\ P(B)\ P(C)$$

$$\left[1 + P(B)\right] \left[P(A) + P(C)\right] > P(A) + P(B)\ P(C) - P(A)\ P(B)\ P(C)$$

$$P(A) + P(C) + P(A)\ P(B) + P(B)\ P(C) > P(A) + P(B)\ P(C) - P(A)P(B)P(C)$$

7.5.3 Even though the probability of a common term may be negligible with respect to other probabilities at an OR gate, its effect as an interacting branch cannot be ignored. For example, suppose P(A) is negligible compared to P(B) in Examples (a) and (b) of Paragraph 7.5.2.1. It can readily be observed that an unconservative error is induced if the A term at the affected OR gate (gate 2) is dropped.

7.5.4 The foregoing results apply when combining failure rates through logic gates as well as when combining probabilities. If the methods of Paragraph 7.5.2.2.2 are used, the following rules govern in the combination of failure rates with unity probability:

7.5.4.1 If failure rates are to be combined with unity probability at an OR gate, the output of the OR gate has a probability of unity.

7.5.4.2 If failure rates are to be combined with unity probability at an AND gate, the input with unity probability is ignored since it has no effect at this gate.

7.5.5 Proof of the Effect of Interacting Branches at a Logic Gate.

7.5.5.1 Preliminary Information

Any branch of a fault tree may be represented as a union of chains. A chain is defined as an intersection of one or more events. For example, suppose a branch of the fault tree has the following Boolean equation.

$$\left[(R + S)\ T\right] \left[N + V\ (W + XY)\right] + Z$$

This equation can be reduced to

$$RTN + RTVW + RTVXY + STN + STVW + STVXY + Z,$$

which is a union of seven chains. In the discussion to follow, the Boolean symbols $\cup$ and $\cap$ will be used in the place of + and x respectively for the sake of clarity. The above equation can then be expressed in the following form.

$$K_1 \cup K_2 \cup K_3 \cup K_4 \cup K_5 \cup K_6 \cup K_7 = \bigcup_{i=1}^{7} K_i$$

where K_1 = RTN, K_2 = RTVW, K_3 = RTVXY, etc.

Now suppose we wish to factor the common event R from each of the terms of the above expression. We can write it as follows:

$$\bigcup_{i=1}^{7} K_i = \bigcup_{i=4}^{7} K_i \cup R \cap \bigcup_{j=1}^{3} L_j$$

where L_1 = TN, L_2 = TVW and L_3 = TVXY.

7.5.5.2 Interacting Branches Unite at an OR Gate

Let A represent an event which is common to more than one branch of a fault tree. Consider the logic gate at which two or more interacting branches unite. Since all inputs of a logic gate can be combined two at a time, the case of two branches into a logic gate need only be considered. Let the two input branches be labeled events B and C.

Representing B and C as unions of chains as above, we get the following:

$$B = \bigcup_{g=1}^{m} D_g \cup A \cap \bigcup_{i=1}^{n} E_i$$

$$C = \bigcup_{j=1}^{p} F_j \cup A \cap \bigcup_{k=1}^{r} G_k$$

These equations express the fact that the common term A is contained in some chains and not in others.

If the two interacting branches unite at an OR gate, the Boolean expression is

$$B \cup C = \bigcup_{g=1}^{m} D_g \cup A \cap \bigcup_{i=1}^{n} E_i \cup \bigcup_{j=1}^{p} F_j \cup A \cap \bigcup_{k=1}^{r} G_k$$

$$= \bigcup_{g=1}^{m} D_g \cup \bigcup_{j=1}^{p} F_j \cup A \cap \left[\bigcup_{i=1}^{n} E_i \cup \bigcup_{k=1}^{r} G_k \right]$$

92

Applying probability as if the terms were mutually exclusive (a good conservative approximation when probabilities are small) we get

$$P\,(B \cup C) = \sum_{g=1}^{m} P(D_g) + \sum_{j=1}^{p} P(F_j) + P(A)\left[\sum_{i=1}^{n} P(E_i) + \mathop{}_{k=1}^{r} P(G_k)\right] =$$

This is equal to the probability $[P(C) + P(D)]$ which would be obtained by combining probabilities through logic gates.

Suppose next that B has the following form:

$$B = \bigcup_{g=1}^{m} D_g \cup A$$

Then all $A \cap G_k$ terms drop out of C and

$$B \cup C = \bigcup_{g=1}^{m} D_g \cup A \cup \bigcup_{j=1}^{p} F_j$$

Applying probability as above we get

$$P(B \cup C) = \sum_{g=1}^{m} P(D_g) + P(A) + \sum_{j=1}^{p} P(F_j).$$

The probability which would be obtained by combining probabilities through logic gates $[P(B) + P(C)]$ is

$$P(B) + P(C) = \sum_{g=1}^{m} P(D_g) + P(A) + \sum_{j=1}^{p} P(F_j) + P(A) \sum_{k=1}^{r} P(G_k)$$

$$P(B) + P(C) = P(B \cup C) + P(A) \sum_{k=1}^{r} P(G_k)$$

therefore,

$$P(B) + P(C) \geq P(B \cup C)$$

Hence, the probability obtained by combining probabilities through logic gates is either correct or conservative for interacting branches which unite at an OR gate.

7.5.5.3 Interacting Branches Unite at an AND Gate

If

$$B = \bigcup_{g=1}^{m} D_g \cup A \cap \bigcup_{i=1}^{n} E_i$$

$$C = \bigcup_{j=1}^{p} F_j \cup A \cap \bigcup_{k=1}^{r} G_k$$

then

$$B \cap C = \bigcup_{g=1}^{m} D_g \cap \bigcup_{j=1}^{p} F_j \cup A \cap \bigcup_{k=1}^{r} G_k \cap \bigcup_{g=1}^{m} D_g$$

$$+ A \cap \bigcup_{i=1}^{n} E_i \cap \bigcup_{j=1}^{p} F_j \cup A \cap \bigcup_{k=1}^{r} G_k \cap \bigcup_{i=1}^{n} E_i.$$

Applying probability assuming mutually exclusive events, we get

$$P(B \cap C) = \sum_{g=1}^{m} P(D_g) \sum_{j=1}^{p} P(F_j) + P(A) \sum_{k=1}^{r} P(G_k) \sum_{g=1}^{m} P(D_g)$$

$$+ P(A) \sum_{i=1}^{n} P(E_i) \sum_{j=1}^{p} P(F_j) + P(A) \sum_{k=1}^{r} P(G_k) \sum_{i=1}^{n} P(E_i).$$

By combining probabilities through logic gates we would get

$$P(B)\ P(C) = \left[\sum_{g=1}^{m} P(D_g) + P(A) \sum_{i=1}^{n} P(E_i)\right] \left[\sum_{j=1}^{p} P(F_j) + P(A) \sum_{k=1}^{r} P(G_k)\right]$$

$$= \sum_{g=1}^{m} P(D_g) \sum_{j=1}^{p} P(F_j) + P(A) \sum_{k=1}^{r} P(G_k) \sum_{g=1}^{m} P(D_g)$$

$$+ P(A) \sum_{i=1}^{n} P(E_i) \sum_{j=1}^{p} P(F_j) + \left[P(A)\right]^2 \sum_{i=1}^{n} P(E_i) \sum_{k=1}^{r} P(G_k)$$

P(B) P(C) and P(B ∩ C) are equivalent except for the last terms.

$$\left[P(A)\right]^2 \sum_{k=1}^{r} P(G_k) \sum_{i=1}^{r} P(F_i) \ll P(A) \sum_{k=1}^{r} P(G_k) \sum_{i=1}^{n} P(E_i)$$

therefore,

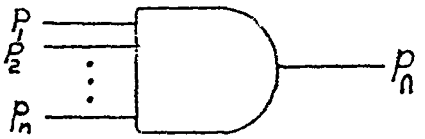
$$P(B)\,P(C) < P(B \cap C)$$

That is, the probability obtained by combining the probabilities of two interacting branches at an AND gate is unconservative.

7.6 Nonrepairable and Short-time System Mode Analysis

7.6.1 During the missile flight or while the system is in a test mode, the effective duration time of a failure (τ) is that length of time which begins with the event of failure and ends at the close of the test mode or end of flight. Since this length of time depends upon the particular event rather than upon a predictable repair time, the method of calculation (λ, τ) applicable to inadvertent launch is not applicable to the faulty launch or test mode analysis. The faulty launch tree is concerned with short-time modes and flight events and a straight-forward probability analysis on a "per launch" basis should be used. Similarly, the portions of a fault tree concerning the system in a test mode or other short-time mode should be treated on a "per test" probability basis.

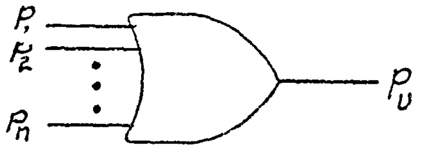
7.6.2 "And" Gates



In general, $P_n = P_1 P_2 \ldots P_n$. Since any requirement for event sequences will tend to reduce the overall probability, the preceding expression is conservative.

Each of the input probabilities must be expressed on the same basis (i.e.: "per test", or "per launch", etc.) and the resultant probability will be in the same units.

7.6.3 "Or" Gates



In general $P_u = P_1 + P_2 + \ldots + P_n$ -- (Probabilities of all combinations). A usefully conservative estimate is $P_u = P_1 + P_2 + \ldots + P_n$ where $P_u \ll 1$.

Each of the input probabilities must be expressed on the same basis (i.e.: "per test", or "per launch", etc.) and the resultant probability will be in the same units.

7.6.4 Conservative Estimates

For either type of gate, decision should be made on an individual basis as to whether to use the preceding, conservative probability expressions or more nearly exact expressions.

7.6.5 In the acquisition of fundamental data, as failure rates, for calculation in a fault tree, events may be characterized by a failure rate (λ) and duration time (τ) or by a probability for a specified time or number of cycles.

For the faulty launch tree which is to be handled on a probability basis, data which is acquired as a failure rate is converted to a probability by multiplying λ by the length of time of the mode where λ is in terms of failures per hour. When λ is given

7.6.5 Continued

in terms of failures per cycle, then λ multiplied by the number of cycles in ~~the~~ mode is the probability of failure.

For the inadvertent launch tree where calculation is done on a (λ , τ) basis, data which is acquired as a probability of failure per cycle or per hour must be incorporated in the mathematical treatment of the tree. Where the cyclical probability of failure for an event is given, an estimated λ in failures per hour may be derived by multiplying the cyclical probability by the estimated number of cycles per hour. τ is determined as the duration time of the failure. Where one event characterized by a probability acts as a moderator (at an "and" gate) of an event characterized by a λ and a τ , the output of the gate may be represented by the product of the input probability and the input failure rate which is interpreted as the output failure rate, and τ output = τ input.

7.7 Final Calculations

7.7.1 System Safety Constants

The system fault trees may be separated into two categories: a system tree(s) dealing with faulty launch and a system tree(s) dealing with inadvertent launch. For the weapon system there is a probability of inadvertent launch during the system life (inadvertent launch safety constant) and a probability of faulty launch during the system use (faulty launch safety constant.) The determination of these constants is the goal of the mathematical treatment of the fault trees.

7.7.2 Squadron Calculations

All calculations in a fault tree should be based upon failures which affect a specific launch facility. For the inadvertent launch tree, the final failure rate (or probability of failure) should then be multiplied by 50 to obtain the applicable failure rate (or probability of failure) for a squadron. For the faulty launch tree, the final failure rate (or probability of failure) is expressed on a "per launch" basis. (Reference)

7.7.3 Inadvertent Launch Safety Constant

The inadvertent launch safety constant, $(S.C.)_{I.L.}$, is composed of contributions both from long-term operating events (characterized by a failure rate λ and duration time $\mathcal{T}$) and from short time test events represented by a probability figure.

Use of the logic gate formulas provides a single failure rate (λ) for inadvertent launch at the top of those tree branches derived from long-term events. To determine the contribution of such a branch to the overall inadvertent launch safety constant for a squadron over any period of time ($\mathcal{T}$), the following formula is used:

$$(S.C.) = 1 - e^{-50\lambda T}$$

which reduces to

$$(S.C.) = 50\lambda T$$

when $50\lambda T$ is small.

Those branches of the tree representing short-time test events provide a single probability of failure for inadvertent launch per branch. Such a probability may be determined either on an event basis or on a time basis. Probabilities on a "per event" basis, when multiplied by the number of events in time $\mathcal{T}$, yield the contribution to inadvertent launch by such branches. If the test event contribution is determined on a time basis rather

7.7.3 Continued

than an event basis, then the probability per hour for a squadron is converted to the squadron probability contribution to inadvertent launch for such branches for time T by the following formula:

$$(S.C.)_T = 1 - \left\{1 - (S.C.)_{1\,hr.}\right\}^T$$

which reduces to:

$$(S.C.)_T = T\,(S.C.)_{1\,hr.}$$

when $T\,(S.C.)_{1\,hr.}$ is small.

The resultant probabilities from the short-time event branches of the tree added to the λ-derived portions of the inadvertent launch safety constant yields the overall $(S.C.)_{I.L.}$ per squadron for the system life.

7.7.4 Faulty Launch Safety Constant

The faulty launch safety constant $(S.C.)_{F.L.}$ is composed of probability contributions from both pre-flight and flight events.

Use of the probability formulas for the flight events of the missile results in a probability of faulty launch per missile which is the faulty launch safety constant contribution due to the flight analysis. Short time events which contribute to faulty launch prior to flight initiation yield a probability contribution to $(S.C.)_{F.L.}$ on a "per event" or "per unit time" basis. Probabilities on a "per event" basis, when multiplied by the number of events prior to launch, form the contribution of such branches to $(S.C.)_{F.L.}$

For test event contributions to $(S.C.)_{F.L.}$ determined on a time basis rather than an event basis, the probability per hour for a missile is converted to the missile probability for any time T by the following formula:

$$(S.C.)_T = 1 - \left\{1 - (S.C.)_{1\,hr.}\right\}^T$$

which reduces to

$$(S.C.)_T = T\,(S.C.)_{1\,hr.}$$

when $T\,(S.C.)_{1\,hr.}$ is small.

The resultant probabilities from the pre-flight events added to the flight event contribution form the overall $(S.C.)_{F.L.}$ per missile for the missile life.

THE BOEING COMPANY

NUMBER D2-30207-1 MODEL NO. WS-133B

TITLE Program Schedule

PREPARED BY R E Harris 3/11/3

SUPERVISED BY 3/11/3

APPROVED BY 3/11/3

APPROVAL 3/13/3

(DATE)

AF04(694)-266
CONTRACT NO.

CHARGE NUMBER

REV B

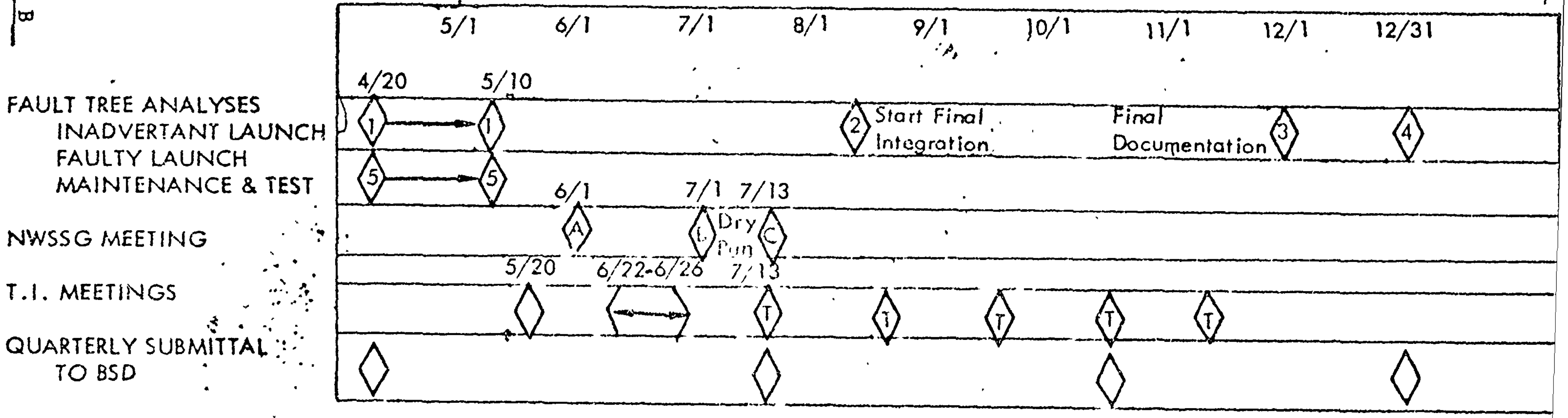
VOL. 1
SEC. 2

NO.
PAGE 1 OF 2

2-5142

SECTION TITLE PAGE U3 4288 0000 REV. 2/61

REV. B



1. A/N submittal of Fault Trees in Boeing format, including LECS, on IL, FL, *Maintenance* and Test, with Backup Data.
2. All Associates - Refined Analysis submitted to Boeing; final form for D2-30207-3with Bibliography and backup data.
3. Completed analysis to Printing, by Boeing.
4. Completed analysis to BSD.
5. Sylvania submittal of updating data on IL and calculations on FL, (IL to include LECS, *Maintenance* & Test) with backup data.

A. Start preparation of presentation for NWSSG Meeting.
B. Refined trees with probabilities completed.
C. Presentation to NWSSG.

* Ⓣ — TENTATIVE

FAULT TREE ANALYSIS
SCHEDULE MILESTONES

THE BOEING COMPANY

NUMBER D2-30207-1 MODEL NO. WS-133B

TITLE Definitions of Terms

PREPARED BY 3-8-63

SUPERVISED BY 3/11/3

APPROVED BY 3/11/3

APPROVAL 3/13

(DATE)

AF04(694)-266

CONTRACT NO.

CHARGE NUMBER

52

B

VOL. 1	NO.
SEC. 3	PAGE 1 OF 3

R

SECTION DOCUMENT (D2-30207-1)

DEFINITIONS OF TERMS

The following is a list of terms and symbols defined for use in this document (D2-30207). It does not necessarily apply to the Bell Telephone Laboratories material reprinted in Sections 4 and 5. R

1. An "Inadvertent Launch" is defined as an unwanted launch (first stage igniticn) of a missile at the tactical site caused by one or more faults. The silo cover is operated to OPEN. The destination or successful firing of succeeding stages is not relevant.

2. A "Faulty Launch" is an authorized launch which malfunctions to result in impact of an armed warhead outside of the area specified in AF BSD 62-123.

3. "Safety" is defined as freedom from the potential or actual occurrence of undesired, unscheduled or out of sequence events which jeopardize life, health or property.

4. A "Safety Item" is a deficiency in the design, procedures or operations which will generate a Hazard.

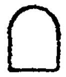
5. A "Hazard" is a condition which will lead to a potential or actual occurrence of undesired or out of sequence events which jeopardize life, health, property, and the international relations of the United States.

6. The "Safety Constant" is the probability for a specified period of time of the occurrence of a defined undesired, unscheduled or out of sequence event which jeopardizes life, health or property.

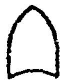
7. A "Fault" is a malfunction within the system. It includes the "Failure" of circuits and equipment to perform due to any cause, excluding human intervention.

8. The "Effective Duration Period" of a failure is the time from the occurrence of a failure to its correction, to shutdown, or to safing of the affected launch facilities or missiles. R

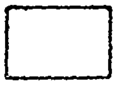
LOGIC SYMBOLS



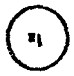
A logical AND relation.



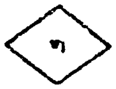
A logical OR relation



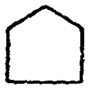
An event, usually a malcondition, describable in functional terms.



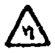
An event, usually a malfunction, describable in terms of a specific circuit or component. It is represented by the symbol X with a numerical subscript.



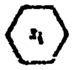
An event not developed further because of lack of information or because of lack of sufficient consequence. It is represented by the symbol W with a numerical subscript.



An event that is normally expected to occur.



A connecting symbol to another part of fault tree within the same major branch. It is represented by the symbol Y with a numerical subscript.



A connecting symbol to another part of fault tree in a different major branch (such as an interconnection between the P/G and DPE branches). It is represented by the symbol Z with a numerical subscript.

δ A probability of failure which, though a numerical value can be assigned, is sufficiently small to be neglected in the context shown.

ϵ A probability of failure which cannot be assigned a numerical value but is considered to be exceedingly small and is assumed to be zero.

THE BOEING COMPANY

NUMBER D2-30207-1 MODEL NO. WS-133B

TITLE Method of Inadvertent Launch Analysis. (Section VII, Vol. I of Bell Telephone Laboratories Launch Control Safety Study - 9-15-62)

PREPARED BY 3-8-63

SUPERVISED BY MLPayne 3/11/3

APPROVED BY 3/11/3

APPROVAL 3/13/3

(DATE)

CONTRACT NO.

CHARGE NUMBER

B

VOL. 1	NO.
SEC. 4	PAGE 1 OF 20

1 INTRODUCTION

1.1 The following pages of this section are a reprint of Section VII of the Bell Telephone Laboratories' Launch Control Safety Study dated September 15, 1962. This reprint describes the fault tree concept and methods for development and construction. Although it was prepared for the WS-133A system, the methods are applicable to the WS-133B system. Its references are to other Sections of the Safety Study which are not included in this document.

1.2 Boeing document page numbers are added to facilitate the handling and release of this section.

Section VII

METHOD OF INADVERTENT-LAUNCH ANALYSIS

1. INTRODUCTION

The task of the study was an examination of a complex data transmission and processing system, called a Launch Control System (LCS), in order to determine its ability to provide safety against an Inadvertent, i.e., accidental, Launch (IL). In particular, it required an identification of those elements of the LCS in which a failure significantly increased the probability of IL.

The "fault tree" concept was devised to carry out this task. The fault tree serves, first of all, to identify the events, usually undesired, that contribute to an IL. It then relates these events, logically, in order to show which events must exist at the same time and which are required on an "either-or" basis.

After fault trees are prepared for the major parts of the LCS, the next step is to determine the probability of occurrence of the significant failures and thence the probability of occurrence of IL in a given time interval. In performing this step, the major contributors to an IL appear. In order to accomplish this step in the analysis, it is desirable to prepare Boolean expressions that are equivalent to the fault tree and which make it possible to take account of multiple appearances of the same failures in the several branches of the tree, as well as the appropriate fault-detection features.

Both of these steps in the IL analysis are described in this section of the report.

2. THE FAULT-TREE CONCEPT

The concept of a fault tree can be illustrated by applying it to a simple and familiar system. Figure 7-1a shows a domestic hot-water system. The problem is to determine its susceptibility to malfunctioning in a catastrophic way — in this case, rupture of the hot-water tank. A fault tree is drawn (Figure 7-1b) that identifies the malfunctions that can contribute to a rupture and that relates these logically. If event B (temperature-measuring device fails to actuate controller), or event C (controller fails to actuate gas valves), or event D (gas valve fails to close) should occur, heat will be applied continuously to the water in the tank. If this happens and event A (relief valve fails to lift) has occurred, the pressure will not be relieved as intended but will continue to rise until the tank eventually ruptures (event F). The Boolean expression for the fault tree is $F = A (B + C + D)$, which states that F

85

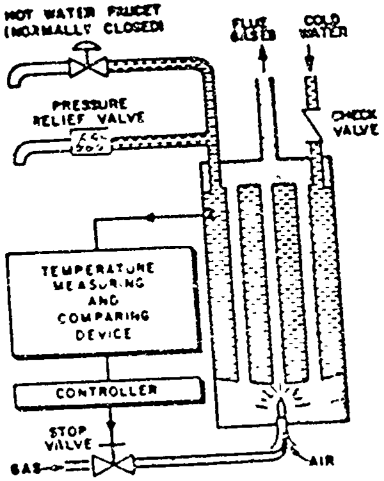
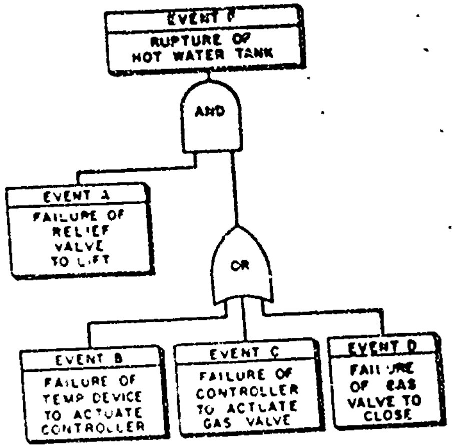


Figure 7-1a. Domestic Hot-Water System


EVENT F
RUPTURE OF HOT WATER TANK
AND
EVENT A
FAILURE OF RELIEF VALVE TO LIFT
OR
EVENT B
FAILURE OF TEMP DEVICE TO ACTUATE CONTROLLER
EVENT C
FAILURE OF CONTROLLER TO ACTUATE GAS VALVE
EVENT D
FAILURE OF GAS VALVE TO CLOSE

BOOLEAN EXPRESSION:

$F = A(B + C + D)$

Figure 7-1b. Fault Tree and Boolean Expression for Hot-Water System

is true if A and (B or C or D) are true. Note that the fault tree assumes that the remainder of the system functions properly so that the check valve and the hot-water faucet do not permit flow out of the tank. The malfunction of either to an open condition would negate event F. The fault tree can be developed further for events A through D in terms of the parts making up the device referred to in each event. If failure rates for the parts were known, the probability of event F occurring in a given period of time could be calculated The calculation would have to account for the fact that, as a practical matter, event F is more likely to occur if event A has occurred prior to event B, C, or D. If B, C, or D occurs and the relief valve works properly, flooding of the basement would provide warning of the malfunction in the gas control loop, which presumably would lead to manual shutdown and repair

3. EXPLANATION OF LAUNCH CONTROL SYSTEM FAULT TREE

The fault tree for the Minuteman LCS is the same in principle as that for the simple system just described, though it is, of course, far more complex. Figure 7-2 summarizes the symbols used in the various fault trees. (Figures 7-2 through 7-6 appear at the end of this section.) The top of the LCS fault tree is shown in Figure 7-3. The fault tree serves, first of all, to identify the events, usually undesired, that contribute to an IL. The fault tree then relates these events logically, using distinctive shape symbols for "AND" and "OR" in relating events. It should be noted that in order for an IL to take place, it is necessary that the required events or malconditions coexist. It is not necessary that the occurrence of these events be simultaneous.

The development of the relation of events proceeds from those describable in functional terms to those that pertain to a specific basic circuit or component or to a specific code group. For instance, in the Launch Enable System (LES) branch, the functional event of having the Safety Control Switch (SCS) armed is the result of any one of three subevents. Two of these are again functional statements that require further tree development, and the other is an event that pertains to a particular component, namely, the failure of a specific relay to the ARM condition. Events of a functional nature are noted in a rectangular box, or, in special cases discussed below, in a hexagon, while events that concern specific circuits or components are shown in a circle.

The fault tree for IL has three major branches. The Programmer Group (P/G) branch includes, as well as the P/G equipment itself, the arm ordnance and ignition circuits to their terminal squibs in or near the missile, and anything else acting directly upon the missile propellant charges, but it excludes the SCS. The second branch of the tree is for the Data Processing Equipment (DPE), the top event of this tree being the operation of the Command Signals Decoder (CSD) switch. The third major branch is for the LES, with the top event here being the arming of the SCS.

In addition to the above, fault trees have been developed for several of the critical electromechanical devices that are used in the LCS, for the formation of code groups, and for the Status Reporting System and power subsystems. Though malfunctions in the Status Reporting System do not contribute directly to IL, they can prevent the detection of malconditions in the in-line equipment, thus permitting them to persist for extended periods of time.

4. DEFINITION OF INADVERTENT LAUNCH

For purposes of the study, IL is defined as an event characterized by ignition of the first stage of the missile. This event may be divided into classes, according to what occurs or does not occur within the Launch Facility (LF) and missile in addition to first-stage ignition. It is useful to define three classes, as follows:

a. In-Silo Explosion

This consists of first-stage ignition and not launcher closure removal.

b. Short Launch

This consists of first-stage ignition and launcher closure removal and not one or more of the other actions essential to a proper launch sequence.

c. Critical Launch

This consists of first-stage ignition and launcher closure removal and all of the other actions essential to a proper LAUNCH sequence.

The different branches of the fault tree are biased in favor of one or another of the classes of IL as defined above. The P/G branch is heavily biased in favor of an In-Silo Explosion, with the probability being less for a Short Launch and much less for a Critical Launch. The DPE branch is biased almost completely in favor of a Critical Launch, since the P/G would be expected to function normally once the CSD switch has operated, assuming the SCS armed, and the normal LAUNCH sequence would occur. The LES branch is not biased one way or the other, SCS ARMED being a necessary condition for any Launch except those generated by the Nozzle Control Units (NCU's) or within the explosive train itself

5. PROGRAMMER GROUP FAULT TREE

Section III of Volume 2 presents the complete development of the fault tree for P/G. This includes, as well as the P/G itself, the ordnance and arming circuits to their terminal squibs in or near the missile, but excludes the SCS. Further, it includes any malconditions that act directly upon the explosive train and propellant of the missile downstream from the ignition squibs. For instance, as shown in

Figure 7-3, if (1) power should be applied to one or more of the NCU's through malfunction of the P/G, and if (2) the heat generated is sufficient to ignite one of the stages, an IL of the In-Silo Explosion class will occur. As a practical matter, it does not matter in this particular case which stage ignites first. In an In-Silo Explosion it can be expected that all stages will be ignited within a short time once any one of them has ignited. It should be noted that the second and third stages of the missile were specifically excluded from the study under the terms of the contract. The NCU's for these stages are included here only because their effects closely parallel those of the first-stage NCU's, and because their relations with the P/G closely parallel those of the first-stage NCU's.

In the fault tree for the P/G, two malconditions must coexist in order to get an output from the fault tree. These are shown in Figure 7-3. The first malcondition is an Ignitor No. 1 or an Ignitor No. 2 firing signal sent by the P/G The second malcondition is an Arm Ordnance signal sent by the P/G or Ignitor Safe and Arm (S&A) device failing armed, or relay K-5 in the S&A module failing closed The last event is shown in a circle in that it is a malfunction describable in terms of a specific component. The Ignitor S&A device failing armed is noted in a hexagon, indicating that a fault tree has been developed separately for this particular electromechanical device. The other events, being describable in functional terms and requiring further development, are shown in rectangles.

The event "Ignitor No. 1 firing signal sent by P/G" will be developed here as an illustration of the fault-tree method. Figure 7-4 is the logic block diagram for the part of the system under consideration. This shows the circuit modules that generate the firing signals to Ignitor No. 1 and Ignitor No. 2 of the first stage. It also shows the final gate in the logic chain that triggers the modules and the contacts of the Launch Enable Switch (LESW) through which the firing signals pass. The fault trees for Ignitor No. 1 and Ignitor No. 2 are identical in form, and that for Ignitor No. 1 only is given in Figure 7-5 Its development is detailed below.

a. An electrical signal to Ignitor No 1 requires both firing of the Squib Driver (an SPS-5) and a path through (or around) the LESW to get the signal to the missile; hence, AND gate A is required.
b. In the left-hand branch, a signal path will exist if either the LESW contact is in the LAUNCH position or if Test Load - Type 2 (TL-2) is shorted; hence, OR gate B is required.
c. LESW contact No. 211 will be in the LAUNCH position if either the individual contact shorts or if the switch is driven to LAUNCH; hence. OR gate C is required.
d. The inadvertent driving of the LESW involves a different set of gates and will not be developed here.

e. In the right-hand branch, an SPS-5 firing signal can be achieved only if both Squib Driver (SD) power is on and the SPS-5 triggered (AND gate D). The SPS-5 is an SD circuit using a Silicon Controlled Rectifier (SCR) as a switch. The SPS-5 driver circuit cannot fail in such a way as to provide squib firing current without driver power being applied. The Driver Power On branch will not be developed here.

f. The SPS-5 either may be self-triggered or may be triggered by receiving a driving signal from the preceding stage (OR gate E).

g. The Power Buffer Amplifier — Type 1 (SA-1) will provide a driving signal to the SD if either it fails so as to produce an output or it receives a driving signal from the preceding stage (OR gate F).

h. Magnetic gate type M-3 (M-3) will produce an output if either the gate malfunctions so as to produce an output or if the correct input conditions are achieved (OR gate G).

i. Both a gate malfunction such as to produce a logical "1" or "true" output from the magnetic core and an INTERLOCK signal to turn on the transistor output amplifier, which is a part of the M-3 module, are required to obtain an output from the circuit module if the correct input conditions are not met (AND gate H). The INTERLOCK signal generation will not be developed here.

j. The input conditions required to yield an output (AND gate I), assuming proper operation of the M-3 module, are:

   1. The presence of an L1 signal (a P/G generated LAUNCH signal) and
   2. The absence of a First-Stage Engine Timer inhibit signal, which is equivalent to saying that a First-Stage Engine Timer signal appears to have been generated, and
   3. The absence of an Ordnance Armed inhibit signal, which is equivalent to saying that the ordnance devices appear to be armed, and
   4. The presence of an INTERLOCK signal to turn on the transistor output amplifier.

The INTERLOCK PRESENT condition is the output of an OR gate, since either a CSD INTERLOCK signal or a TEST INTERLOCK signal will turn on the transistor output amplifier. This is not shown in Figure 7-5 nor is the generation of the other input signals. The complete development will be found in Section III of Volume 2.

6. DATA PROCESSING EQUIPMENT FAULT TREE

The fault tree for the DPE was developed in a manner similar to that described for the P/G. The logic diagrams for the DPE were studied in order to identify and relate in fault-tree form those events that contribute to IL. As shown in Figure 7-3, the top event of the tree is the operation of the CSD switch. This may be caused by

C

R

either of two events, operation by failures internal to the CSD itself, or operation by having the proper code read into the CSD. The latter in turn requires that all of three conditions coexist. First, the proper code must be in the Fire Code (FC) store of LEU No. 2. Second, the FC gate must be enabled, and third, FC shift pulses must be received. Each of these events requires further fault-tree development, which is presented fully in Section IV of Volume 2.

The DPE fault tree shows a number of hexagon symbols, indicating that these events are developed further in additional fault trees. One case is in the operation of the CSD by a failure within the device itself. The seven other cases concern the formation of particular code groups; namely, the 18-bit FC, the "sync" group, and the five Launch Control Center (LCC) addressor codes. Each such event is identified by the symbol Z with a numerical subscript.

7. LAUNCH ENABLE SYSTEM FAULT TREE

The LES was added to the LCS as a part of Block Change No. 1. The purpose was to increase protection against IL and to provide selective control of the firing of individual missiles. It was designed to be a FAIL-ARM system in order not to increase the vulnerability to enemy action of the Minuteman squadron. As a consequence there are many malconditions, any one of which occurring will result in the arming of the SCS, which is the top event of the fault tree for the LES This circumstance is reflected in the predominance of OR gates in the tree.

As shown in Figure 7-3, either of three conditions may cause the top event — arming of the SCS — to occur. These are a failure internal to the SCS, a failure of relay K-2 in the Safe and Arm Module of the Main Junction Box to the open state, or the condition where the output relay in the 3400-cps detector is not closed. The last condition requires further fault-tree development, which is presented fully in Section V of Volume 2. Arming of the SCS by internal failure, shown in a hexagon symbol, is considered in Section XII of Volume 2.

8. SUPPLEMENTARY FAULT TREES

In addition to the three major fault trees described above, there have been fault trees developed in several other areas of special interest as discussed below.

a. Status System Fault Tree. Section VI of Volume 2 develops the fault tree for the Status System. This system is relevant to the IL problem because it informs the operator of the existence of faulty conditions in the DPE and P/G equipment at the LF's. If the Status System fails to provide such indications, the faulty condition, once having occurred, will be allowed to persist for a prolonged period of time.

The status indication of the SCS is a good example of the above point. The operator is provided with an ARMED light at the LCC when the SCS has left the SAFE position, provided that the Status System is functioning properly. If certain particular malfunctions or combinations thereof have occurred in the Status System, as shown on the fault tree for this system, the ARMED light at the console will fail to illuminate so that any one of a number of malfunctions in the LES that results in the arming of the SCS will go undetected for a prolonged period of time.

b. Electromechanical Device Fault Trees. Section XII of Volume 2 contains the fault trees for the critical electromechanical devices that are used in the LCS. These devices are the CSD, SCS, S&A devices, LESW, and the Volatile Decoder of the DPE. Fault trees are developed separately for these devices because of their mechanical aspects and the critical function that they perform in the LCS. The outputs of the fault trees for these devices appear as inputs at appropriate places in the P/G, DPE, and LES fault trees. They are identified by a Z symbol, with a numerical subscript, enclosed in a hexagon.

c. Fault Tree For Code-Group Formation. Section X of Volume 2 uses the fault-tree method in order to identify and relate the conditions necessary for the formation of code groups in the cable plant When modified by the probability of having a particular code group formed, the outputs of such a tree can be used as inputs to the appropriate places in the fault tree for the DPE. Such inputs are also identified by a Z symbol, with a numerical subscript, enclosed in a hexagon.

d. Power Subsystems Fault Tree Though this is developed as a part of the LES fault tree in Section V of Volume 2, it is of interest in other respects as well, such as in preventing an LCF from initiating an INHIBIT message when operating procedures call for it.

9. QUANTITATIVE ANALYSIS OF INADVFRTENT LAUNCH PROBABILITY

Conceivable causes of IL in the LCS were reviewed in Section VI to determine which had the greatest significance. Component part failures were particularly significant, so that the relevant circuits and electromechanical devices which appeared on the fault trees were analyzed to determine insofar as possible their numerical rates of failure. In addition, a group of the causes reviewed were found to be significant in the generation of undesired codes in the cable system. Their effects were also analyzed and the numerical probabilities of occurrence determined for the formation of particular code groups of interest. It now remains to apply the results of these analyses to the fault trees in order to evaluate quantitatively the susceptibility of various parts of the LCS to IL. Before this task becomes manageable, there are several factors to be considered.

a. Factors To Be Considered

(1) Simplification. The first factor is that the fault tree can be simplified immediately to some extent by disregarding two types of malconditions. The first is a malcondition that has a probability of occurrence which, though a numerical value can be assigned, is sufficiently small to be neglected in the context in which it appears. The symbol δ denotes this value of probability. For example, if there are three inputs to an OR gate and the probability of one of these inputs being true is very small compared to the probabilities of the other two inputs being true, then it is a valid simplification to ignore the first input. The second type of malcondition that permits simplification of the fault tree is one that has a probability of failure which cannot be assigned an exact value but which is judged to be exceedingly small so that it can be assumed to be zero. The symbol ϵ is used to denote this value of probability. For instance, if there are three inputs to a given AND gate, one of which has a probability of ϵ of becoming true, then the output of this gate can be considered as having a probability of ϵ of becoming true, and the entire branch up to and including the AND can be ignored.

(2) Interconnections. The second factor that must be considered is that there are interconnections that appear in intermediate areas of some of the fault trees. An example of this appears in Figure 7-6, which shows a simplified fault tree for the P/G in the STRATEGIC ALERT mode. The basic events in this tree have been designated with the letters A through H in order to permit a description here of the principles involved in manipulating fault trees. In the left branch of this tree there are two intermediate events developed, Y_1 and Y_2. (Y_1 is the input to the top gate from the left branch, but it appears as well at three places in the middle branch of the tree and at one place in the right branch; Y_2 appears once in the middle branch and once in the right branch.) Given the probabilities of the basic events A through H occurring, the problem is to calculate the probability of the output of Gate No. 1 being true, taking into account the cross-connections represented by Y_1 and Y_2.

(3) Fault-Detection Features of LCS. The third factor that must be considered is the effect of the various fault-detection features within the LCS. Such features include the status indications, the Alarm and No-Go indications, and the automatic shutdown provisions, for the various modes of operation such as STRATEGIC ALERT, TEST, and CALIBRATE. The fault-detection features must be taken into account in estimating the probabilities of IL because of their effects on the expected duration of the in-line malconditions that they sense.

The characteristics of the fault-detection features that are of particular interest are:

(a) Frequency of Operation. Some fault-detection features, such as the ARMED status indication and the Critical Error (CE) circuitry of the DPE, operate

R

continuously. A fault should be noted immediately upon occurrence. Other fault-detection features operate only at discrete times, such as during a Sensitive Command Network Test (SCNT) or a TEST.

(b) Effect of Detecting a Fault. Information on some faults is displayed on the LCC, while information on others is registered with the Voice Reporting Signal Assembly (VRSA), with only a gross FAULT indication showing at the LCC. Selected faults, such as CE's in the DPE, have an additional effect in producing a No-Go condition at the LF.

(c) Reliability of Fault Detection Path. If a failure should occur in the fault-detection path, then the duration of the in-line malfunction will be extended, perhaps indefinitely.

b. Boolean Expressions

In order to accommodate the factors listed above, it is very useful to develop a Boolean expression that describes the fault tree. Through proper algebraic manipulation, multiple connections drop out and the fault-tree output can be expressed in terms of the basic malconditions. Moreover, the terms of the final expression can be grouped in whatever manner is most convenient to allow for fault-detection features.

Before proceeding further it may be useful to discuss Boolean algebra briefly This algebra was first conceived by George Boole and presented in his book entitled, "An Investigation of the Laws of Thought," published in London in 1854. (Boolean algebra is related to symbolic logic, algebra of classes, calculus of propositions, algebra of logic, and switching algebra.) Unlike ordinary algebra, Boolean algebra deals with variables that are permitted to assume only two different values Depending on the type of problem being treated, a Boolean variable might have the values: on or off, good or bad, something or nothing, true or false, yes or no, open or closed, present or absent, etc. For a generalized mathematical approach, it is convenient to assign 0 and 1 as the two possible values of the variable and, in turn, to let the 0 and 1 represent the two possibilities of a particular problem. In the case of the fault tree, 0 represents false and 1 represents true, with respect to a given malcondition that appears in the fault tree.

The basic operations most commonly used in Boolean algebra are a special form of negation, a special form of addition, and a special form of multiplication. The special form of negation used is symbolized with an overline, as $\bar{a}$, or with a prime, as a', and may be read as "not a" or as "a prime." Functionally, the operation may be written as NOT (a) = a'. Since only two variable values are permissible, if a = 1, then a' = 0, and if a = 0, then a' = 1.

The special form of addition employed is symbolized by a plus sign, as a + b, and may be read as "a plus b." The expression signifies a "mixing" or "inclusive OR" process and is also read as "a OR b." Functionally, OR (a, b) = a + b.

The special form of multiplication used is symbolized like a product in ordinary algebra, as a · b, a(b), a x b, or simply ab. It may be read as "a times b" or just "ab." The product indicates a "coincidence" or "ANDing" process, and it is also read as "a AND b." Functionally, AND (a, b) = ab. Unlike a product in ordinary algebra, ab = 1 if, and only if, both a = 1 and b = 1.

Table 7-1 shows some of the fundamental identities of Boolean algebra that are relevant to the remainder of this discussion.

A typical example of the development of a Boolean expression for a fault tree will now be described. Figure 7-6 shows the simplified fault tree for a part of the P/G in the STRATEGIC ALERT mode. The numbers within the logic gates denote the output variable of that gate in the Boolean expressions. The letters A through H denote basic events, usually malconditions describable in terms of a specific circuit or component. The symbols Y_1 and Y_2 are intermediate events that appear at more

Table 7-1

FUNDAMENTAL IDENTITIES OF BOOLEAN ALGEBRA

Title	Identity
Elementary Propositions	a + a' = 1
	aa' = 0
	a + 1 = 1
	a · 1 = a
	a + a = a
	aa = a
	a'' = a
Associative Law	(a + b) + c = a + (b + c)
	(ab)c = a(bc)
Commutative Law	a + b = b + a
	ab = ba
Distributive Law	a(b + c) = ab + ac
	a + bc = (a + b)(a + c)

than one place in the fault tree. The outputs of Gates Nos. 1, 2, 4, and 10 have been described in terms of system functions in order to indicate briefly the relation of the fault tree to the physical system. An expression for the output of Gate No. 1 in terms of the basic events A through H will now be developed.

Starting at the bottom of the left branch

$$(14) = C + D$$

For convenience let

$$(14) = Y_2 = C + D$$
$$(13) = Y_2 + E = C + D + E$$
$$(12) = B + C$$
$$(11) = (12) \cdot (13)$$

Substituting

$$(11) = (B + C)\,(C + D + E)$$

Distributing

$$(11) = BC + BD + BE + CC + CD + CE$$

From the elementary propositions of Boolean algebra

$$C \cdot C = C = C \cdot 1$$

Grouping, commutating, and distributing

$$C \cdot 1 + CB + CD + CE = C\,(1 + B + D + E) = C$$

Substituting and distributing

$$(11) = C + B(D + E)$$
$$(10) = A + (11) = A + C + B(D + E)$$

For convenience let

$$(10) = Y_1 = A + C + B(D + E)$$

Going to the middle branch

$$(9) = Y_1 + Y_2$$
$$(8) = G \cdot (9) = G(Y_1 + Y_2)$$
$$(7) = F \cdot (9) = F(Y_1 + Y_2)$$
$$(6) = Y_1 \cdot (8) = Y_1 G(Y_1 + Y_2)$$

Commutating and distributing

$$(6) = GY_1Y_1 + GY_1Y_2$$

As before

$$Y_1 \cdot Y_1 = Y_1 = Y_1 \cdot 1$$

Substituting and distributing

$$(6) = GY_1 \cdot 1 + GY_1Y_2$$
$$= GY_1(1 + Y_2)$$
$$= GY_1$$

Similarly

$$(5) = Y_1 \cdot (7) = Y_1F(Y_1 + Y_2)$$
$$= FY_1$$
$$(4) = (5) + (6)$$
$$= FY_1 + GY_1$$
$$= Y_1(F + G)$$

Going to the right branch

$$(3) = Y_1 + Y_2$$
$$(2) = H \cdot (3) = H(Y_1 + Y_2)$$

Bringing the three branches together

$$(1) = (10) \cdot (4) \cdot (2)$$
$$= Y_1Y_2(F + G)\, H(Y_1 + Y_2)$$

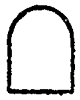
Reducing in the same manner as for function (6) above

$$(1) = H(F + G)\, Y_1$$

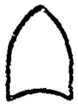
Substituting

$$(1) = H[\, F + G\,][\, A + C + B(D + E)\,]$$

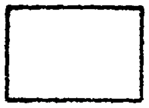
Thus, the output of the simplified fault tree used in this example can be expressed entirely as a function of the basic events. All basic events appear in the expression, and each appears only once. This permits a quantitative estimate of the probability of occurrence of the top event in the fault tree (i.e., the output of Gate No. 1 in Figure 7-6), if the probabilities of occurrence of the basic events are known. The next section will discuss these probabilities for significant elements in the IL fault trees.



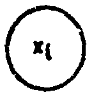
A logical AND relation.



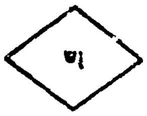
A logical OR relation



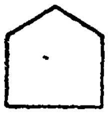
An event, usually a malcendition, describable in functional terms.



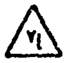
An event, usually a malfunction, describable in terms of a specific circuit or component. It is represented by the symbol X with a numerical subscript.



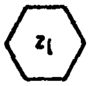
An event not developed further because of lack of information or because of lack of sufficient consequence. It is represented by the symbol W with a numerical subscript.



An event that is normally expected to occur.



A connecting symbol to another part of fault tree within the same major branch. It is represented by the symbol Y with a numerical subscript.



A connecting symbol to another part of fault tree in a different major branch (such as an interconnection between the P/G and DPE branches). It is represented by the symbol Z with a numerical subscript.

δ A probability of failure which, though a numerical value can be assigned, is sufficiently small to be neglected in the context shown.

ϵ A probability of failure which cannot be assigned a numerical value but is considered to be exceedingly small and is assumed to be zero.

Figure 7-2. Fault-Tree Symbols

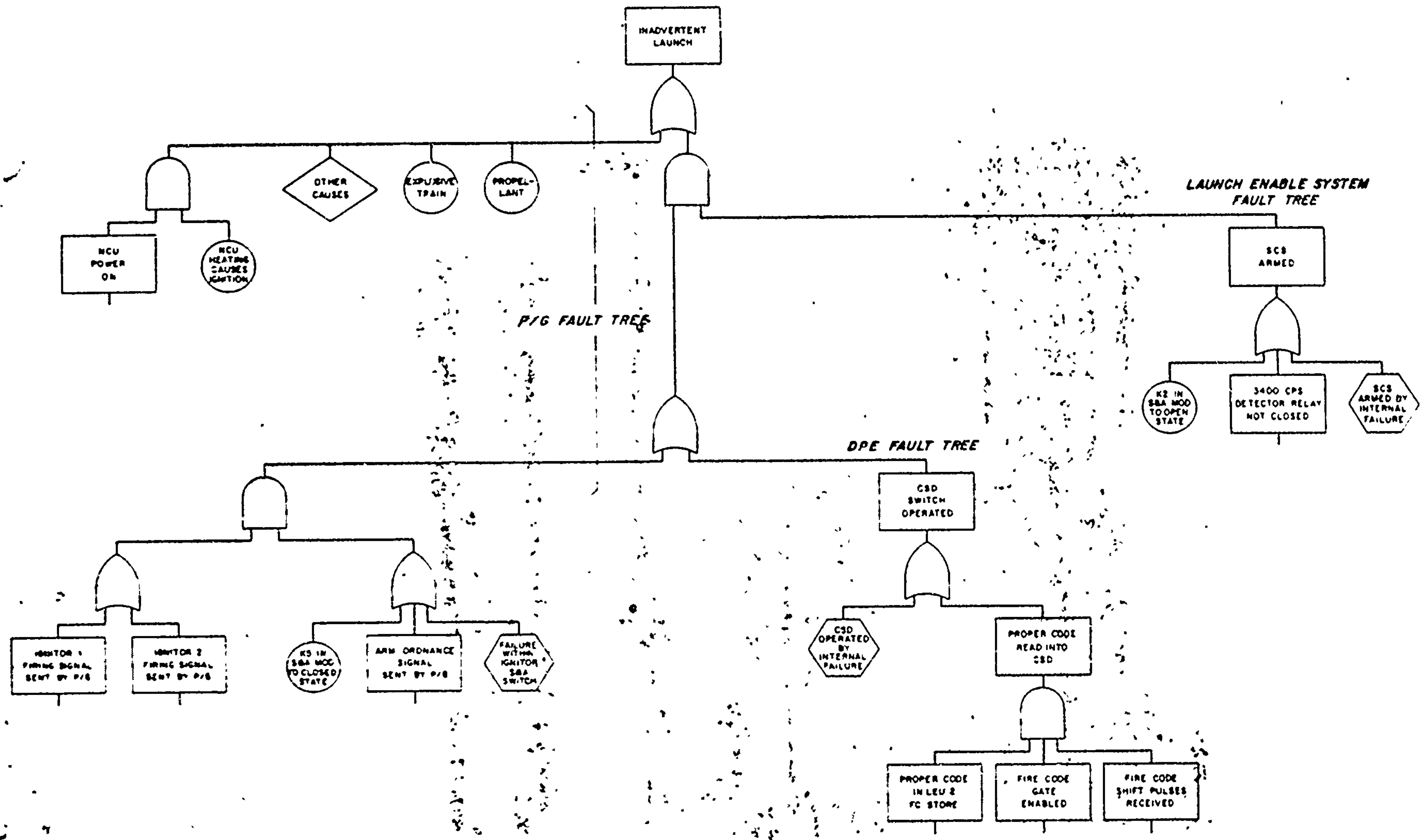
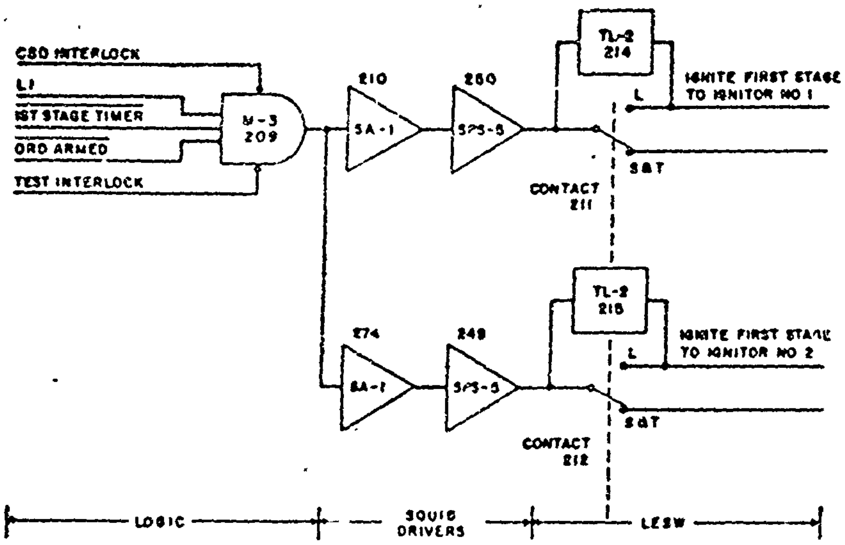

INADVERTENT LAUNCH
NCU POWER ON
NCU HEATING CAUSES IGNITION
OTHER CAUSES
EXPLOSIVE TRAIN
PROPEL-LANT
LAUNCH ENABLE SYSTEM FAULT TREE
SCS ARMED
K2 IN S&A MOD TO OPEN STATE
3400 CPS DETECTOR RELAY NOT CLOSED
SCS ARMED BY INTERNAL FAILURE
P/G FAULT TREE
DPE FAULT TREE
CSD SWITCH OPERATED
CSD OPERATED BY INTERNAL FAILURE
PROPER CODE READ INTO CSD
PROPER CODE IN LEU 2 FC STORE
FIRE CODE GATE ENABLED
FIRE CODE SHIFT PULSES RECEIVED
IGNITOR 1 FIRING SIGNAL SENT BY P/G
IGNITOR 2 FIRING SIGNAL SENT BY P/G
K3 IN S&A MOD TO CLOSED STATE
ARM ORDNANCE SIGNAL SENT BY P/G
FAILURE WITHIN IGNITOR S&A SWITCH

Figure 7-3. LCS Fault-Tree Development



TRIGGER SIGNAL FROM GATE 209 = (L1) •(1ST STAGE TIMER)•
(ORD ARMED)•(INTERLOCK)

Figure 7-4. Typical Example of Logic Block Diagram, P/G

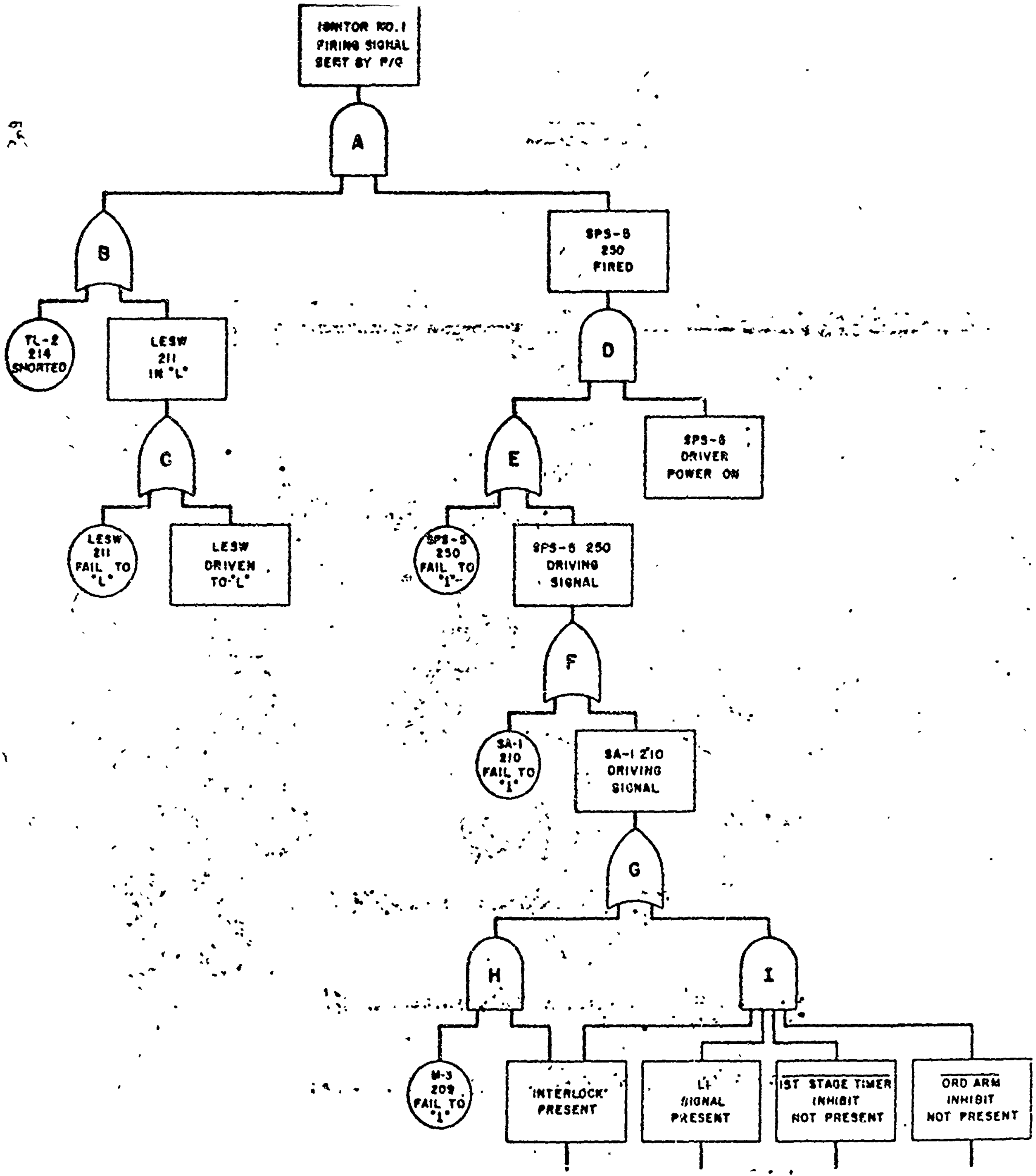
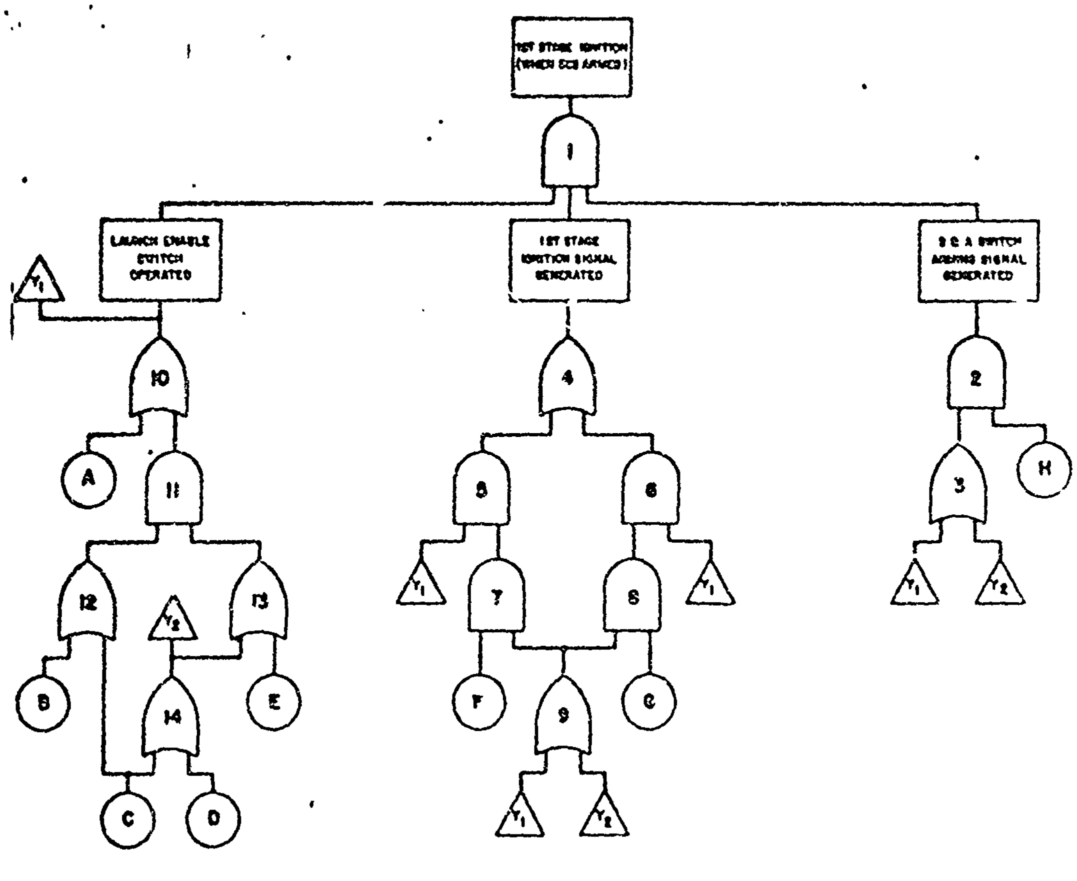


Figure 7-5. Typical Example of Fault Tree, P/G



1ST STAGE IGNITION (WHEN SCS ARMED)
1
LAUNCH ENABLE SWITCH OPERATED
1ST STAGE IGNITION SIGNAL GENERATED
S C A SWITCH ARMING SIGNAL GENERATED
Y_1
10
4
2
A
11
5
6
3
H
12
Y_2
13
Y_1
7
8
Y_1
Y_1
Y_2
B
14
E
F
9
G
C
D
Y_1
Y_2

Figure 7-6. A Simplified P/G Fault Tree (STRATEGIC ALERT Mode)

THE BOEING COMPANY

NUMBER D2-30207-1 MODEL NO. WS-133B

TITLE Discussion of Probabilities and their Combination (Section II, Vol. II of Bell Telephone Laboratories Launch Control Safety Study - 9-15-62)

PREPARED BY C R Eckberg 3/8/63

SUPERVISED BY 3/11/3

APPROVED BY 3/11/3

APPROVAL M C Nichols 3/12/3

(DATE)

CONTRACT NO.

CHARGE NUMBER

B

VOL. 1
SEC. 5

NO.
PAGE 1 OF 18

1. INTRODUCTION

1.1 The following pages of this section are reprinted from Section II Volume II of the Bell Telephone Laboratories' Launch Control Safety Study dated September 15, 1962. It contains significant mathematical analysis applicable to probability computations.

1.2 Boeing document page numbers are added to facilitate the handling and release of this section.

Section II

DISCUSSION OF PROBABILITIES AND THEIR COMBINATION

The theory of probability forms the basis for the quantitative aspects of this study, and this section documents the manner in which probability theory was applied. It is intended to be neither a philosophical treatise nor a rigorous mathematical treatment, but rather a self-contained account of the basic probability rules and procedures employed in the program.

Before giving consideration to the development of these rules, some cautionary remarks are in order regarding the application of probability theory to a real problem, and the interpretation of the numbers resulting therefrom. Like all mathematical disciplines, the theory of probability is developed in relation to specific, abstract, conceptual models, and the formulas derived apply with exactness only to those models. In applying the theory to the real world, even a most carefully formulated model may not be a wholly adequate representation of the real situation. The degree of confidence in the results must then be tempered by objective estimation of the disparity between model and reality. Because, however, the formulas may be applied mechanically, and the results of a probability analysis, even a poor one, are usually expressed as definite numbers, there is a strong tendency to place implicit faith in the numbers once they are generated, forgetting their shaky foundations. Thus, for example, the simple exponential failure model is used for component failure almost universally in the study. While this model is believed to be a good description of device failure behavior, it is surely not a complete one. Burn-in and wear-out failures are not included, this simplifying omission being justified by the inception time and duration of the operation period. In other parts of the analysis, probabilities may be combined in a manner that is valid only for events that are "exhaustive and exclusive." While attempts are made to insure that the proper conditions apply to the problem at hand, in the actual combinations some overlapping may be present that will impair somewhat the validity of results. Moreover, mathematical approximations are made for convenience throughout the work. This should not affect the more significant figures in the computations, but it will have a minor impact on the results. It must be emphasized that the probability figures generated in this study are not sacred (they are not necessarily accurate to the two significant figures in which they are expressed). At the same time, one must recognize their utility in pinpointing critical areas. It should also be emphasized that meticulous care must be taken in stating a probabilistic problem and in formulating the mathematical model so as to minimize errors in the derived results.

1. AN INTERPRETATION OF PROBABILITY FIGURES

In connection with the problem of interpreting probability figures, it may be useful to discuss an implicit meaning of a given numerical probability value. To illustrate, consider the operation of the random code model discussed in paragraph 2 of Section X. This model is not representative of actual system behavior but is, rather, an artificial invention developed to help estimate a lower bound of system performance. It assumes that an arbitrary sequence of 1's and 0's is continuously being generated at the bit rate. The probability that a bit is a 0 is 0.5. Under this condition, and assuming each new bit initiates an independent message, the model generates a 56-bit code with probability of 5.6×10^{-5} for a Flight of ten Launch Facilities (LF's) in ten years.

It is difficult to comprehend the magnitude of this number, let alone its significance in context. To make both aspects more meaningful, the following proposition in probability theory is used: "If an event A has probability p of occurring in a single trial, the most likely number of occurrences of A in n trials is np." Using this proposition, the illustrative probability figure can be translated to other terms as follows:

Let a trial for code generation constitute exposure of ten LF's to the random model environment for ten years. Then, for example, ten trials would mean any one of the following exposures: 100 LF's for 10 years, or 10 LF's for 100 years, or 25 LF's for 40 years, or any other ten-fold scaling of the product of LF-years.

Now it can be seen that the above proposition applied to the probability in the example implies that the most liekly number of occurrences of code generation will be one launch code when

$$np = 1 \text{ or } n = \frac{1}{p} \cong 2 \times 10^4 \text{ trials}$$

Thus, the probability is equivalent to stating that the most probable time to a single code generation for a Flight of ten LF's will be 2×10^5 years; or, alternatively, the expected number of codes will be one in 2×10^5 years. (If it is assumed that a Poisson probability model applies, the probability associated with this single code generation in 2×10^5 years can be shown to be $1/e = 0.37$, but it drops off quickly to near-zero values in the realistic future, diminishing to 5.6×10^{-5} in ten years.)

The above is one of several possible interpretations which may help give a probability value some significance related to experience.

2. BACKGROUND PREPARATORY TO COMBINING PROBABILITIES IN FAULT TREES

a. Basic Considerations

This section is devoted to developing the background required for deriving the relations expressing overall probabilities, given the probabilities of component events and the manner in which they are related logically as prescribed by the fault tree. The basic mathematical doctrine drawn upon here is the set of rules governing combinations of independent events. (Independent events are those for which the occurrence of one does not influence the occurrence of another.) The qualification "independent" is imposed not only because of the resulting simplification but also because the Boolean version of the fault tree contains only events that may be regarded as independent, as will be shown below.

For combining probabilities of two independent events A and B, the basic rules as given by probability theory are:

1. The probability of the occurrence of both A and B, written in set symbology $P(A \cap B)$, is

$$P(A \cap B) = P(A) \cdot P(B)$$

2. The probability of the occurrence of either A or B or both, written $P(A \cup B)$, is

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

In this case, since A and B are independent, rule 1 is used to obtain

$$P(A \cup B) = P(A) + P(B) - P(A) \cdot P(B)$$

and note that if both $P(A)$ and $P(B)$ are small,

$$P(A \cup B) \cong P(A) + P(B)$$

This approximate result is used throughout the subsequent development and in all computations.

b. Composite Probability from Fault Tree and Boolean Expression

Turn now briefly to the format of the fault tree for an illustration of the application of the probability rules thereto and the reason for introducing the Boolean concept. Figure 2-1 shows a typical portion of a tree. The labels on the tree are Boolean functions which take on the value 1 when the failures or malfunctions exist and the value 0 otherwise. The tree shows that the joint occurrence of events A and B $(A \cap B)$ constitutes event C which together with D either singly or jointly $(C \cup D)$ produces the event E. Thus

$$E = (C \cup D) = (A \cap B) \cup D$$

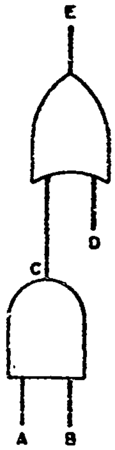


Figure 2-1. Portion of Typical Fault Tree

(Strictly speaking, E is not identical to the event $[(A \cap B) \cup D]$, but rather E is implied by, or always occurs with, the indicated composite event.)

Another way to express E is in Boolean terms:

$$E = A \cdot B + D$$

The probability of E may be found from either of the above relationships. Using the first, together with rules 1 and 2,

$$\begin{aligned} P(E) &= P[(A \cap B) \cup D] \\ &= P(A \cap B) + P(D) \\ &= P(A) \cdot P(B) + P(D) \end{aligned}$$

P(E) also follows directly from the Boolean expression and suggests that a simple, unifying approach to fault probability determination may be to write the Boolean expression for the occurrence of an event and then convert it to a probability relation. This approach also has the virtue of avoiding possible errors due to common events (a form of dependency), as illustrated by the following example:

In Figure 2-2a, B is an event which renders D and E mutually dependent. Ignoring this fact and mechanically applying the rules yields

$$P(F) = P(D) + P(E) = P(A) \cdot P(B) + P(B) + P(C)$$

If, however, the Boolean representation is used,

$$\begin{aligned} F &= A \cdot B + (B + C) \\ &= AB + B + C \\ &= B(A + 1) + C \\ &= B + C \end{aligned}$$

thus

$$P(F) = P(B) + P(C)$$

This differs markedly from the first expression. The latter is the correct result, and it is portrayed in the Boolean tree of Figure 2-2b. In this form, all events are independent. (Note that the use of set relationships could also yield a correct result, but this approach is more unwieldy and difficult to apply to complex cases.) It is now evident that the Boolean approach is a simple technique which handles the problem of dependent events (of the type caused by a common element) by yielding an equivalent format wherein all events are independent.

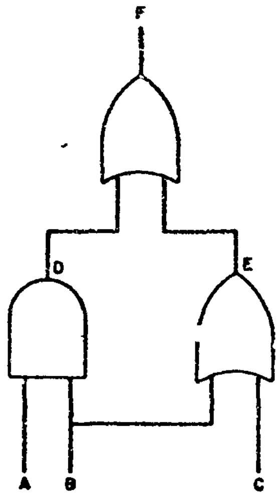


Figure 2-2a. Portion of Fault Tree with Dependent Events

c. Reliability Function

Before proceeding to the development of actual composite event probabilities, it is necessary to introduce yet another fundamental relationship — the reliability function used extensively throughout the fault-tree computations. Because of its importance and the degree to which it is called upon in the subsequent development, an extended if nonrigorous discussion of the reliability function, its complement, and its associated density functions is presented.

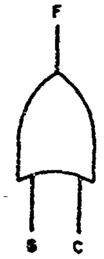


Figure 2-2b. Boolean Equivalent of Figure 2-2a

(1) Device Reliability. Suppose a large set of N_0 identical (with respect to manufacture) devices is subjected to life test, after having eliminated "burn-in" or early-life failures of the substandard members. At time t, $N_F(t)$ devices have failed and $N_S(t)$ survive. Then the reliability of the device, R(t), may be defined as the probability of a member's survival to time t and would be given empirically by the ratio of surviving to original members as a function of time, averaged over many such life tests.

$$\begin{aligned} R(t) &= \frac{N_S(t)}{N_0} \\ &= \frac{N_0 - N_F(t)}{N_0} \\ &= 1 - \frac{N_F(t)}{N_0} \end{aligned}$$

Although $N_F(t)$, and consequently R(t), take on only discrete values, it may be assumed that continuous functions approximate them, and then

$$\frac{d\,R(t)}{dt} = -\frac{1}{N_0} \cdot \frac{d\,N_F(t)}{dt}$$

or

$$\frac{d\,N_F(t)}{dt} = -N_0 \frac{d\,R(t)}{dt}$$

Now $d\,N_F(t)/dt$ is the failure rate at time t, while $\left[d\,N_F(t)/dt\right] dt$ is the number of failures in the interval (t, t + dt). On dividing $d\,N_F(t)/dt$ by $N_S(t)$, the failure rate per surviving member is obtained, which is called the hazard function, h(t).

$$h(t) = \frac{1}{N_S(t)} \frac{d\,N_F(t)}{dt}$$

The hazard function h(t) is in the nature of a conditional probability density of time-to-failure, because

$$h(t)\ dt = \frac{d\ N_F(t)}{N_S(t)}$$

is the fraction of surviving members at the start of an interval (time t) which fail in the interval (t, t + dt).

(2) Failure Density Function. If d $N_F(t)$ /dt is divided by N_0 instead of by $N_S(t)$, the failure rate per original member, designated f(t), is obtained as

$$f(t) = \frac{1}{N_0} \cdot \frac{d\ N_F(t)}{dt}$$

This failure rate f(t) is also a probability density function of time-to-failure, since

$$f(t)\ dt = \frac{d\ N_F(t)}{N_0}$$

represents the fraction of original members that fail in the interval (t, t + dt).

Some useful reliability relationships can be derived from these definitions. Starting with h(t):

$$h(t) = \frac{1}{N_S(t)} \cdot \frac{d\ N_F(t)}{dt}$$

$$= -\frac{N_0}{N_S(t)} \cdot \frac{d\ R(t)}{dt}$$

$$= -\frac{1}{R(t)} \cdot \frac{d\ R(t)}{dt}$$

or

$$h(t)\ dt = -\frac{d\ R(t)}{R(t)}$$

Integrating,

$$\int_0^t h(t)\ dt = -\ln R(t) + k$$

Since

$$R(0) = \frac{N_S(0)}{N_0} = 1$$

then k = 0, and

$$R(t) = e^{-\int_0^t h(t)\,dt}$$

If h(t) is assumed to be constant, a condition closely ~~r~~ealized in life testing experience, and $h(t) = \lambda$ is called simply the failure rate, the $R(t) = e^{-\lambda t}$ is the reliability function giving the probability of member survival to time t. (It is assumed that the device is not operated long enough to exceed the constant λ range.)

The probability that the device will have failed by time t is the complementary function Q(t), where

$$\begin{aligned} Q(t) &= 1 - R(t) \\ &= 1 - e^{-\lambda t} \end{aligned}$$

This is the expression used to evaluate the fault-tree "circles" (basic circuit failures). To illustrate its use, suppose that a device failure rate λ = 250 failures per 10^9 hours, and t = 30,000 hours. Then

$$\begin{aligned} Q &= 1 - e^{-\lambda t} \\ &= 1 - 1 + \lambda t - \frac{1}{2}\lambda^2 t^2 + \ldots \\ &\cong \lambda t \end{aligned}$$

if higher order terms may be neglected (the usual situation in this study).

$$\therefore\ Q = \frac{250}{10^9} \times 30{,}000 = 0.0075$$

An interpretation of this result (as indicated in paragraph 1) is that if 10,000 such circuits were run for 30,000 hours each, about 75 failures could be expected among them.

Returning now to f(t),

$$f(t) = \frac{1}{N_0}\frac{d\,N_F(t)}{dt}$$

$$\begin{aligned} \therefore\ f(t) &= -\frac{d\,R(t)}{dt} \\ &= -\frac{d}{dt}e^{-\lambda t} \\ &= \lambda e^{-\lambda t} \end{aligned}$$

On integrating f(t),

$$\begin{aligned}
\int_0^\infty f(t)\,dt &= \int_0^t f(t)\,dt + \int_t^\infty f(t)\,dt \\
&= -e^{-\lambda t}\Big|_0^t + \left[-e^{-\lambda t}\right]\Big|_t^\infty \\
&= (1 - e^{-\lambda t}) + e^{-\lambda t} \\
&= Q(t) + R(t) \\
&= 1
\end{aligned}$$

The preceding states that Q(t), the probability of failure by time t, may be found by integrating the density function from 0 to t; the graphical significance is shown in Figure 2-3a.

To obtain the probability of failure in some crucial interval subsequent to 0, say (t_1, t_2), f(t) must be integrated over that interval:

$$\begin{aligned}
Q(t_1, t_2) &= \int_{t_1}^{t_2} f(t)\,dt \\
&= \int_{t_1}^{t_2} \lambda e^{-\lambda t}\,dt \\
&= -e^{-\lambda t}\Big|_{t_1}^{t_2} \\
&= e^{-\lambda t_1} - e^{-\lambda t_2} \\
&= e^{-\lambda t_1} - e^{-\lambda (t_1 + \tau)} \\
&= e^{-\lambda t_1}\left[1 - e^{-\lambda \tau}\right] \\
Q(t_1, t_2) &= R(t_1) \cdot Q(\tau)
\end{aligned}$$

where

$$\tau = t_2 - t_1$$

This result states that the failure probability in an interval of length τ starting at t_1 is equal to the probability that the device has survived to time t_1, multiplied by the probability of failure in an interval of length τ which starts at 0. The graphical interpretation of $Q(t_1, t_2)$ is shown in Figure 2-3b.

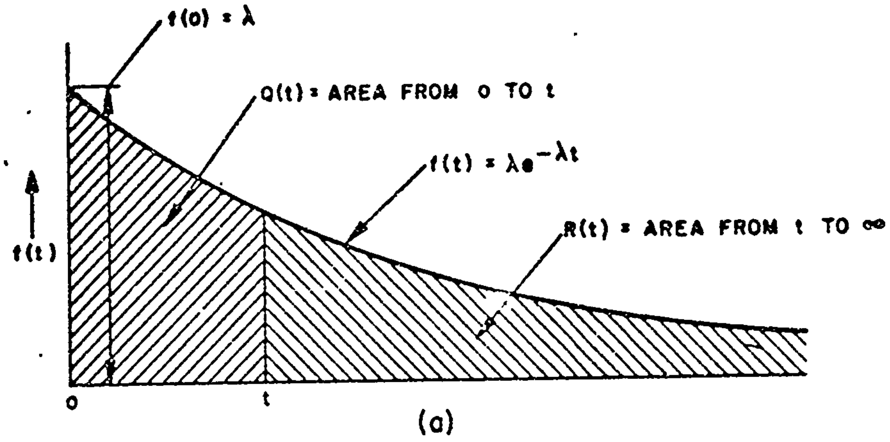


Figure 2-3a. Graphical Significance of Q(t) and R(t)

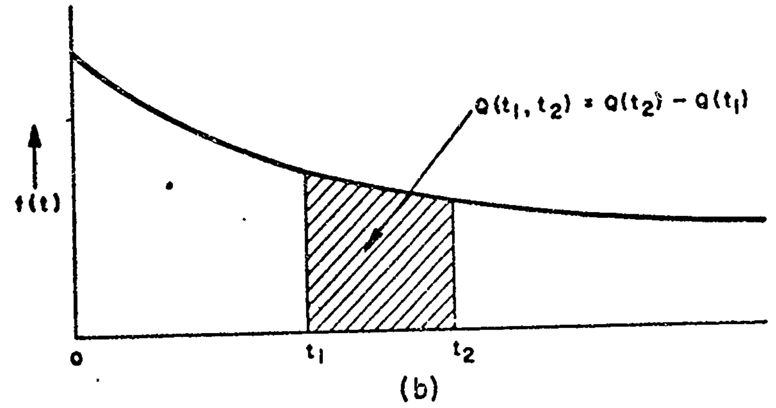


Figure 2-3b. Graphical Significance of $Q(t_1, t_2)$

One additional fact is drawn from f(t). Since f(t) is a probability density of time-to-failure (which is to say that there is a time distribution of failure probability densities), it is in order to inquire which value of t is the mean of this distribution. The answer is found by "weighting" each value of t with its associated density and integrating over all t:

$$m_t = \int_0^\infty t \cdot f(t)\, dt$$

$$= \int_0^\infty t\lambda\, e^{-\lambda t}\, dt$$

$$= e^{-\lambda t}\left(t + \frac{1}{\lambda}\right)\Big|_0^\infty = \frac{1}{\lambda}$$

Thus, for the constant hazard function,

$$m_t = \frac{1}{\lambda}$$

That is, the mean-time-between-failure (MTBF) is the reciprocal of the failure rate.

In the following work, m and $1/\lambda$ are used interchangeably as convenience dictates.

3. COMPOSITE FAILURE PROBABILITY UNDER SPECIFIC CONDITIONS

With the background of paragraph 2, the main objective of this section may be undertaken — the derivation of relationships for composite probability of failure under specific conditions prescribed by the fault trees. (Note that rules are not developed here for determining circuit failure from probabilities of component failure. This aspect is dealt with in Sections VII and VIII.)

In the following discussion the fault detection feature associated with some events is at once the significant element in the composite event and the complicating part of the analysis. Fault detection enters the analysis by prescribing a necessary sequence or order of failures if the composite event is to occur. It enters the physical system through the alarm and status features, as well as through test modes.

One starts with two events, A and B, which are independent failure conditions having constant failure rates λ_A, λ_B or, alternatively, MTBF's m_A, m_B, respectively. The composite event of interest is the combination of A and B in an AND Gate under various conditions, resulting in event F. (In Boolean terms, $F = A \cdot B$.) Required is the probability P(F) that F occurs under the following different circumstances:

CASE I. Neither A nor B is subject to detection throughout the entire operation period T_0.

Solution: This is the case that applies to the bulk of the computations. Since A and B are independent,

$$\begin{aligned} P(F) &= P(A) \cdot P(B) \\ &= \left(1 - e^{-\lambda_A T_0}\right)\left(1 - e^{-\lambda_B T_0}\right) \\ &\cong \lambda_A T_0 \, \lambda_B T_0 \\ &= \frac{T_0^2}{m_A m_B} \end{aligned}$$

CASE II. Condition A triggers a detection alarm and is corrected immediately on occurrence. B is not subject to detection.

Solution: Under the given hypothesis, the only way for F to occur is to have B precede A, since if A precedes B, A is always corrected and the two events can never coexist (neglecting precisely simultaneous failures). An implicit order condition is thus imposed by the detection feature.

First express the probability that B occurs in the differential interval dt which starts at t and is followed by the occurrence of A in the interval (t, T_0), given that A has not occurred up to t:

$$P\left[B(dt)\right] \cdot P\left[A(T_0 - t)\right] = \frac{1}{m_B} e^{-t/m_B} dt \left[1 - e^{-(T_0 - t)/m_A}\right]$$

Since F will result if the above compound event occurs for any t in $(0, T_0)$, P(F) is obtained by integrating over t in the overall interval:

$$P(F) = \int_0^{T_0} \frac{1}{m_B} e^{-t/m_B} \left[1 - e^{-(T_0 - t)/m_A}\right] dt$$

$$= \frac{1}{m_B} \int_0^{T_0} e^{-t/m_B} dt - \frac{1}{m_B} \int_0^{T_0} e^{-T_0/m_A + t/m_A - t/m_B} dt$$

If $m_A = m_B = m$,

$$P(F) = -e^{-t/m} \Big|_0^{T_0} - \frac{e^{-T_0/m}}{m} t \Big|_0^{T_0}$$

$$= 1 - e^{T_0/m} - \frac{T_0}{m} e^{-T_0/m}$$

$$= 1 - \left(1 + \frac{T_0}{m}\right) e^{-T_0/m}$$

Preserving only first and second order exponential terms,

$$P(F) \cong \frac{T_0^2}{2m^2}$$

F

If $m_A \neq m_B$

$$P(F) = 1 - e^{-T_0/m_B} - \frac{e^{-T_0/m_A}}{m_B} \cdot \frac{m_A m_B}{m_B - m_A} \, e^{[(m_B - m_A)/(m_A m_B)]t} \Big|_0^{T_0}$$

$$= 1 - e^{-T_0/m_B} + \frac{m_A}{m_B - m_A}\left(e^{-T_0/m_A} - e^{T_0/m_B}\right)$$

This is the exact expression for the general case. On expanding the exponentials to second order terms,

$$P(F) \approx \frac{T_0^2}{2m_A m_B}$$

Comparing this result with the approximation in Case I, one notes that the instantaneous detection feature has decreased the failure probability to half the unchecked value. This aspect is discussed more fully later.

In addition to the alarm detection situation specified in the hypothesis, Case II also applies to the following: Suppose B is the failure of an enable input to a gate. A is a sporadic pulse whose rise (or fall) in conjunction with B results in F. Before the occurrence of B (the persistent change of state) the appearance of A (a sporadic pulse) has no effect and is equivalent to failure and immediate correction But once B has occurred, the reappearance of A gives F

CASE IIa. F results only if B occurs before A in (0, T_0), but neither is subject to detection.

<u>Solution</u>: This case is similar to Case II in that an order condition is imposed. (Here it is explicit) It differs from Case II in that absence of failure detection requires P(F) to include an additional factor for the probability that A has not occurred up to the time B occurs. (In Case II, this factor is unity by virtue of the instantaneous detection and correction condition.) Therefore, the expression wanted is for the probability of the event, "B occurs in the differential interval dt starting at t, A has not occurred up to t, A occurs in (t, T_0)"

$$P[B(dt)] \cdot P[\bar{A}(t)] \cdot P[A(T_0 - t)] \quad \frac{1}{m_B} e^{-t/m_B} dt \cdot e^{-t/m_A}\left[1 - e^{-(T_0 - t)/m_A}\right]$$

As before, F will result if this compound event occurs for any t in $(0, T_0)$. P(F) is obtained by integration:

$$P(F) = \int_0^{T_0} \frac{1}{m_B} e^{-t/m_B} e^{-t/m_A} \left[1 - e^{-(T_0 - t)/m_A} \right] dt$$

$$= \frac{1}{m_B} \int_0^{T_0} e^{-t/m_B} \left[e^{-t/m_A} - e^{-T_0/m_A} \right] dt$$

$$= \frac{m_A}{m_A + m_B} e^{-[(m_A + m_B)/m_A m_B] t} \Bigg|_0^{T_0} + e^{-T_0/m_A} e^{-t/m_B} \Bigg|_0^{T_0}$$

$$= \frac{m_A}{m_A + m_B} \left[1 - e^{-[(m_A + m_B)/m_A m_B] T_0} \right] - e^{-T_0/m_A} \left[1 - e^{-T_0/m_B} \right]$$

$$= \frac{m_A}{m_A + m_B} + \frac{m_B}{m_A + m_B} e^{-[(m_A + m_B)/m_A m_B] T_0} - e^{-T_0/m_A}$$

This is the exact expression in the general case. If $m_A = m_B = m$,

$$P(F) = \frac{1}{2} + \frac{1}{2} e^{-2T_0/m} - e^{-T_0/m}$$

Again neglecting exponential terms above the second degree,

$$P(F) \cong \frac{T_0^2}{2m^2}$$

This result is the same as in Case II.

If one now approximates P(F) when $m_A \neq m_B$ by preserving terms only up to the second order, one again obtains

$$P(F) \approx \frac{T_0^2}{2m_A m_B}$$

as in Case II. Apparently the order condition alone has reduced the probability of failure by one half.

CASE III. The system is examined for the occurrence of A at discrete times $T_1, 2T_1, \ldots, nT_1 = T_0$. If A has occurred, corrective action is taken to replace the failure at the end of the interval in which it occurred. B's occurrence is not subject to detection throughout $(0, T_0)$.

Solution: This case introduces the effect of periodic testing of one critical element in the logical AND gate. In the actual system, T_1 could correspond to the daily Sensitive Command Network Test (SCNT) or the monthly TEST.

F will occur if both A and B coexist at any time. Because B's failure is persistent, while A's lasts only for the balance of the interval in which it occurs, F is the event "B fails in an interval, and A fails in the same or a subsequent interval."

$$\begin{aligned} P\left[F(0, T_0)\right] = {} & P\left[B(0, T_1)\right] \cdot P\left[A(0, T_0)\right] \\ & + P\left[B(T_1, 2T_1)\right] \cdot P\left[A(T_1, T_0)\right] \\ & + P\left[B(2T_1, 3T_1)\right] \cdot P\left[A(2T_1, T_0)\right] \\ & + \ldots + P\left\{B\left[(n-1)\,T_1, nT_1\right]\right\} \cdot P\left\{A\left[(n-1)\,T_1, nT_1\right]\right\} \end{aligned}$$

But

$$P\left[A(iT_1, nT_1)\right] = 1 - \left\{P\left[\bar{A}(0, T_1)\right]\right\}^{n-i}$$

The probability that A occurs in at least one of (n - i) intervals is the complement of the probability that it fails to occur in all of them.

$$\begin{aligned} \therefore P\left[F(0, T_0)\right] = {} & P\left[B(0, T_1)\right]\left\{1 - P^n\left[\bar{A}(i)\right]\right\} + P\left[B(T_1, 2T_1)\right]\left\{1 - P^{n-1}\left[\bar{A}(I)\right]\right\} \\ & + \ldots + P\left[B(n-1)\,T_1, nT_1\right]\left\{1 - P\left[\bar{A}(I)\right]\right\} \end{aligned}$$

where

$$P\left[\bar{A}(I)\right] = P\left[\bar{A}(0, T_1)\right]$$

Now

$$P\left[B(iT_1, (i+1)\,T_1\right] = e^{-\lambda_B iT_1}\left[1 - e^{-\lambda_B T_1}\right]$$

and

$$\left\{1 - P^{n-i}\left[\bar{A}(I)\right]\right\} = 1 - e^{-\lambda_A (n-i)T_1}$$

$$\therefore P\left[F(0, T_0)\right] = \left[1 - e^{-\lambda_B T_1}\right]\sum_{i=0}^{n-1} e^{-\lambda_B iT_1}\left[1 - e^{-\lambda_A (n-i)\,T_1}\right]$$

If $\lambda_A = \lambda_B = \lambda$,

$$P\left[F(0, T_0)\right] = \left[1 - e^{-\lambda T_1}\right] \sum_{i=0}^{n-1} e^{-\lambda i T_1} \left[1 - e^{-\lambda(n-i)T_1}\right]$$

$$= \left[1 - e^{-\lambda T_1}\right] \sum_{i=0}^{n-1} \left[e^{-\lambda i T_1} - e^{-\lambda n T_1}\right]$$

$$= \left[1 - e^{-\lambda T_1}\right] \left[\frac{1 - e^{-\lambda n T_1}}{1 - e^{-\lambda T_1}} - ne^{-\lambda n T_1}\right]$$

$$= 1 - e^{-\lambda n T_1} - ne^{-\lambda n T_1} + ne^{-\lambda(n+1)T_1}$$

$$= 1 - (n+1)\, e^{-\lambda n T_1} + ne^{-\lambda(n+1)T_1}$$

Preserving only first and second order terms,

$$P\left[F(0, T_0)\right] \cong \frac{\lambda^2 T_1^2}{2}\, n(n+1)$$

Again the similarity to Case II is noted.

If $\lambda_A \neq \lambda_B$,

$$P\left[F(0, T_0)\right] = \left[1 - e^{-\lambda_B T_1}\right] \sum_{i=0}^{n-1} e^{-\lambda_B i T_1} \left[1 - e^{-\lambda_A(n-i)T_1}\right]$$

Let

$$r = e^{-\lambda_B T_1}$$

$$s = e^{-\lambda_A T_1}$$

Then

$$P\left[F(0, T_0)\right] = (1 - r) \sum_{i=0}^{n-1} r^i - (1 - r) \sum_{i=0}^{n-i} r^i s^{n-i}$$

$$= (1 - r)\left[\frac{1 - r^n}{1 - r}\right] - (1 - r)\, s\left[\frac{s^n - r^n}{s - r}\right]$$

$$= 1 - r^n - \frac{(1 - r)s}{s - r}\,(s^n - r^n)$$

$$= 1 - r^n - \frac{(1 - r)s}{s - r}\left[(1 - r^n) - (1 - s^n)\right]$$

$$= (1 - r^n)\left[1 - \frac{(1-r)s}{s-r}\right] + \frac{(1-r)s}{s-r}\left[1 - s^n\right]$$

$$= 1 - r^n\left[\frac{s - r - s + rs}{s-r}\right] + \frac{(1-r)s}{s-r}\left[1 - s^n\right]$$

$$= \frac{(1-r)s}{s-r}(1 - s^n) - \frac{(1-s)r}{s-r}(1 - r^n)$$

The result has been expressed in this form to exhibit the remarkable symmetry in r and s or, equivalently, in λ_A and λ_B. This means that, if λ_A and λ_B are interchanged, the composite failure probability is not changed. Thus, if A has an MTBF of 10^7 hours while B has an MTBF of 10^5 hours, the probability of F is exactly the same as if these attributes were reversed. An even more surprising interpretation of the symmetry is that the probability of composite failure is the same whether one checks the more reliable or the less reliable device at the periodic intervals! This fact may have significant implications on maintenance procedures.

For use in computations, $P\left[F(0, T_0)\right]$ is expressed as

$$P\left[F(0, T_0)\right] = \left[1 - e^{-\lambda_B T_1}\right]\left\{\frac{1 - e^{-\lambda_B n T_1}}{1 - e^{-\lambda_B T_1}} - e^{-\lambda_A n T_1}\left[\frac{1 - e^{-(\lambda_B - \lambda_A) n T_1}}{1 - e^{-(\lambda_B - \lambda_A) T_1}}\right]\right\}$$

Once again the approximate expression retaining squared terms only is

$$P\left[F(0, T_0)\right] \cong \frac{1}{3}\lambda_A \lambda_B\, n(n+1)T_1^2 - \left[1 + \frac{1}{n}\right]\frac{T_0^2}{2}\lambda_A \lambda_B$$

This result tells how much protection is achieved by checking one device n times in the interval $(0, T_0)$. In particular, if there is no checking (n = 1),

$$P\left[F(0, T_0)\right] \cong (1+1)\frac{T_0^2}{2}\lambda_A \lambda_B = T_0^2 \lambda_A \lambda_B$$

as in Case I, and the probability of composite failure is twice as great as in the case of instantaneous checking (Case II). (The Case II result also follows by putting n = ∞ in the above approximation for P[F].) If a check is made once at the midpoint of $(0, T_0)$ so that n = 2, the probability of F is reduced by 25 percent from the no-check condition. Nine checks (n = 10) give a 45 percent reduction of the probability of F from the no-check case. With 100 checks, the probability of F is practically as low as in the Case II condition. Thus Case III includes Cases I and II as special cases.