KfK 2530
EUR 5754e
Februar 1980

Generalized Fault Tree Analysis Combined with State Analysis

L. Caldarola
Institut für Reaktorentwicklung
Projekt Nukleare Sicherheit

Kernforschungszentrum Karlsruhe

KERNFORSCHUNGSZENTRUM KARLSRUHE
Institut für Reaktorentwicklung
Projekt Nukleare Sicherheit

KfK 2530
EUR 5754e

Generalized Fault Tree Analysis Combined with State Analysis

L. Caldarola

Kernforschungszentrum Karlsruhe GmbH, Karlsruhe

Habilitationsschrift, Karlsruhe 1980

Kernforschungszentrum Karlsruhe GmbH
ISSN 0303-4003

Generalized Fault Tree Analysis Combined with State Analysis

Abstract

An analytical theory has been developed which allows one to calculate the occurrence probability of the top event of a fault tree with multistate (two or more than two states) components.

It is shown that, in order to correctly describe a system with multistate components, a special type of boolean algebra is required. This is called "boolean algebra with restrictions on variables" and its basic rules are the same as those of the traditional boolean algebra with some additional restrictions on the variables. These restrictions are extensively discussed in the paper. It is also shown that the boolean algebra with restrictions on variables facilitates the task of formally combining fault tree analysis with state analysis.

The definition of component has been generalized. A new classification of components into priviledged and unprivileged is proposed. It is shown that this classification eases the calculation of the expectation of a stochastic boolean variable especially in the case of statistical dependence.

The problem of statistical dependence has been solved either (1) by removing it, that is by replacing in the fault tree the statistically dependent primary variables by means of "ad hoc" new defined primary variables or (2) by evaluating separately (by means of the state analysis) the conditional probabilities of the statistically dependent events. The theory then provides the tools for correctly incorporating these conditional probabilities in the fault tree analysis. Criteria to establish which one of the two methods should be used are given in the paper.

A new definition of coherent boolean function is given in the paper.

Important features of the method are the identification of the complete base and of an irredundant base of a boolean function which does not necessarily need to be coherent. The identification of the complete as well as of an irredundant base of a boolean function requires the application of some algorithms which are not used in today's computer programmes for fault tree analysis. It is also shown that the knowledge of the complete base offers the possibility to find out whether or not two fault trees of the same system are equal, although they look apparently different.

The paper includes also small demonstrative examples to illustrate the theory.

The computer program MUSTAFA 1 based on the above theory has been developed. It can analyse fault trees of system containing statistically independent as well as dependent components with two or more than two states. MUSTAFA 1 can handle coherent as well as non coherent boolean functions.

Kombination von Fehlerbaumanalyse und Zustandsanalyse

Kurzfassung

Es wurde eine analytische Theorie entwickelt, mit der die Eintrittswahrscheinlichkeit des Top-Ereignisses eines Fehlerbaums mit Komponenten, die mehrere Zustände haben können (2 oder mehr als 2), berechnet werden kann.

Es wird gezeigt, daß eine spezielle Boolesche Algebra benötigt wird, um ein System mit solchen Komponenten richtig beschreiben zu können. Es ist die sogenannte "Boolesche Algebra mit beschränkten Variablen"; ihre Grundregeln sind die gleichen wie bei der gewöhnlichen Booleschen Algebra, mit einigen zusätzlichen Beschränkungen bezüglich der Variablen. Diese Beschränkungen werden im vorliegenden Beitrag ausführlich diskutiert. Außerdem wird gezeigt, daß die Boolesche Algebra mit beschränkten Variablen die Aufgabe der formellen Kombination von Fehlerbaumanalyse und Zustandsanalyse erleichtert.

Die Definition der Komponenten wurde allgemeiner formuliert. Es wird eine neue Einteilung der Komponenten in privilegierte und nicht privilegierte Komponenten vorgeschlagen und gezeigt, daß diese Einteilung die Berechnung der Erwartung einer stochastischen Booleschen Variablen, insbesondere bei statistischer Abhängigkeit, erleichtert.

Die Frage der statistischen Abhängigkeit wurde auf zwei Arten gelöst: (1) durch Ausschalten, d.h., die statistisch abhängigen, primären Variablen werden im Fehlerbaum ersetzt durch "ad hoc" neu definierte primäre Variablen; oder (2) durch getrennte Ermittlung (mit Hilfe der Zustandsanalyse) der bedingten Wahrscheinlichkeiten der statistisch abhängigen Ereignisse. Die Theorie liefert dann die Möglichkeiten für eine korrekte Berücksichtigung dieser bedingten Wahrscheinlichkeiten in der Fehlerbaumanalyse. Der Bericht enthält Kriterien dafür, welche der beiden Methoden benutzt werden sollte.

Eine neue Definition einer kohärenten Booleschen Funktion ist im Bericht enthalten.

Wichtige Merkmale der Methode sind die Identifizierung der vollständigen Basis und einer nichtredundanten Basis einer Booleschen Funktion, die nicht unbedingt kohärent sein muß. Die Identifizierung der vollständigen sowie einer nichtredundanten Basis einer Booleschen Funktion verlangt den Einsatz einiger Algorithmen, die in den derzeitigen Rechenprogrammen für die Fehlerbaumanalyse nicht benutzt werden. Weiterhin wird gezeigt, daß die Kenntnis der vollständigen Basis die Möglichkeit liefert festzustellen, ob zwei Fehlerbäume desselben Systems auch dann gleich sind, wenn sie unterschiedliche Struktur haben.

Der Beitrag enthält darüber hinaus kleine Demonstrationsbeispiele zur Erläuterung der Theorie.

Das auf der genannten Theorie beruhende Rechenprogramm MUSTAFA 1 wurde entwickelt. Mit ihm können Fehlerbäume eines Systems analysiert werden, das sowohl statistisch unabhängige als auch abhängige Komponenten mit 2 oder mehr als 2 Zuständen enthält. MUSTAFA 1 kann kohärente wie auch inkohärente Boolesche Funktionen bearbeiten.

C O N T E N T S

INTRODUCTION

The evaluation of the occurrence probability of the top event of a fault tree can be carried out by means of simulation methods (Monte Cartlo-type methods) or by means of analytical methods. Numerical simulation allows reliability information to be obtained for systems of almost any degree of complexity. However, this method provides only estimates and no parametric relation can be obtained. In addition, since the failure probability of a system is usually very low, precise results can be achieved only at the expense of very long computational times.

Analytical methods give more insight and understanding because explicit relationships are obtainable. Results are also more precise because these methods usually give the exact solution of the problem.

In 1970 Vesely /1/ gave the foundations of the analytical method for fault tree analysis.

Vesely's theory was improved by the author. A computer program for fault tree analysis was developed based on this theory /16; 8/. This computer program proved to be the best analytical program for fault tree analysis in the Federal Republic of Germany /17/.

Vesely's method can be applied only to coherent systems with binary (two states) components. Another important limitation of the method is that the boolean function which describes the top variable of the fault tree must not contain negated variables. Finally the theory does not give any indication on how to handle statistically dependent components.

Since there are components (e.g. a switch) which have more than two states, a theory was developed by the author in 1977 /2/ to handle systems with multistate components. Here the basic idea to associate the primary variables with the states of the primary components instead than with the primary components was introduced. In addition the basic boolean algorithms were described. In 1978 the author /3/ showed that the technique of multistate super-components can be used to remove statistical dependencies from a fault tree.

An interesting feature of the method proposed in /2/ and /3/ is that the boolean function which describes the top variable of the fault tree does not necessarily need to be coherent. In addition boolean functions containing negated variables can be treated.

A formalization of the theory by means of the so called "boolean algebra with restriction on variables" has been developed by the author in /12/. The basic and important boolean operations of this special type of boolean algebra are also described in this paper.

Hystorically two basic analytical tools have been developed to perform reliability analysis of systems. They are the state analysis and the fault tree analysis. The method of the block diagrams can be considered basically similar to that of the fault tree.

In the state analysis each individual elementary state of the system is considered. Usually (but not necessarily) the stochastic process which describes the system behaviour is Markovian. Since the number of elementary states in a complex system is very large, this type of analysis cannot be used in most practical cases. On the other hand, since the analysis is carried out at the level of elementary states, the statistical dependence among components can be easily incorporated in the model.

In the fault tree analysis, instead, the system is described by the so called minimal cut sets, which can be considered practically as macrostates, i.e. large sets of system elementary states. Since the number of minimal cut sets in a complex system is orders of magnitude smaller than the number of elementary states, the fault tree is in principle a more suitable tool to analyze complex systems. However the treatment of statistical dependence among components is not straight forward in this case.

We can say that in the state analysis the net of states considered is characterized by a very fine mesh. The net used in the fault tree analysis has instead a much coarser mesh. Since the problem of statistical dependence among components (such as common mode failure) affects the fine structure of a system, the coarse mesh used in the fault tree analysis is not suitable to handle the problem of statistical dependence. On the other hand the fine mesh used in the state analysis, although it would be suitable to cope with statistical dependence, is much too fine to handle complex systems.

From the above discussion it is clear that an intermediate mesh size is required for the analysis of statistical dependencies in complex systems. This mesh must be fine enough to retain the basic properties of statistical dependence and sufficiently coarse to still allow one to analyze complex systems.

This can be obtained by properly combining fault tree analysis with state analysis.
In the state analysis one deals with elementary states; in the fault tree analysis, instead, with variables. This fact makes it rather difficult to combine fault tree analysis with state analysis in a manageable way.

The boolean algebra with restriction on variables is the common language which can be used in both types of analysis.

We want now to give a short summary of the contents of each chapter of this paper with the purpose of offering some kind of guidance to the patient reader.
In chapter 1 the basic properties of the boolean algebra with restrictions on variables are described and the very close connection of this algebra to the set theory is discussed. A new definition of fault tree is also given.
In chapter 2 the expectation of a stochastic boolean variable is defined.

The relationships between boolean variables and indicator variables are also extensively discussed. Finally the normal disjunctive form of a boolean function is defined.

In chapter 3 the concept of component has been generalized. This new definition of component includes as a special case the primary component, which is here intended as a component whose probability data are directly available (e.g. from data banks). The differences between logical and statistical dependence are discussed. The conditional expectation of a boolean variable is defined and a theorem on these conditional expectations is given.

In chapter 4 the state analysis is introduced by using the notation of the boolean algebra with restrictions on variables. The methods of the condensation of two or more states into one state and of the expansion of one state into two or more states are described and discussed. Components are classified into privileged and unprivileged. This classification differs from that of statistically independent and statistically dependent components and is of basic importance for the proposed treatment of the statistical dependence among components.

In chapter 5 the state analysis is applied to the primary components. The main problem here is that of the state analysis of the dependent components. Here only the components which are statistically dependent on each other are considered. The remaining components of the system do not need to be considered. This means that the mesh size used in the analysis is defined by the elementary states of only a part of the system (smallest privileged super component) and is therefore much coarser than the mesh size defined by the system elementary states. However the selected mesh size is fine enough to retain the basic properties of statistical dependence.

In chapter 6 the state analysis of a bipolar switch (circuit breaker) is developed.

In chapter 7 the fault tree symbology is introduced.

In chapter 8 a system with only a few primary components is described and its fault tree is constructed.

In chapter 9 the occurrence probability of the primary events of the fault tree of chapter 8 are calculated by making use of the theory developed in chapter 6.

In chapter 10 the boolean operations to analyse a fault tree are extensively described. The theory is then applied to the example introduced in chapter 8.

In chapter 11 it will be shown how to calculate the occurrence probability of the top event of a fault tree. Only here will it become fully clear how the results of the state analysis are incorporated in the fault tree analysis.

In chapter 12 a new definition of a coherent boolean function is given and its properties are discussed.

Finally the concluding remarks about the proposed method are given in chapter 13.

1. BOOLEAN ALGEBRA WITH RESTRICTIONS ON VARIABLES. DEFINITION OF FAULT TREE

We consider a system at a fixed moment in time. Each elementary state of the system at a given time is obviously defined by the states occupied at that time by each individual primary component belonging to the system. A state of a primary component is called a primary state. The event of the system occupying one of its elementary states is called an elementary event. The event of a primary component occupying one of its states is called a primary event. We shall call a state (of the system) any defined set of elementary states (of the system).

The occurrence probability of a primary event is directly available (e.g. from reliability data banks). This property of the primary event can be taken as a basis for its definition

> "A primary event is an event whose occurrence probability is directly available."

Probability data associated with the failure of primary components (such as a pump, a relay etc.) are in general directly available from reliability data banks.

We now select a special set of elementary states of the system (e.g. the set of all elementary failed states) and call it the top state of the system (with small letters).

If we want to calculate the occurrence probablity of the event

$$\{\text{System is failed}\} \equiv \{\text{System is in the top state}\}$$

we have first to express the occurrence probability of this event as a sum of the occurrence probabilities of each elementary event.

$$P\{\text{System is in the top state}\} = \sum_{i=1}^{n} P\{\text{System is in the elementary state } s_i\}$$

where

> $P\{....\}$ indicates the occurrence probability of the event in brackets

and

> n = total number of elementary events.

The occurrence probability of each elementary state of the system is obtained by carrying out the state analysis of the system.

If the system is very complex, the number of its elementary states is extremely large. In this case the procedure described above becomes very cumbersome and cannot be applied in practice.

Another method is therefore needed.

We associate with the top state of the system a boolean variable which we call TOP (with capital letters). The variable TOP will take the value 1 (true) if the system occupies one of the elementary states belonging to the selected top set and the value 0 (false) otherwise.

{System is in the top state} ≡ {TOP = 1}

If all primary components of the system are binary, i.e. are characterized by only two states (intact and failed), we assign to each primary component a boolean variable which takes the value 1 if the component is failed and the value 0 if the component is intact. These are called primary variables. The value taken by a primary variable at a given time is a primary event.

If we want now to calculate the occurrence probability of the event

{TOP = 1}

we must first dissect the TOP variable into combinations of primary variables, that is to express the TOP variable as a proper function of the primary variables. The occurrence probability of the event {TOP = 1} can then be calculated as a function of the occurrence probabilities of the primary events.

Due to the complexity of most systems, the operation of dissection of the TOP variable into combinations of primary variables is in general carried out in steps. The TOP variable is first dissected into combinations of simpler non-primary variables (intermediate variables). These intermediate variables are in turn dissected into combinations of even simpler intermediate variables and so on. The process of dissection comes to an end when all combinations are combinations of primary variables only.

The process of dissection can be carried out in a graphic form by constructing a fault tree of the chosen TOP variable.

A fault tree is a logic model which shows in diagrammatic form the connections between the TOP variable and the primary variables.

A more precise definition of a fault tree can be given by making use of the graph theory.

> "A fault tree is a finite directed graph without loops. Each vertex may be in one of several states. For each vertex a function is given which specifies its states in terms of the states of its predecessors. Those vertices without predecessors are considered the independent variables of the fault tree." /4/

We are following the graphical terminology of Berge /5/ here. In the technical literature a vertex with predecessors is currently called a gate. The output variable of a gate is called (improperly) an output event of the gate. An input variable to a gate is called a predecessor or (again improperly) an input event to the gate. In the technical literature the improper terms TOP event, primary event are also currently used. One should instead use the more correct terms TOP variable and primary variable. In fact the word event is used (in the set theory and in the propositional calculus) to indicate a value or a set of values of a variable. We shall use the correct mathematical terminology here.

Note that in the above definition of fault tree the term "independent variable" is used and not "primary variable". The word indepdendent in this context means "logically independent", that is each input variable to the tree can take any value of its domain of definition independently of the values taken by the other input variables.

In the case of a fault tree with only binary primary components, the primary variables are the independent variables.

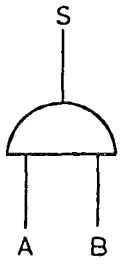
The truth table of the fault tree contains all possible combination among the values of the input variables. Each row of the truth table represents an elementary state of the system.

If the fault tree has m binary primary components, that is m input variables, the truth table of the fault tree has 2^m rows.

The function which links the output to the inputs of a gate are boolean functions. The basic gates are the AND (conjunction), OR (disjunction) and the NOT (negative) gates.

Let us first consider an AND gate with two inputs, namely A and B (Fig. 1-1)

AND Gate



Truth Table

Inputs		Output
A	B	S
0	0	0
0	1	0
1	0	0
1	1	1

Fig. 1-1. AND Gate ($S = A \wedge B$)

The truth table of Fig. 1-1 gives the value of the output S for each pair of values of the two predecessors A and B. This truth table can be expressed in words as follows

"Output takes the value 1 if and only if all predecessors take the value 1, and the value 0 if at least one of its predecessors takes the value 0."

We now order the values 1 and 0 in that we say, for instance that 1 is larger than 0

$$1 > 0$$

We can synthetize the AND operation as follows

$$S = \min (A; B)$$

which means that S takes the smaller of the values of A and B.

Fig. 1-2 shows the OR gate with associated truth table.

OR Gate

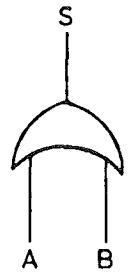


Fig. 1-2. OR Gate ($S = A \vee B$)

Truth Table

Inputs		Output
A	B	S
0	0	0
0	1	1
1	0	1
1	1	1

Also in this case the truth table of Fig. 1-2 can be expressed in words as follows

" Output takes the value 1 if at least one of the predecessors takes the value 1 and the value 0 if and only if all predecessors take the value 0."

If we put 1 > 0, we can write in the case of the OR gate

$$S = \max (A; B)$$

which means that S takes the larger of the values of A and B.

Fig. 1-3 shows the NOT gate with associated truth table.

NOT Gate

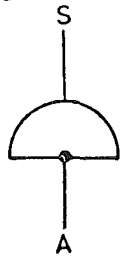


Fig. 1-3. NOT Gate ($S = \overline{A}$)

Truth Table

Inputs	Output
A	S
0	1
1	0

In words

"Output takes the value 1 if predecessor takes the value 0 and vice versa."

In a fault tree the truth tables of each gate are properly combined to get the truth table of the TOP. We show this by means of an example.

We consider the simple fault tree of Fig. 1-4 (Example No. 1). Each one of the two OR gates will be characterized by a truth table of the type of Fig. 1-2. The outputs of the two OR gates will be the inputs to the AND gate, which has a truth table of the type shown in Fig. 1-1. By properly combining the three truth tables one finally gets the overall truth table of the fault tree. This truth table has 16 rows (Fig. 1-5).

We now consider an elementary state of the system. Each elementary state of the system can be expressed by the cartesian product of the corresponding primary states. Consider, for instance, the row No. 7 of the truth table of Fig. 1-5.

System elementary state No. 7 "s_7" = $\{A_1=0\} \times \{B_1=1\} \times \{C_1=1\} \times \{A_2=0\}$ (1-0)

We now introduce the notation for the primary states (small letters). We have

$$\{A_1=0\} \equiv \bar{a}_1$$

$$\{B_1=1\} \equiv b_1$$

$$\{C_1=1\} \equiv c_1$$

$$\{A_2=0\} \equiv \bar{a}_2$$

Taking into account the above positions, Eq. 1-0 becomes

$$s_7 = \bar{a}_1 \times b_1 \times c_1 \times \bar{a}_2 \qquad (1\text{-}0a)$$

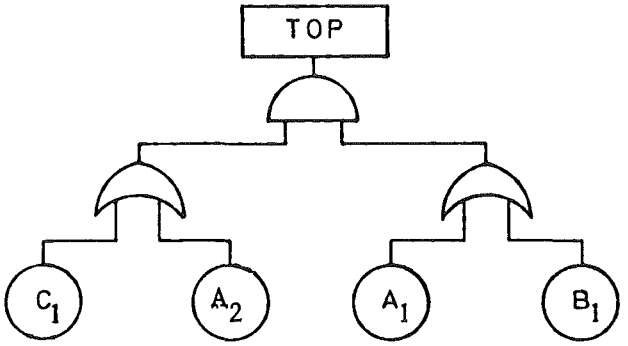


Fig. 1-4. Fault Tree - TOP = $(C_1 \vee A_2) \wedge (A_1 \vee B_1)$

	Row Number	Inputs				Output
		A_1	B_1	C_1	A_2	TOP
+	1	0	0	0	0	0
	2	0	0	0	1	0
+	3	0	0	1	0	0
	4	0	0	1	1	0
+	5	0	1	0	0	0
	6	0	1	0	1	1
+	7	0	1	1	0	1
	8	0	1	1	1	1
	9	1	0	0	0	0
—	10	1	0	0	1	1
	11	1	0	1	0	1
—	12	1	0	1	1	1
	13	1	1	0	0	0
—	14	1	1	0	1	1
	15	1	1	1	0	1
—	16	1	1	1	1	1

Fig. 1-5.
Complete truth table of the fault tree of Fig. 1-4 (Example No.1)

In the previous example we have assumed that all primary components are binary. There are however primary components which are characterized by more than two states. For instance an electrical circuit breaker is characterized by at least three states, namely (1) intact, (2) failed closed and (3) failed open.

One could in this case assign to each primary component a multivalued variable characterized by a number of values equal to the number of states of the primary component. Each value of the variable corresponds to a specific state of the primary component. These multivalued variables are the primary variables. They are pairwise mutually logically independent. Primary variables and independent variables are also in this case identical. The function which links the output to the input of a gate is a logic function which is in general very complex. This way of thinking is consistent with the definition of fault tree given above. There is however, a considerable drawback, namely that a more complicated multivalued logic must be developed. The basic gates are not any more simply the AND, OR and NOT gates as in the case of the boolean binary algebra. New basic gates must be found. Some authors /6/ are following this way of thinking. We want to follow another path instead. We want to have primary variables which are binary.

Let us consider the state space of a primary component. A state belonging to the state space of a primary component is called primary state. The event of the primary component occupying a given state of its state space at a given time is called primary event.

A primary component will be indicated by the small letter c followed by an integer positive number (c1; c2; c3 etc.). In general we shall have cj with j=1;2...; m, where "m" is the total number of primary components contained in the system.

A state of a primary component will be indicated by the same notation of the primary component to which it belongs followed by a positive integer number as an index. (cj_1; cj_2; cj_3 etc.) In general we shall have cj_q with q=1;2;...nj, where nj is the total number of states belonging to primary component cj.

We can now associate with each state cj_q a boolean variable Cj_q which takes the value 1 (true) if primary component cj occupies state cj_q and the value 0 (false) if cj does not occupy cj_q.

The event

$$\left\{Cj_q = 1\right\} \equiv cj_q$$

indicates that primary component cj occupies state cj_q.

Conversely, the event

$$\left\{Cj_q = 0\right\} \equiv \bigcup_{k=1}^{nj} cj_k \qquad k \neq q$$

indicates that primary component cj does not occupy state cj_q and therefore occupies one of its other possible states.

Note the one to one correspondence between state cj_q (small c) and boolean variable Cj_q (capital C) associated with it. We have

$$cj_q = \left\{ Cj_q = 1 \right\} \quad \text{and} \quad \overline{cj}_q \equiv \left\{ \overline{Cj}_q = 1 \right\} \equiv \left\{ Cj_q = 0 \right\}$$

We shall say that the primary state cj_q belongs to component cj ($cj_q \in cj$). The word "primary component" (with small c) is here intended as the set of all possible states which the component can occupy.

We shall also say that the variable Cj_q belongs to Component Cj ($Cj_q \in Cj$). The word "primary Component" (with capital C) means here the complete set of variables associated with its states.

The binary variables Cj_q are the primary variables. They are however not any more pairwise mutually independent.

Since a primary component must occupy one of its states and can occupy only one state at a time, the variables Cj_q must obviously satisfy the following two types of restrictions.

Restriction Type 1 The disjunction of all binary variables associated with the same primary Component is always equal to 1

$$\bigvee_{q=1}^{nj} Cj_q = 1 \qquad (1\text{-}1)$$

The notation "1" in Eq. 1-1 means "true". Eq.1 must be read as follows. The proposition "at least one of the variables Cj_q (q=1; ;...nj) takes the value 1" is always true.

Eq. 1-1 means that the variables Cj_q are prohibited to be all equal to 0 at the same time.

Restrictions Type 2 The conjunction of two different binary variables associated with the same primary Component is always equal to 0.

$$Cj_q \wedge Cj_k = 0 \qquad q \neq k \qquad (1\text{-}2)$$

The notation "0" in Eq. 1-2 means "false". Eq. 2 must be read as follows. The proposition "both variables Cj_q and Cj_k ($q \neq k$) take the value 1" is always false.

Eq. 1-2 can also be expressed in words as follows: "the variables Cj_q and Cj_k are mutually exclusive."

Note that there is only one restriction type 1 and $\frac{nj(nj-1)}{2}$ restrictions type 2.

Note also that Eqs. 1-1 and 1-2 can be translated straightforwardly into the equivalent equations among states. We have obviously

Restriction Type 1

$$\bigcup_{q=1}^{nj} cj_q = 1 \qquad (1\text{-}1a)$$

and

Restrictions Type 2

$$cj_q \cap cj_k = 0 \qquad q \neq k \qquad (1\text{-}2a)$$

Eqs. 1-1a and 1-2a have been obtained respectively from Eqs. 1-1 and 1-2 by carrying out the following simple operations.

Capital C		is replaced by		small c
Disjunction operator	$\vee$	"	"	Union operator $\cup$
Conjunction operator	$\wedge$	"	"	Intersection operator $\cap$

Note that the notation "1" and "0" in Eqs. 1-1a and 1-2a have a different meaning. They indicate respectively the "universal set" and the "empty set". Eq. 1-1a means therefore that the union of all states of a primary component constitutes an universal set, that is its complete state space. Eq. 1-1b means that the intersection of two different states of a primary component constitutes an empty set.

Since we have introduced primary variables which are not any more pairwise mutually independent, we have to slightly modify the definition of a fault tree.

> "A fault tree is a finite directed graph without loops. Each vertex may be in one of several states. For each vertex a function is given which specifies its states in terms of the states of its predecessors. Those vertices without predecessors are the primary variables of the fault tree. The primary variables may satisfy some conditions (called restrictions) which are associated with the fault tree. The restrictions must be such that they do not generate any loop in the fault tree".

We shall limit ourselves to consider fault trees characterized by a boolean TOP variable and by boolean primary variables which satisfy restrictions of the types given respectively by the Eqs. 1-1 and 1-2. These restrictions do not generate any loop in the fault tree.

It is worthwhile to stress once more the point that the primary variables in the traditional fault trees are associated with the primary components. In the fault trees proposed in this paper, instead, they are associated with the states of the primary components.

We consider now the truth table of the TOP variable.

Restriction type 1 means that the primary events

$$\left\{Cj_1 = 0\right\} \quad ; \quad \left\{Cj_2 = 0\right\};\ldots;\left\{Cj_{nj} = 0\right\}$$

cannot co-exist all together at the same time. This is equivalent to saying that all the rows of the truth table in which the variables Cj_1; Cj_2; Cj_3... take simultaneously the value 0 are prohibited and must be deleted.

The restrictions type 2 mean that the primary events

$$\left\{Cj_q = 1\right\} \quad \text{and} \quad \left\{Cj_k = 1\right\} \quad , \quad q \neq k$$

cannot co-exist at the same time. This is equivalent to saying that all the rows of the truth table in which both the two input variables Cj_q and Cj_k take the value 1 are prohibited and must be deleted.

The following two examples will make this point clearer.

Let us consider the fault tree of Fig. 1-4 and let us assume that the primary variables A_1 and A_2 belong both to the same primary Component which is characterized by two states (Example No. 2). Eqs. 1-1 and 1-2 become respectively

$$A_1 \vee A_2 = 1 \qquad (1\text{-}3)$$
$$A_1 \wedge A_2 = 0 \qquad (1\text{-}4)$$

Eq. 1-3 tells us that the events $\left\{A_1 = 0\right\}$ and $\left\{A_2 = 0\right\}$ cannot co-exist. If we now look at the complete truth table of the fault tree (Fig. 1-5) we notice that the rows 1; 3; 5 and 7 are prohibited because in these rows A_1 and A_2 have both the value 0. These rows must therefore be deleted.

Eq. 1-4 tells us that the events $\left\{A_1 = 1\right\}$ and $\left\{A_2 = 1\right\}$ cannot co-exist. This is equivalent to saying that the row No. 10; 12; 14 and 16 (Fig. 1-5) are also prohibited and must be deleted. The truth table of the fault tree of Fig. 1-4 with the additional conditions 1-3 and 1-4 will be reduced to that of Fig. 1-6 which contains eight rows only.

The input (primary) variables of the truth table of Fig. 1-6 are not all pairwise mutually independent. In fact the eight rows containing the combinations of values (0;0) or (1;1) for the variables A_1 and A_2 do not appear in the truth table of Fig. 1-6.

Row Number	Inputs				Output
	A_1	B_1	C_1	A_2	TOP
1	0	0	0	1	0
2	0	0	1	1	0
3	0	1	0	1	1
4	0	1	1	1	1
5	1	0	0	0	0
6	1	0	1	0	1
7	1	1	0	0	0
8	1	1	1	0	1

Fig. 1-6. Truth Table of Example No.2

It is sometimes possible however to reduce the number of the primary variables and to get the independent variables only. In the case of example No. 2 this is possible.

We notice that Eqs. 1-3 and 1-4 can be reduced to the following equation.

$$A_2 = \bar{A}_1 \qquad (1\text{-}5)$$

Eq. 1-5 means that, once a value has been assigned to the variable A_1, the variable A_2 takes a defined value according to the truth table of Fig. 1-3 (NOT Gate). For this reason the column corresponding to the variable A_2 in the truth table of Fig. 1-6 is redundant and can be deleted. The value of the TOP is in fact completely determined if the values of the primary variables A_1; B_1; C_2 havebeen previously chosen. The truth table of Fig. 1-6 can be further reduced by deleting the column of the primary variable A_2 (Fig. 1-7).

Row Number	Inputs			Output
	A_1	B_1	C_1	TOP
1	0	0	0	0
2	0	0	1	0
3	0	1	0	1
4	0	1	1	1
5	1	0	0	0
6	1	0	1	1
7	1	1	0	0
8	1	1	1	1

Fig. 1-7. Truth Table of Example No. 2 (Final)

Conversely one could keep the variable A_2 as independent variable and delete in Fig. 1-6 the column corresponding to the variable A_1 which would now be redundant.

Let us consider again the fault tree of Fig. 1-4 and let us assume that the primary variables A_1 and A_2 belong both to the same primary Component (as in example No. 2) but that this component is characterized now by three states and that the primary variable associated to the third state (call it A_3) is not present in the fault tree (example No. 3). In this case Eqs. 1-1 and 1-2 become respectively

$$A_1 \vee A_2 \vee A_3 = 1 \qquad (1\text{-}6)$$

and

$$A_1 \wedge A_2 = 0 \ (1\text{-}7a) \quad A_1 \wedge A_3 = 0 \ (1\text{-}7b) \quad A_2 \wedge A_3 = 0 \qquad (1\text{-}7c)$$

The rows 10; 12; 14; 16 of the truth table of Fig. 1-5 are prohibited because the events $\{A_1=1\}$ and $\{A_2=1\}$ cannot co-exist at the same time (Eq. 1-7a). By deleting these rows one obtains the truth table of Fig. 1-8 which contains 12 rows only.

Row Number	Inputs				Output
	A_1	B_1	C_1	A_2	TOP
1	0	0	0	0	0
2	0	0	0	1	0
3	0	0	1	0	0
4	0	0	1	1	0
5	0	1	0	0	0
6	0	1	0	1	1
7	0	1	1	0	1
8	0	1	1	1	1
9	1	0	0	0	0
10	1	0	1	0	1
11	1	1	0	0	0
12	1	1	1	0	1

Fig. 1-8. Truth Table of Example No. 3.

Note that in this case we don't make any use of the restrictions given by Eqs. 1-6; 1-7a and 1-7c because the primary variable A_3 is not explicitly contained in the fault tree.

The input variables of the truth table of Fig. 1-8 are not all pairwise mutually independent. In fact the four rows which contain the combination of values (1; 1) for the variables A_1 and A_2 do not appear in the truth table of Fig. 1-8. In this case however it is not possible to reduce the number of primary variables as in the case of Example No. 2. In fact no column in the truth table of Fig. 1-8 is redundant.

In conclusion the following rule can be stated (Rule No. 1)

"The truth table of the TOP variable of a fault tree can be obtained from the complete truth table (in which all primary variables present in the fault tree are assumed to be pairwise mutually independent) by deleting the prohibited rows and the redundant columns. The restrictions allow one to identify these prohibited rows and redundant columns. Each surviving row corresponds to a specific elementary state of the system. The surviving primary variables may or may not be pairwise mutually independent."

We notice that we have defined primary variables which are binary as in the classical boolean algebra, but not necessarily pairwise mutually independent. We shall therefore introduce the term "boolean algebra with restrictions on variables" to indicate an algebra in which the basic (primary) variables are boolean but not necessarily pairwise mutually independent. The classical binary boolean algebra can be considered as a particular case of this boolean algebra with restrictions on variables in that the basic variables are all pairwise mutually independent.

We now consider the elementary states of the top state. Consider, for instance, the row 7 of the truth table of Fig. 1-8 (Example No. 3).

$$\text{System elementary state No. 7 "}s_7\text{"} = \{B_1=1\} \times \{C_1=1\} \times \left[\{A_1=0\} \cap \{A_2=0\}\right] \quad (1\text{-}8)$$

Note that Equation 1-8 is obtained (1) by grouping all events which belong to the same component and linking them with the intersection operator $\cap$ and (2) by linking all groups with the cartesian product operator x. In fact the events $\{A_1=0\}$ and $\{A_2=0\}$ belong to the same component and must therefore be grouped together. Note that this problem does not exist in the case of the classical fault trees with binary components (Eq. 1-0)!

We now want to eliminate the groups.

Taking into account the boolean identities $A_3 \vee \bar{A}_3 = 1$ and $A_3 \wedge \bar{A}_3 = 0$, we get from Eqs. 1-6, 1-7b and 1-7c

$$A_3 = \overline{A_1 \vee A_2} = \bar{A}_1 \wedge \bar{A}_2 \quad (1\text{-}9)$$

From Eq. 1-9 we get

$$\{A_3=1\} \equiv \{\bar{A}_1 \wedge \bar{A}_2 = 1\} \equiv \{\bar{A}_1=1\} \cap \{\bar{A}_2=1\} \quad (1\text{-}10)$$

We have the following identities

$$\{\bar{A}_1=1\} \equiv \{A_1=0\} \quad (1\text{-}11)$$

and

$$\{\bar{A}_2=1\} \equiv \{A_2=0\} \quad (1\text{-}12)$$

Taking into account Eqs. 1-11 and 1-12, Eq. 1-10 becomes

$$\{A_1=0\} \cap \{A_2=0\} \equiv \{A_3=1\} \qquad (1\text{-}13)$$

Taking into account Eq. 1-13, Eq. 1-8 becomes

$$s_7 = \{B_1=1\} \times \{C_1=1\} \times \{A_3=1\} \qquad (1\text{-}14)$$

Note that Eq. 1-14 does not contain any more the intersection operator $\cap$ and all events contain the symbol 1.

We now introduce the notation for the states of the primary components (small letters). We have

$$\{B_1=1\} \equiv b_1 \qquad (1\text{-}15)$$

$$\{C_1=1\} \equiv c_1 \qquad (1\text{-}16)$$

$$\{A_3=1\} \equiv a_3 \qquad (1\text{-}17)$$

Taking into account Eqs. 1-15, 1-16, 1-17, Eq. 1-14 becomes

$$\text{System elementary state No. 7 } "s_7" = b_1 \times c_1 \times a_3 \qquad (1\text{-}18)$$

The expression on the right side of Eq. 1-18 is called the smallest form of system elementary state No. 7.

Each elementary state of a system has only one smallest form.

We can now state the following definition

" The smallest form of an elementary state of a system is defined by the cartesian product of the states occupied by each single primary component belonging to the system."

We now go back to Eq. 1-14 which we can now write in a more compact form.

$$s_7 = \{B_1=1\} \times \{C_1=1\} \times \{A_3=1\} = \{B_1 \wedge C_1 \wedge A_3 = 1\} \qquad (1\text{-}19)$$

From Eqs. 1-18 and 1-19, we get

$$b_1 \times c_1 \times a_3 = \{B_1 \wedge C_1 \wedge A_3 = 1\} \qquad (1\text{-}20)$$

Before discussing Eq. 1-20, we want to introduce some new terms. A variable which results from the conjunction of primary variables is called monomial. A monomial containing two or more primary variables belonging to the same primary component is obviously equal to zero (restrictions type 2). A non-zero monomial containing a number of primary variables equal to the number of primary components present in the system is called "complete monomial". It is important to point out that the primary variables of a complete monomial must not be negated. For instance, the monomial $B_1 \wedge C_1 \wedge A_3$ of Example 3 is a complete monomial. For a given system the number of complete monomials is equal to the number of its elementary states.

Eq. 1-20 tells us that, given the complete monomial $B_1 \wedge C_1 \wedge A_3$, one obtains the smallest form of the corresponding elementary state $b_1 \times c_1 \times a_3$ by carrying out the following operation

B_1 is replaced by b_1
C_1 " " " c_1
A_3 " " " a_3
conjunction operator $\wedge$ " " " cartesian product operator x

We can now state the following rule (Rule No. 2).

"The smallest form of an elementary state of a system is obtained from its corresponding complete monomial by replacing each primary variable by its associated primary state and each conjunction operator ($\wedge$) by the cartesian product operator (x).

Conversely we have

"A complete monomial of a system is obtained from the smallest form of its corresponding system elementary state by replacing each primary state by its associated primary variable and each cartesian product operator (x) by the conjunction operator ($\wedge$)."

It is important to point out that the complete monomial $B_1 \wedge C_1 \wedge A_3$ can be obtained from the truth table of Fig. 1-8 by applying a more straight forward procedure, i.e. the rules of the traditional boolean algebra and those due to the restrictions. We have from the truth table of Fig. 1-8

$$S_7 = \bar{A}_1 \wedge B_1 \wedge C_1 \wedge \bar{A}_2 \qquad (1\text{-}20a)$$

Taking into account Eq. 1-9 , Eq.1-20a becomes

$$S_7 = A_3 \wedge B_1 \wedge C_1 \qquad (1\text{-}20b)$$

Going back to the truth table of Fig. 1-18 (Example No. 3), we select the rows for which TOP = 1. These are the rows No. 6, 7, 8, 10 and 12. Each selected row respresents an elementary state of the system for which the equation TOP = 1 is satisfied. We now find the smallest form of each row. In order to do that we must introduce the states b_2 and c_2 which satisfy the restrictions respectively with b and c.

$$b_1 \cup b_2 = 1 \quad (1\text{-}21a) \; ; \quad b_1 \cap b_2 = 0 \qquad (1\text{-}21b)$$

and

$$c_1 \cup c_2 = 1 \quad (1\text{-}22a) \qquad c_1 \cap c_2 = 0 \qquad (1\text{-}22b)$$

The smallest forms of the rows 6, 7, 8, 10 and 12 are given in the following table (Fig. 1.9).

System elementary state	Smallest form
6	$b_1 \times c_2 \times a_2$
7	$b_1 \times c_1 \times a_3$
8	$b_1 \times c_1 \times a_2$
10	$a_1 \times b_2 \times c_1$
12	$a_1 \times b_1 \times c_1$

Fig. 1.9 Smallest form of system states (from the truth table of Fig. 1.8).

By making use of the above table we can now write

$$top = (b_1 x c_2 x a_2) \cup (b_1 x c_1 x a_3) \cup (b_1 x c_1 x a_2) \cup (a_1 x b_2 x c_1) \cup (a_1 x b_1 x c_1) \quad (1\text{-}23)$$

Eq. 1-23 can be written as follows

$$\{TOP = 1\} = \{B_1 \wedge C_2 \wedge A_2 = 1\} \vee \{B_1 \wedge C_1 \wedge A_3 = 1\} \vee \{B_1 \wedge C_1 \wedge A_2 = 1\} \vee \{A_1 \wedge B_2 \wedge C_1 = 1\} \vee \{A_1 \wedge B_1 \wedge C_1 = 1\} \quad (1\text{-}24)$$

Eq. 1-24 can be written in a more compact form

$$\{TOP=1\} = \{(B_1 \wedge C_1 \wedge A_2) \vee (B_1 \wedge C_2 \wedge A_3) \vee (B_1 \wedge C_1 \wedge A_2) \vee (A_1 \wedge B_2 \wedge C_1) \vee (A_1 \wedge B_1 \wedge C_1) = 1\} \quad (1\text{-}25)$$

From Eq. 1-25 we also get

$$TOP = (B_1 \wedge C_2 \wedge A_2) \vee (B_1 \wedge C_1 \wedge A_3) \vee (B_1 \wedge C_1 \wedge A_2) \vee (A_1 \wedge B_2 \wedge C_1) \vee (A_1 \wedge B_1 \wedge C_1) \quad (1\text{-}26)$$

Eqs. 1-23 and 1-26 tell us that given the variable TOP as a disjunction of complete monomials (Eq. 1-26) one obtains the expression of the **top set** (Eq. 1-23) by carrying out the following operations

TOP	is	replaced	by	top
A_1	"	"	"	a_1
B_1	"	"	"	b_1
B_2	"	"	"	b_2
C_1	"	"	"	c_1
C_2	"	"	"	c_2
A_2	"	"	"	a_2
A_3	"	"	"	a_3

conjunction operator $\wedge$ " " " cartesian product operator x
disjunction operator $\vee$ " " " union operator $\cup$

The disjunction of complete monomials of a boolean function is called "disjunctive canonical form" of the function.

Now we can state the following rule (Rule No. 3)

"If the variable TOP is given in its disjunctive canonical form, the corresponding top state is obtained by replacing each complete mononomial by the corresponding smallest form of system elementary state and each disjunction operator ($\vee$) by the union operator ($\cup$)."

Conversely we have

"If the top state is given in the form of union of smallest forms of elementary states the corresponding disjunctive canonical form of the variable TOP is obtained by replacing each smallest form of elementary state by the corresponding complete monomial and each union operator ($\cup$) by the disjunction operator ($\vee$)."

We notice that the disjunction operator $\vee$ is always replaced by the union operator $\cup$. The conjunction operator $\wedge$ instead is replaced by the intersection operator $\cap$ in the case of the restrictions type 2 (Eqs. 1-2 and 1-2a) and by the cartesian product operator x in the case of the complete monomials. This fact however does not cause any problem. In fact any complete monomial is a non-zero monomial which corresponds to a specific elementary state of the system. A state is by definition a non-empty set. Since the restrictions are only used to identify the zero monomials of a boolean function, that is the prohibited rows of the corresponding truth table, and these are always deleted, it is impossible to get smallest forms of system elementary states containing the intersection operator, and complete monomials which contain two or more primary variables belonging to the same primary component.

In conclusion the boolean algebra with restrictions on variables allows us to operate on boolean variables in a way similar to the classical boolean algebra, but with the additional complication of the restrictions. Once that the boolean expression of the TOP variable has been found, the rules No. 2 and 3 allow one to easily identify the smallest form of the elementary states belonging to the top state.

The advantage of using boolean variables instead of states is obviously that of having a more flexible instrument to operate. We show this point by developing Eq. 1-26. We notice that

$$(B_1 \wedge C_2 \wedge A_2) \vee (B_1 \wedge C_1 \wedge A_2) = (B_1 \wedge A_2) \qquad (1\text{-}27)$$

and

$$(A_1 \wedge B_2 \wedge C_1) \vee (A_1 \wedge B_1 \wedge C_1) = (A_1 \wedge C_1) \qquad (1\text{-}28)$$

Taking into account Eqs. 1-27 and 1-28, Eq. 1-26 becomes

$$TOP = (B_1 \wedge A_2) \vee (A_1 \wedge C_1) \vee (B_1 \wedge C_1 \wedge A_3) \qquad (1\text{-}29)$$

We also notice that

$$A_3 = \bar{A}_1 \wedge \bar{A}_2 \qquad (1\text{-}30)$$

and therefore

$$(B_1 \wedge A_2) \vee (B_1 \wedge C_1 \wedge A_3) = B_1 \wedge \left[A_2 \vee (C_1 \wedge \bar{A}_1 \wedge \bar{A}_2)\right] = (B_1 \wedge A_2) \vee (B_1 \wedge C_1 \wedge \bar{A}_1) \qquad (1\text{-}31)$$

Taking into account Eq. 1-31, Eq. 1-29 becomes

$$TOP = (B_1 \wedge A_2) \vee (A_1 \wedge C_1) \vee (B_1 \wedge C_1 \wedge \bar{A}_1) \qquad (1\text{-}32)$$

We have

$$(A_1 \wedge C_1) \vee (B_1 \wedge C_1 \wedge \bar{A}_1) = C_1 \wedge \left[A_1 \vee (B_1 \wedge \bar{A}_1)\right] = (C_1 \wedge A_1) \vee (C_1 \wedge B_1) \qquad (1\text{-}33)$$

Taking into account Eq. 1-33, Eq. 1-32 becomes finally

$$TOP = (B_1 \wedge A_2) \vee (A_1 \wedge C_1) \vee (C_1 \wedge B_1) \qquad (1\text{-}34)$$

The top set is simply given by

$$top = \left\{ (B_1 \wedge A_2) \vee (A_1 \wedge C_1) \vee (C_1 \wedge B_1) = 1 \right\} \qquad (1\text{-}35)$$

Note that the expression of the top state given by Eq. 1-35 (i.e. by using the boolean variables) is much simpler and much more compact than the equivalent expression given by Eq. 1-23 (i.e. by using the state analysis). In addition the expression 1-34 can be obtained directly by solving the fault tree without considering the complete monomials. This is the great advantage of using fault tree analysis!

The fundamental rules of the boolean algebra with restrictions on variables have been explained by the author in /24/. There it is shown that the restricted variables can be understood as minterms x) of an "ad hoc" defined filter function which allows one to sort out the desired elements of a set. The relationships between the restrictions and the axioms of the boolean algebra are also illustrated in /24/. In particular it is shown that the complement of a primary variable (say A_i) is equal to the disjunction of all remaining primary variables belonging to the same primary Component, that is

$$\bar{A}_i = \bigvee_{k=1}^{n} A_k \qquad (k \neq i) \qquad (i=1,2,\ldots,n) \qquad (1\text{-}36)$$

where

n = total number of primary variables belonging to the primary Component A.

By complementing both sides of Eq. 1-36, one gets

$$A_i = \bigwedge_{k=1}^{n} \bar{A}_k \qquad (k \neq i) \qquad (i=1,2,\ldots,n) \qquad (1\text{-}37)$$

In the following we shall write the word component always with small "c".

x) minterm = complete monomial

2. STOCHASTIC BOOLEAN VARIABLES. EXPECTATION OF A STOCHASTIC BOOLEAN VARIABLE. NORMAL DISJUNCTIVE FORM OF A BOOLEAN FUNCTION.

In the preceeding chapter we have introduced boolean variables which can take a value (either 0 or 1) and we have shown that the state of the system at a given time can be described by these variables. This is like a photograph of the system at the chosen time.

The state of the system will change with time due to the fact that e.g. some parts of it will fail and some other parts will be repaired. This means that the TOP variable will change randomly with time. The process which describes how this variable changes with time is a stochastic process. This stochastic process is a function of the stochastic processes of each individual primary component, i.e. of the primary variables.

We shall speak therefore of stochastic boolean variables as variables which can take at each time either the value 0 or 1, and which can jump from one value to the other according to some probability laws which must be specified.

The theory of reliability has been traditionally developed by introducing the so called binary indicator variables /14/. Each primary component is given a stochastic binary indicator variable which takes at a given time the value 1 if the component is failed and the value 0 if the component is intact. Here the values 1 and 0 are real numbers. The behaviour of the system too is characterized by a stochastic binary indicator variable, which can be expressed as a function (structure function) of the primary indicator variables.

The advantage of using binary indicator variables is that the expected value of the variable is equal to the probability that the variable takes the value 1. If we indicate with A' a stochastic binary indicator variable, we have in fact

$$E\left\{A'\right\} = 1 \cdot P\left\{A'=1\right\} + 0 \cdot P\left\{A'=0\right\} = P\left\{A'=1\right\} \qquad (2\text{-}1)$$

where

$E\{\cdots\}$ = expectation (expected value) of the variable in brackets.

and

$P\{\cdots\}$ = occurrence probability of the event in brackets.

Note the Eq. 2-1 holds only in the case that the indicator variable is binary. If one uses multivalued indicator variables to describe multistate components, Eq. 2-1 does not hold any more!

We want to use boolean variables instead of indicator variables, because boolean functions are much simpler and more compact than

structure functions.

The problem therefore arises of the definition of the expectation of a stochastic boolean variable.

The definition of the expectation of a stochastic boolean variable cannot be introduced straight-forwardly because the values 1 and 0 that a boolean variable can take are not numbers. According to what was said in the preceeding chapter 1 means true and 0 means false.

In order to define correctly the expectation of boolean variables, we introduce the binary indicator variables (also stochastic) which can take either the value 1 or the value 0, where 1 and 0 are now real numbers.

We can therefore associate with each boolean primary variable a primary binary indicator variable which takes the value 1 if and only if the boolean variable takes the value 1 and the value 0 if and only if the boolean variable takes the value 0. Given a boolean primary variable A, we shall indicate with A' its associated primary indicator variable

$$A \longleftrightarrow A' \tag{2-2}$$

Relationship 2-2 means that A and A' are equivalent to each other.

Due to the above definition of indicator variable, the following two identities among events hold

$$\{A = 1\} \equiv \{A' = 1\} \tag{2-3}$$

and

$$\{A = 0\} \equiv \{A' = 0\} \tag{2-4}$$

We take now the occurrence probabilities of both primary events respectively of Eqs. 2-3 and 2-4 and we get the following two equalities among probabilities

$$P\{A = 1\} = P\{A' = 1\} \tag{2-5}$$

and

$$P\{A = 0\} = P\{A' = 0\} \tag{2-6}$$

Note that the two probabilies defined respectively by Eqs, 2-5 and 2-6 must obviously satisfy the following equation

$$P\left\{A = 1\right\} + P\left\{A = 0\right\} = 1 \qquad (2\text{-}7)$$

It seems logical now to define the expectation of a stochastic primary boolean variable to be identical with the expectation of its associated stochastic primary indicator variable, that is

$$E\left\{A\right\} \stackrel{def}{=} E\left\{A'\right\} \qquad (2\text{-}8)$$

From Eqs. 2-1, 2-3 and 2-8 it follows

$$E\left\{A\right\} = P\left\{A = 1\right\} \qquad (2\text{-}9)$$

Either Eq. 2-8 or Eq. 2-9 can be used to define the expectation of the stochastic primary boolean variable A.

For the sake of simplicity we drop from now on the attribute stochastic.

We want now to extend the validity of Eq. 2-8 also to the case of boolean variables which are not necessarily primary. For this purpose we must define the three basic arithmetical operations among binary indicator variables which are equivalent respectively to the three basic boolean operations of negation (NOT), conjunction (AND) and disjunction (OR). An arithmetical operation is said to be equivalent to a boolean operation if and only if the truth tables of the two operations are formally identical. Formally identical means that the arithmetical truth table is obtained from the boolean one by replacing each boolean 1 with an arithmetical 1 and each 0 with a 0. In fact, since each row of the truth table is a state of the output variable, formal identity of the two truth tables means identity of the events, i.e. Eqs. 2-3 and 2-4 are satisfied for each event of the truth tables.

The arithmetical operation which is equivalent to the boolean negation is the complementation to unity.

$$\bar{A} \longleftrightarrow 1 - A' \qquad (2\text{-}10)$$

In fact the truth tables associated to the two above operations are formally identical (Fig. 2-1).

Taking into account Eq. 2-8 and relationship 2-10, we can write

$$E\left\{\bar{A}\right\} = E\left\{1-A'\right\} = 1 - E\left\{A'\right\} = 1 - E\left\{A\right\} \qquad (2\text{-}11)$$

Note that Eq. 2-11 must be identical with the result which one would obtain by applying the definition given by Eq. 2-9 directly

Truth table of the boolean negation (NOT)

Input	Output
A	$\bar{A}$
0	1
1	0

Truth table of the arithmetical complementation to unity

Input	Output
A'	1 - A'
0	1
1	0

Fig. 2-1: Truth tables of the boolean negation and of the arithmetical complementation to unity.

to $\bar{A}$. From Eq. 2-9 we get for $\bar{A}$

$$E\left\{\bar{A}\right\} = P\left\{\bar{A} = 1\right\} \qquad (2\text{-}12)$$

On the other hand, taking into account Eqs. 2-7 and 2-9 and the truth table of the boolean negation, Eq. 2-11 becomes

$$E\left\{\bar{A}\right\} = 1 - E\left\{A\right\} = 1 - P\left\{A=1\right\} = P\left\{A=0\right\} = P\left\{\bar{A}=1\right\} \qquad (2\text{-}13)$$

which is identical with Eq. 2-12.

The conjunction of two boolean variables A and B has as equivalent operation the product of the two associated binary indicator variables, namely A' and B'.

$$A \wedge B \longleftrightarrow A' \cdot B' \qquad (2\text{-}14)$$

The truth tables associated to the two above operations are in fact formally identical (Fig. 2-2)

Truth table of the boolean conjunction (AND)

Inputs		Output
A	B	$A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	1

Truth table of the arithmetical product

Inputs		Output
A'	B'	A' • B'
0	0	0
0	1	0
1	0	0
1	1	1

Fig. 2-2: Truth tables of the boolean conjunction and of the arithmetical product.

Taking into account Eq. 2-8 and relationship 2-14 we can write

$$E\left\{A \wedge B\right\} = E\left\{A' \cdot B'\right\} \qquad (2\text{-}15)$$

It is easy to verify that Eq. 2-15 is identical with the result which one would obtain by applying the definition of expectation (given by Eq. 2-9) directly to the boolean variable $A \wedge B$. In the particular case that A = B, we have (idempower law)

$$A \wedge A = A \longleftrightarrow A' \cdot A' = (A')^2 = A' \qquad (2\text{-}16)$$

The disjunction of two boolean variables A and B has an equivalent operation between the associated binary indicator variables A' and B' which is directly deducible from the already introduced arithmetical operations of complementation to unity (correspondent to NOT) and of product (correspondent to AND).

We have

$$A \vee B = \overline{\bar{A} \wedge \bar{B}} \qquad (2\text{-}17)$$

By applying relationships 2-10 and 2-14 we have obviously the following equivalence between boolean variables and indicator variables

$$\overline{\bar{A} \wedge \bar{B}} \longleftrightarrow 1 - (1 - A') \cdot (1 - B') \qquad (2\text{-}18)$$

From Eq. 2-17 and relationship 2-18 it follows

$$A \vee B \longleftrightarrow 1 - (1 - A') \cdot (1 - B') \qquad (2\text{-}19)$$

Since we have

$$1 - (1 - A') \cdot (1 - B') = A' + B' - A' \cdot B' \qquad (2\text{-}20)$$

relationship 2-19 can also be written as follows

$$A \vee B \longleftrightarrow A' + B' - A' \cdot B' \qquad (2\text{-}21)$$

The truth tables associated with the two above operations (boolean disjunction and arithmetical disjunction) are formally identical (Fig. 2-3).

Taking into account Eq. 2-8 and relationship 2-21 we can write

$$E\left\{A \vee B\right\} = E\left\{A'+B'-A' \cdot B'\right\} = E\left\{A'\right\} + E\left\{B'\right\} - E\left\{A' \cdot B'\right\} =$$
$$= E\left\{A\right\} + E\left\{B\right\} - E\left\{A \wedge B\right\} \qquad (2\text{-}22)$$

If the two boolean variables A and B are mutually exclusive (restriction type 2) we have

$$A \wedge B = 0 \qquad (2\text{-}23)$$

Truth table of the boolean disjunction (OR)

Inputs		Output
A	B	A ∨ B
0	0	0
0	1	1
1	0	1
1	1	1

Truth table of the arithmetical disjunction

Inputs		Output
A'	B'	A'+B'-A'·B'
0	0	0
0	1	1
1	0	1
1	1	1

Fig. 2-3: Truth tables of the boolean disjunction and of the arithmetical disjunction

This means that the last row of the truth table of the boolean conjunction (Fig. 2-2) and of the boolean disjunction (Fig. 2-3) must be deleted. In order to save the formal identity between the two truth tables of Fig. 2-2 and between the two truth tables of Fig. 2-3, the last row of the truth table of the arithmetical product (Fig. 2-2) and of the arithmetical disjunction (Fig. 2-3) must be also deleted. This is equivalent to saying

$$A' \cdot B' = 0 \tag{2-24}$$

In this case relationship 2-21 becomes simply

$$A \vee B \longleftrightarrow A' + B' \tag{2-25}$$

Eqs. 2-15 and 2-22 become respectively

$$E\left\{A \wedge B\right\} = E\left\{A' \cdot B'\right\} = 0 \tag{2-26}$$

and

$$E\left\{A \vee B\right\} = E\left\{A'+B'\right\} = E\left\{A'\right\} + E\left\{B'\right\} = E\left\{A\right\} + E\left\{B\right\} \tag{2-27}$$

We are now in the position to write the restrictions type 1 and 2 for the primary indicator variables.

We indicate with C'_{j_q} the primary indicator variable equivalent to the primary boolean variable C_{j_q}

$$C_{j_q} \longleftrightarrow C'_{j_q} \tag{2-28}$$

The restrictions type 2 are (Eq. 1-2)

$$C_{j_q} \wedge C_{j_k} = 0 \quad q \neq k \quad q,k=1,2,\ldots,n_j \tag{2-29}$$

The equivalent equations for the primary indicator variables are obtained by making use of relationship 2-14 and of Eqs. 2-23 and 2-24. We get

$$C'_{j_q} \cdot C'_{j_k} = 0 \qquad q \neq k \qquad q,k=1,2,\ldots,n_j \tag{2-30}$$

The restriction type 1 is (Eq. 1-1)

$$\bigvee_{q=1}^{n_j} C_{j_q} = 1 \tag{2-31}$$

Taking into account relationships 2-28 and 2-25, we can write

$$\bigvee_{q=1}^{n_j} C_{j_q} \longleftrightarrow \sum_{q=1}^{n_j} C'_{j_q} \tag{2-32}$$

Finally (by taking into account Eq. 2-31) the restriction type 1 can be written as follows

$$\sum_{q=1}^{n_j} C'_{j_q} = 1 \tag{2-33}$$

In conclusion the restrictions type 1 and 2 in the case of the primary indicator variables are the following

Restriction type 1

$$\sum_{q=1}^{n_j} C'_{j_q} = 1 \tag{2-34}$$

and

Restrictions type 2

$$C'_{j_q} \cdot C'_{j_k} = 0 \qquad q \neq k \qquad q,k=1,2,\ldots,n_j \tag{2-35}$$

The restrictions type 1 and 2 can also be written in the form of relationships among expectations. We have obviously

Restriction Type 1

$$\sum_{q=1}^{n_j} E\left\{C_{j_q}\right\} = \sum_{q=1}^{n_j} E\left\{C'_{j_q}\right\} = 1 \qquad (2\text{-}36)$$

and

Restrictions Type 2

$$E\left\{C_{j_q} \wedge C_{j_k}\right\} = E\left\{C'_{j_q} \cdot C'_{j_k}\right\} = 0 \qquad (2\text{-}37)$$

$q \neq k \qquad q,k=1,2,\ldots,n_j$

It is known that a complex boolean variable (TOP) can be expressed as a combination of basic operations (NOT, AND, OR) among primary boolean variables. If we associate a primary indicator variable to each primary boolean variable and replace each basic boolean operation by its equivalent arithmetical operation, we get an arithmetical expression for the binary indicator variable TOP' associated with the boolean variable TOP. The complete truth table of TOP' is formally identical with that of TOP.

The restrictions type 1 and 2 (Eqs. 1-1 and 1-2) allow us to identify the prohibited rows and the redundant columns of the truth table of the boolean variable TOP. Eqs. 2-34 and 2-35 allow us to identify the prohibited rows and the redundant columns in the truth table of the indicator variable TOP' in a similar way to that shown in chapter 1 in the case of the primary boolean variables.

Due to the way in which Eqs. 2-34 and 2-35 have been derived, these prohibited rows and redundant columns are formally identical with the equivalent prohibited rows and redundant columns of the complete truth table of the boolean variable TOP.

The prohibited rows and the redundant columns are now deleted in both truth tables. The surving rows and columns in the resulting truth tables are formally identical. This is the same as saying that TOP and TOP' are equivalent

$$TOP \longleftrightarrow TOP' \qquad (2\text{-}38)$$

Taking into account relationship 2-38, we can write the following equation

$$E\left\{TOP\right\} = E\left\{TOP'\right\} \qquad (2\text{-}39)$$

Since

$$E\left\{TOP'\right\} = P\left\{TOP' = 1\right\} \geq P\left\{TOP = 1\right\} \qquad (2\text{-}40)$$

we have finally

$$E\left\{TOP\right\} = P\left\{TOP = 1\right\} \qquad (2\text{-}41)$$

The following two rules can now be stated

Rule No. 1

> Given a boolean function TOP the equivalent arithmetical function TOP' is obtained from the TOP by replacing (1) each primary boolean variable with the equivalent primary indicator variable, (2) each operation of boolean negation with the arithmetical complementation to unity, (3) each operation of boolean conjunction with the arithmetical product, (4) each operation of boolean disjunction with the arithmetical disjunction and (5) each restriction among primary boolean variables with the equivalent restriction among primary indicator variables.

Rule No. 2

> The expectation of a boolean function TOP (i.e. the occurrence probability of the event $\{TOP = 1\}$) is equal to the expectation of the corresponding arithmetical function TOP'.

In order to illustrate the two above rules, we consider now an example. We have

$$TOP = G_1 \vee (F_2 \wedge G_2) \vee (L_2 \wedge G_3) \vee (L_1 \wedge G_2) \vee (F_1 \wedge G_3) \vee (L_1 \wedge F_1) \qquad (2\text{-}42)$$

Each of the primary components L and F has three states. The component G has four states.

The following table (Fig. 2-4) shows the various steps for the calculation of the arithmetical function TOP' which corresponds to the TOP. The content of the table is selfexplanatory.

Step No.	Boolean Expression	Equivalent Arithmetical Expression
1	G_1	G_1'
2	$G_1 \vee (F_2 \wedge G_2)$	$G_1'+F_2'\cdot G_2'$
3	$G_1 \vee (F_2 \wedge G_2) \vee (L_2 \wedge G_3)$	$G_1'+F_2'\cdot G_2'+L_2'\cdot G_3'$
4	$G_1 \vee (F_2 \wedge G_2) \vee (L_2 \wedge G_3) \vee (L_1 \wedge G_2)$	$G_1'+F_2'\cdot G_2'+L_2'\cdot G_3'+L_1'\cdot G_2'-L_1'\cdot F_2'\cdot G_2'$
5	$G_1 \vee (F_2 \wedge G_2) \vee (L_2 \wedge G_3) \vee$ $\vee (L_1 \wedge G_2) \vee (F_1 \wedge G_3)$	$G_1'+F_2'\cdot G_2'+L_2'\cdot G_3'+L_1'\cdot G_2'-L_1'\cdot F_2'\cdot G_2' +$ $+F_1'\cdot G_3'-F_1'\cdot L_2'\cdot G_3'$
6	$G_1 \vee (F_2 \wedge G_2) \vee (L_2 \wedge G_3) \vee$ $\vee (L_1 \wedge G_2) \vee (F_1 \wedge G_3) \vee (L_1 \wedge F_1)$	$G_1'+F_2'\cdot G_2'+L_2'\cdot G_3'+L_1'\cdot G_2'-L_1'\cdot F_2'\cdot G_2'+$ $+F_1'\cdot G_3'-F_1'\cdot L_2'\cdot G_3'+L_1'\cdot F_1'-L_1'\cdot F_1'\cdot G_1'-$ $-L_1'\cdot F_1'\cdot G_2'-L_1'\cdot F_1'\cdot G_3'$

Fig. 2-4. Table of equivalence between boolean expression and arithmetical expression (Example).

From the table of Fig. 2-4 we get

$$\begin{aligned} TOP' = {} & G_1'+F_2'\cdot G_2'+L_2'\cdot G_3'+L_1'\cdot G_2'-L_1'\cdot F_2'\cdot G_2'+F_1'\cdot G_3'- \\ & -F_1'\cdot L_2'\cdot G_3'+L_1'\cdot F_1'-L_1'\cdot F_1'\cdot G_1'-L_1'\cdot F_1'\cdot G_2'-L_1'\cdot F_1'\cdot G_3' \end{aligned} \tag{2-43}$$

The expression 2-43 is called structure function of the TOP.

By taking the expectations of both sides of Eq. 2-43 and by taking into account Eq. 2-39, we get

$$\begin{aligned} E\{TOP\} = {} & E\{G_1'\} + E\{F_2'\cdot G_2'\} + E\{L_2'\cdot G_3'\} + E\{L_1'\cdot G_2'\} - \\ & - E\{L_1'\cdot F_2'\cdot G_2'\} + E\{F_1'\cdot G_3'\} - E\{F_1'\cdot L_2'\cdot G_3'\} + \\ & + E\{L_1'\cdot F_1'\} - E\{L_1'\cdot F_1'\cdot G_1'\} - E\{L_1'\cdot F_1'\cdot G_2'\} - \\ & - E\{L_1'\cdot F_1'\cdot G_3'\} \end{aligned} \tag{2-44}$$

Going back to the primary boolean variables, Eq. 2-44 finally becomes

$$E\{TOP\} = E\{G_1\} + E\{F_2 \wedge G_2\} + E\{L_2 \wedge G_3\} + E\{L_1 \wedge G_2\} - E\{L_1 \wedge F_2 \wedge G_2\} + E\{F_1 \wedge G_3\} - E\{F_1 \wedge L_2 \wedge G_3\} + E\{L_1 \wedge F_1\} - E\{L_1 \wedge F_1 \wedge G_1\} - E\{L_1 \wedge F_1 \wedge G_2\} - E\{L_1 \wedge F_1 \wedge G_3\} \quad (2\text{-}45)$$

Eq. 2-45 can also be obtained by taking the expectation of both sides of Eq. 2-42 and by applying systematically either the rule given by Eq. 2-22 in the general case or the rule given by Eq. 2-27 if the two variables are mutually exclusive.

One important point is that the boolean function must be first developed in a normal disjunctive form.

We first define what we understand by normal disjunctive form of a boolean function. In the following primary variables will be also called literals. A boolean function can be expressed in the form of a disjunction of conjunctions of literals (disjunctive form). A conjunction of literals belonging to a disjunctive form of a boolean function will be called shortly "monomial". A monomial X of a disjunctive form of a boolean function (TOP) is said to be an implicant of the boolean function because it implies it. If X is an implicant of the TOP, it must satisfy the following boolean identity.

$$TOP \wedge X = X \quad (2\text{-}46)$$

Let X_j and X_k be two monomials. We say that X_k subsumes X_j if every literal of X_j is contained in X_k. This is the same as saying that X_k is an implicant of X_j, that is

$$X_j \wedge X_k = X_k \quad (2\text{-}47)$$

We can give now the definition of normal disjunctive form of a boolean function

"A disjunctive form of a boolean function will be called normal disjunctive form if its monomials satisfy the following four properties.

1. Each monomial (X) must be a non-zero monomial ($X \neq 0$, i.e. no pair of mutually exclusive literals must be contained in it).

2. Each monomial must not contain any literal more than once (no repeated literals).

3. Monomials must not subsume pairwise each other. ($X_j \neq X_j \wedge X_k \neq X_k$)

4. Monomials must not contain negated literals."

If a boolean function contains a negated literal (say $\bar{A}_i$), this must be replaced by the disjunction of all remaining literals belonging to the same primary component, that is (Eq. 1-36).

$$\bar{A}_i = \bigvee_{k=1}^{n} A_k \qquad k \neq i \quad (i=1,2,\ldots,n) \tag{2-48}$$

where n = total number of literals belonging to primary component A.

A boolean function can have in general many normal disjunctive forms. For a given fault tree, there is a particular normal disjunctive form of its TOP variable which is associated with that fault tree. We shall call it "associated normal disjunctive form."

We notice that Eq. 2-42 satisfies the requirements of the definition of normal disjunctive form.

We can therefore state the following rule (Rule No. 3)

"If a boolean function (TOP) is given in a normal disjunctive form, that is

$$TOP = \bigvee_{j=1}^{N} X_j \tag{2-49}$$

where

the X_j are non zero monomials with no repeated literals and with no negated literals and which do not subsume pairwise each other,

and

N = total number of monomials

its expected value is given by the following equation

$$E\left\{TOP\right\} = \sum_{j=1}^{N} E\left\{X_j\right\} + (-1)^1 \sum_{j=2}^{N} \sum_{k=1}^{j-1} E\left\{X_j \wedge X_k\right\} +$$

$$+ (-1)^2 \sum_{j=3}^{N} \sum_{k=2}^{j-1} \sum_{s=1}^{k-1} E\left\{X_j \wedge X_k \wedge X_s\right\} + \cdots \cdot \quad (2\text{-}50)$$

$$\cdots + (-1)^{N-1} E\left\{\bigwedge_{j=1}^{N} X_j\right\}$$

Note that Eq. 2-50 is equivalent to the very well known equation of the probability of the union of events / 21 /.

Note that the boolean expressions under brackets are all monomials because they are generated from conjunctions of monomials.

The original non zero monomials X_j will be called first order monomials. The other monomials will be called second order, third order monomials etc., if they are generated respectively from the conjunction of two, three etc. monomials of the first order.

One important point is that a monomial of order greater than one may be a zero monomial. This happens if the monomial contains at least one pair of mutually exclusive literals. In this case the monomial is deleted because its expectation is equal to zero.

We can now apply the rule given by Eq. 2-50 to Eq. 2-42. We have

$$E\left\{TOP\right\} = E\left\{G_1\right\} + E\left\{F_2 \wedge G_2\right\} + E\left\{L_2 \wedge G_3\right\} + E\left\{L_1 \wedge G_2\right\} +$$

$$+ E\left\{F_1 \wedge G_3\right\} + E\left\{L_1 \wedge F_1\right\} - \Big[E\left\{G_1 \wedge L_1 \wedge F_1\right\} +$$

$$+ E\left\{F_2 \wedge L_1 \wedge G_2\right\} + E\left\{L_2 \wedge F_1 \wedge G_3\right\} + E\left\{L_1 \wedge G_2 \wedge F_1\right\} +$$

$$+ E\left\{F_1 \wedge L_1 \wedge G_3\right\} \Big] \qquad (2\text{-}51)$$

Eq. 2-51 is identical with Eq. 2-45.

3. COMPONENTS AND CONDITIONAL EXPECTATION OF BOOLEAN VARIABLES.

3.1 Definition of component. Logical and statistical independence.

In section 1 we have defined primary components and primary variables. We want now to give a more general definition of component.

> "A set of boolean variables $A_1; A_2;...; A_n$ constitute a component, if the variables satisfy the two restriction types, namely

Restriction type 1

$$\bigvee_{i=1}^{n} A_i = 1 \qquad (3\text{-}1)$$

and

Restrictions type 2

$$A_i \bigwedge A_j = 0 \qquad i \neq j \qquad (3\text{-}2)$$

$$(i,j = 1,2,..,n)$$

If all variables A_i belonging to a component are primary variables, the component is a primary component.

In the following primary variables will also be called literals, for short. We recall again the definition of logical independence.

> "Two boolean variables (say A_i and B_k) are said to be mutually logically independent if each variable can take each value of its domain of definition independently of the value previously assigned to the other variable."

Taking into account the restrictions among literals belonging to the same primary component, it follows (corollary)

> "Two literals (primary variables) are logically independent of each other if they belong to two different primary components"

Taking into account the above definition and associated corollary on logical independence, one can also state the following

> "Two boolean function (say A_i and B_k) are said to be logically independent of each other if the literals contained in the first function belong to primary components which are different from the primary components whose literals appear in the second boolean function."

In other words the primary components appearing in the first boolean function must all be different from those appearing in the second boolean function.

We come now to the definition of logical independence among components.

> "Two components are said to be mutually logically independent if the boolean variables belonging to the first component are pairwise mutually logically independent of the boolean variables of the second component."

We introduce now the definition of conditional expectation of a boolean variable with respect to another variable.

We consider the contitional probability of the event $\{B_k = 1\}$ given the event $\{A_i = 1\}$. Taking into account the definition of the expectation of a stochastic boolean variable given in chapter 2, we can write

$$P\{B_k=1 \mid A_i=1\} = \frac{P\{B_k \wedge A_i=1\}}{P\{A_i=1\}} = \frac{E\{B_k \wedge A_i\}}{E\{A_i\}} \qquad (3\text{-}3)$$

We consider now the truth table of the variable $B_k \wedge A_i$ and we delete all the rows for which $\{A_i = 0\}$. We call this the reduced truth table. In addition we associate with each survived row a normalized occurrence probability which is equal to the occurrence probability of the elementary event associated with the row devided by the occurrence probability of the event $\{A_i = 1\}$. The conditional probability $P\{B_k=1 \mid A_i=1\}$ is obviously equal to the sum of the normalized occurrence probabilities associated with the elementary events for which $\{B_k=1\}$. On the other hand the reduced truth table with associated normalized probabilities can be understood as the truth table with associated probabilities of a new stochastic boolean variable which we indicate with the notation $B_k \mid A_i$ and which we call conditioned variable. Since the sets $\{B_k=1 \mid A_i=1\}$ and $\{(B_k \mid A_i)=1\}$ contain the same elementary events we obviously have

$$\{B_k = 1 \mid A_i = 1\} \equiv \{(B_k \mid A_i) = 1\} \qquad (3\text{-}4a)$$

and

$$P\{B_k = 1 \mid A_i=1\} = P\{(B_k \mid A_i) = 1\} \qquad (3\text{-}4b)$$

We recall now the definition of a stochastic boolean variable given in chapter 2 and we can write

$$E\left\{B_k \mid A_i\right\} = P\left\{(B_k \mid A_i) = 1\right\} \qquad (3\text{-}4c)$$

From Eqs. 3-4b and 3-4c we get

$$E\left\{B_k \mid A_i\right\} = P\left\{B_k = 1 \mid A_i = 1\right\} \qquad (3\text{-}5a)$$

Eq. 3-5a is equivalent to the following statement

> "The expectation of the conditioned variable $B_k|A_i$ is equal to the conditional probability of the event $\{B_k=1\}$ given the event $\{A_i=1\}$ ".

From Eqs. 3-3 and 3-5ait follows

$$E\left\{B_k \mid A_i\right\} = \frac{E\left\{B_k \wedge A_i\right\}}{E\left\{A_i\right\}} \qquad (3\text{-}5b)$$

Eq. 3-5b is equivalent to the following statement

> "Given two stochastic boolean variables (say A_i and B_k) the expectation of the conditioned variable $B_k|A_i$ is equal to the ratio between the expectation of the conjunction of the two variables $(B_k \wedge A_i)$ and the expectation of the variable A_i".

In the following we shall use the more convenient expression "conditional expectation of B_k given A_i" instead of the expression "expectation of the conditioned variable $B_k \mid A_i$".

We can now introduce the definition of statistical independence among stochastic boolean variables.

> "Two stochastic boolean variables (say A_i and B_k) are said to be mutally statistically independent if the expectation of their conjunction is equal to the product of the expectations of each variable."

This is equivalent to writing

$$E\left\{A_i \wedge B_k\right\} = E\left\{A_i\right\} \cdot E\left\{B_k\right\} \qquad (3\text{-}6)$$

From Eqs.3-5a and 3-5b it follows immediately that, if two boolean functions A_i and B_k are mutually statistically independent, the conditional expectation of one variable given the other is equal to the expectation of the same variable. This is equivalent to writing

$$E\left\{ B_k \mid A_i \right\} = E\left\{ B_k \right\} \qquad (3\text{-}7a)$$

and

$$E\left\{ A_i \mid B_k \right\} = E\left\{ A_i \right\} \qquad (3\text{-}7b)$$

It is important to point out that a necessary condition for two variables to be mutually statistically independent is that they are already mutually logically independent.

We come now to the definition of mutual statistical independence among components.

> "Two components are said to be mutually statistically independent if the boolean variables of the first component are pairwise mutually statistically independent of the variables of the second component."

If two components are mutually statistically independent, they are also mutually logically independent. However, if they are mutually logically independent, they are not necessarily mutually statistically independent.

We give now the definition of statistically independent component

> "A component is said to be statistically independent if it is pairwise mutually statistically independent of each primary component of the system, whose literals do not appear in the variables of the component".

A component which is not independent is said to be dependent.

3.2 A theorem on the conditional expectation.

Three boolean variables namely Z_j, I_k and X_s are such that

(1) a variable Y_q exists which satisfies the following boolean equation

$$Y_q \wedge I_k = X_s \wedge I_k \qquad (3\text{-}8)$$

(2) Y_q is statistically independent of I_k as well as of Z_j^q that is

$$E\left\{X_s \wedge I_k\right\} = E\left\{Y_q \wedge I_k\right\} = E\left\{Y_q\right\} \cdot E\left\{I_k\right\} \qquad (3\text{-}9)$$

and

$$E\left\{Z_j \wedge Y_q\right\} = E\left\{Y_q\right\} \cdot E\left\{Z_j\right\} \qquad (3\text{-}10)$$

If the Eqs. 3-8 to 3-10 hold, the expectation of Z_j given $I_k \wedge X_s$ is equal to the expectation of Z_j given I_k. This is equivalent to writing

$$E\left\{Z_j \mid I_k \wedge X_s\right\} = E\left\{Z_j \mid I_k\right\} \qquad (3\text{-}11)$$

To demonstrate that Eq. 3-11 holds, we start by making the conjunction of both sides of Eq. 4-1 with Z_j. We get

$$Z_j \wedge Y_q \wedge I_k = Z_j \wedge X_s \wedge I_k \qquad (3\text{-}12)$$

By taking the expectation of both sides of Eq. 3-12 we get

$$E\left\{Z_j \wedge Y_q \wedge I_k\right\} = E\left\{Z_j \wedge X_s \wedge I_k\right\} \qquad (3\text{-}13)$$

Taking into account Eqs. 3-9 and 3-10 and the definition of conditional expectation (eq. 3-3), we have

$$E\left\{Z_j \wedge Y_q \wedge I_k\right\} = E\left\{Y_q\right\} \cdot E\left\{Z_j \mid I_k\right\} \cdot E\left\{I_k\right\} \qquad (3\text{-}14)$$

In addition we have obviously

$$E\left\{Z_j \wedge X_s \wedge I_k\right\} = E\left\{Z_j \mid X_s \wedge I_k\right\} \cdot E\left\{X_s \wedge I_k\right\} \qquad (3\text{-}15)$$

Taking into account Eqs. 3-14 and 3-15, Eq. 3-13 becomes

$$E\left\{Z_j \mid I_k\right\} \cdot E\left\{Y_q\right\} \cdot E\left\{I_k\right\} = E\left\{Z_j \mid X_s \wedge I_k\right\} \cdot E\left\{X_s \wedge I_k\right\} \qquad (3\text{-}16)$$

Taking into account Eq. 3-9, Eq. 3-16 finally becomes

$$E\left\{Z_j \mid I_k\right\} = E\left\{Z_j \mid X_s \wedge I_k\right\} \qquad (3\text{-}17)$$

which is identical with Eq. 3-11.

4. STATE ANALYSIS.

4.1 Generalities. State Diagrams. Product of components.

The most direct way to calculate the occurrence probability of the event $\{ TOP = 1 \}$ is the state analysis.

Fig. 4-1 shows a fault tree which is identical with that of Fig. 1-4. Its truth table is shown in Fig. 4-2 and is idential with that of Fig. 1-8. Each row of the truth table is an elementary state of the system under consideration.

In chapter 1 we have seen that each elementary state of the system can be represented by the cartesian product of the states occupied by each individual primary component (smallest form of system elementary state). In addition we have also seen that there is a one to one correspondence between smallest forms of elementary states and complete monomials.

Fig. 4-3 shows the so called table of system elementary states with the corresponding values of the TOP variable in the last column. Each row of the table corresponds to an elementary state of the system. Let us consider for instance the row number 7. The plus sign in the column A_3 means that primary component A occupies state a_3, that is

$$a_3 = \left\{ A_3 = 1 \right\} \tag{4-1}$$

Let us indicate with s_i a generic elementary state of the system and with S_i its associated boolean variable. From the row number 7 of Fig. 4.2 we get

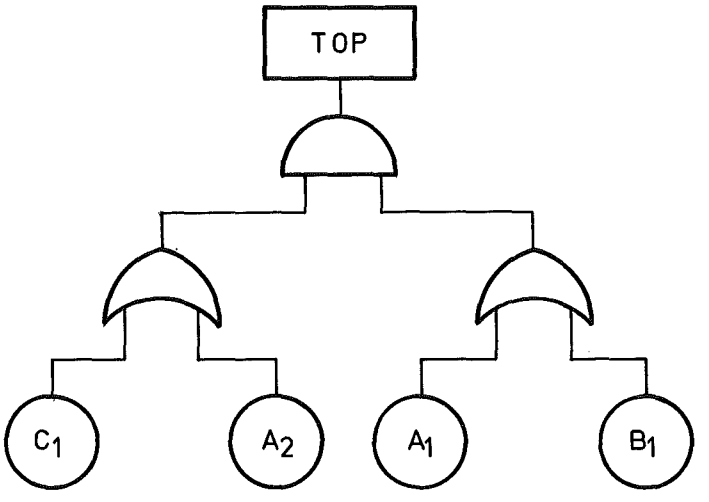
$$s_7 = a_3 \times b_1 \times c_1 \tag{4-2}$$

and therefore

$$S_7 = A_3 \wedge B_1 \wedge C_1 \tag{4-3}$$

It is important to point out that the set of the variables S (i=1,2,..,n) constitute a component because the variables S_i satisfy the restrictions. The complete set of states (state space) can be represented in a diagramatic form by a state diagram. Fig. 4-4 shows a state diagram in the case of the system whose table of states is given in Fig. 4-3 (n=12). Each circle indicates a state. The symbol of the variable associated with a particular state is marked inside the circle corresponding to the state under consideration. A line connecting two circles indicates the transition from one state to the other. The arrow on the line indicates the direction of the transition.

Two states are said to be mutually communicable (or mutually accessible) if each one of the two states is directly accessible



Primary Component	Number of States
A	3
B	2
C	2

$$TOP = (C_1 \vee A_2) \wedge (A_1 \vee B_1)$$

Fig. 4-1. Fault Tree.

Row Number	Inputs				Output
	A_1	B_1	C_1	A_2	TOP
1	0	0	0	0	0
2	0	0	0	1	0
3	0	0	1	0	0
4	0	0	1	1	0
5	0	1	0	0	0
6	0	1	0	1	1
7	0	1	1	0	1
8	0	1	1	1	1
9	1	0	0	0	0
10	1	0	1	0	1
11	1	1	0	0	0
12	1	1	1	0	1

Fig. 4-2. Truth Table of the fault tree of Fig. 4-1.

State Number	Primary Components							TOP
	A			B		C		
	A_1	A_2	A_3	B_1	B_2	C_1	C_2	
1			+		+		+	0
2		+			+		+	0
3			+		+	+		0
4		+			+	+		0
5		+		+			+	0
6		+		+			+	1
7			+	+		+		1
8		+		+		+		1
9	+				+		+	0
10	+				+	+		1
11	+			+			+	1
12	+			+		+		1

Fig. 4-3. Table of system elementary states. (Fault tree of Fig. 4-1)

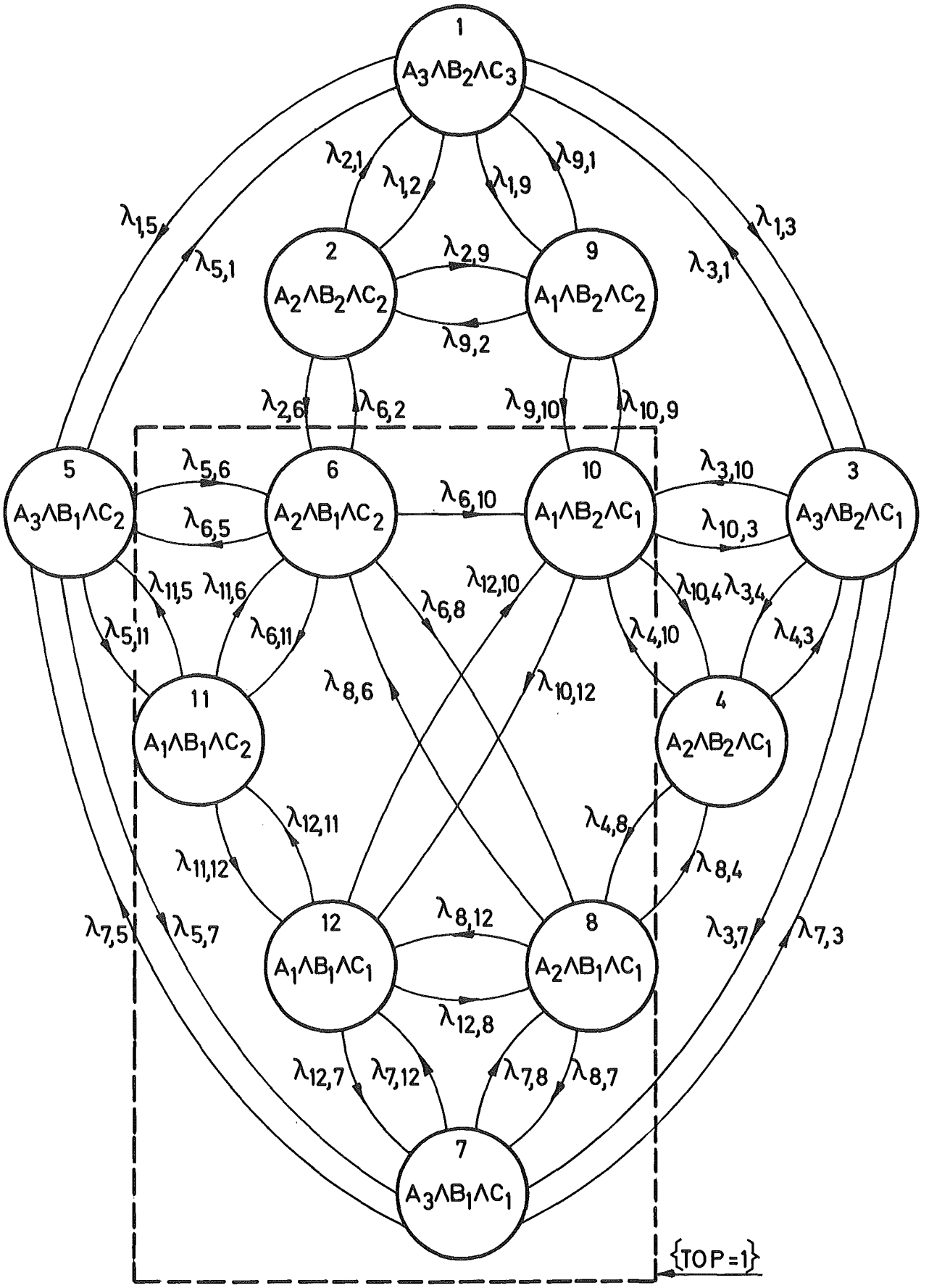


Fig. 4-4: State Diagram (Fault Tree of Fig.4-1)

from the other by means of only one transition. In this case the corresponding circles in the state diagram are linked to each other by two lines (one for each direction).

Two states are said to be unidirectionally communicable (unidirectionally accessible) if only one of the two states is directly accessible from the other by only one transition. In this case the corresponding circles in the state diagram are linked to each other by only one line with an arrow indicating the direction of the only possible transition.

Finally two states are said to be mutually incommunicable (or mutually inaccessible) if neither of the two states is directly accessible from the other by means of only one transition. In this case the corresponding circles in the state diagram are not directly connected by any line.

In the state diagram of Fig. 4-4 the states s_2 and s_3 are mutually inaccessible and the states s_6 and s_{10} are unidirectionally accessible (s_{10} is directly accessible from s_6 but, s_6 is not directly accessible from s_{10}). Finally the states s_1 and s_3, are mutually accessible.

Note that there are transitions (like that from state s_1 to s_3 in Fig. 4-4) in which only one primary component changes its state and transitions in which more primary components change their state simultaneously. For instance, in the transition from s_6 to s_{10} all three primary components change their state simultaneously.

In the above example we have assumed that the components A; B and C are primary components. This assumption is however not necessary. We can also assume that A; B and C are in general not primary components. We shall say that component S is obtained by multiplying the components A; B and C and we shall write

$$S = A\pi\ B\pi C \tag{4-4}$$

where the symbol π indicates the operation of product among components. The operation of multiplication (product) among components means in practice to generate the state diagram of a new component (super component) from the state diagrams of some given components, which are called factor components. Each state of the new state diagram is characterized by a variable which is a non zero monomial containing a number of factor variables equal to that of factor components. The total number of states of the super component is equal to the product of the number of states of all factor components.

With reference to the state diagram of Fig. 4-4 state s_{10} of component S is associated with the variable S_{10} which is a monomial obtained by the conjunction of the parent variables A_1; B_2 and C_1

$$S_{10} = A_1 \wedge B_2 \wedge C_1 \tag{4-5}$$

In the following we shall indicate a state of a component by means of its associated variable. In saying that, we mean that the state is equal to the value 1 of its associated variable. We can therefore completely forget the set theory and handle our problems by using only the boolean algebra with restrictions on variables. This formalism facilitates enormously the possibility to combine fault tree analysis with state analysis.

In accordance with the new formalism, the occurrence probability of a state will be replaced by the expectation of the corresponding boolean variable. For instance we have:

$$P_7(t) = P\left\{\text{Component S occupies state } s_7 \text{ at } t\right\} = P\left\{S_7=1 \text{ at } t\right\} =$$

$$= P\left\{S_7(t) = 1\right\} = E\left\{S_7(t)\right\} = E\left\{A_3 \wedge B_1 \wedge C_1 \text{ at } t\right\} \quad (4\text{-}6)$$

We shall call the stochastic process the set of probability laws governing the transitions from each state to any other state of the state space. These probability laws must be specified in such a way that the occurrence probability of each event as a function of time can be uniquely calculated.

We shall limit ourselves to the case of Markow processes continuous in time and with a finite number of states /13,15/. This process is completely defined if the so called instantaneous transition rates are known functions of time and the occurrence probabilities of each event at the initial time (t = 0) are also known. The instantaneous transition rate $\lambda_{ij}(t)$ from state s_i to state s_j ($i \neq j$) can be defined by the following eqation

$$\lambda_{ij}(t) = \lim_{dt \to o} \frac{1}{dt} \; P\left\{\text{Component S occupies state } s_j \text{ at } t+dt \;\middle|\; \text{System occupies state } s_i \text{ at } t\right\} \quad (4\text{-}7)$$

By using the new notation, Eq. 4-7 can be written as follows

$$\lambda_{ij} = \lim_{dt \to o} \frac{1}{dt} \; E\left\{S_j(t+dt) \;\middle|\; S_i(t)\right\} \quad (4\text{-}8)$$

If states s_i and s_j are mutually inaccessible the two corresponding transition rates are equal to zero, that is

$$\lambda_{ij} = \lambda_{ji} = 0 \quad (4\text{-}9)$$

If states s_j and s_i are unidirectionally accessible and exactly s_j is directly accessible from s_i but not s_i from s_j, we have instead

$$\lambda_{ji} = 0 \qquad (4\text{-}10)$$

and

$$\lambda_{ij} \neq 0 \qquad (4\text{-}11)$$

In a state diagram (e.g. Fig. 4-4) the transient rates λ_{ij} are written near their corresponding connecting lines. If a transition rate is equal to zero, its corresponding line in the state diagram can be deleted.

With reference to state s_i we shall say that the transition rate λ_{ij} is a departure transition rate and the failure rate λ_{ij} is an arrival transition rate.

In the following we shall assume that the transition rates can take only finite values and that they are regular functions of the time (without discontinuities). It is known from the literature /13,15/ that under the above hypothesis a system of n first order linear differential equations linking the occurrence probabilities of the states to the transition rates can be written.

We first introduce the shorter symbol E_i defined as follows

$$E_i = E\left\{S_i\right\} \qquad i=1,2,..,n \qquad (4\text{-}12)$$

The n first order linear differential equations can be written as follows

$$\frac{dE_i}{dt} = \sum_{j=1}^{n} \lambda_{ji} E_j - E_i \sum_{j=1}^{n} \lambda_{ij} \qquad (i\neq j) \quad i,j=1,2,\ldots,n \qquad (4\text{-}13)$$

Eq. 4-13 refers to state s_i. Note the particular way in which Eq. 4-13 is written. The derivative of E_i is given by the difference between two terms. The first term is equal to the sum of the expectations of the other variables of the state diagram, each expectation being multiplied by the corresponding arrival transition rate λ_{ji}. The second term is simply given by the expectation of the variable associated to the state s_i multiplied by the sum of all departure transition rates λ_{ij}.

Note that only n-1 out of n equations are independent. In fact the expectations E_i must also satisfy the first type restriction (Eq. 2-36), that is

$$\sum_{i=1}^{n} E_i = 1 \qquad (4\text{-}14)$$

The system of equations made of Eq. 4-14 and of n-1 out of n differential equations (Eqs. 4-13) can be uniquely solved if the initial values E_{io} at time t=0 of each E_i are also known. The methods of solving a system of first order linear differential equations are well known in the literature especially in the usual case in which the transition rates are constant with time (homogeneous Markow process). In this last case the Laplace transformation method can be applied. The general solution can be expressed as a sum of exponential functions. We shall not go into detail here because these are very well known methods which the reader can learn from the usual textbooks on linear differential equations.

We shall only point out that the asymptotic values $E_{i\infty}$ ($t\to\infty$) can be directly obtained (without solving the system of differential equations) by putting in Eqs. 4-13 all $dE_i/dt=0$ and all $\lambda_{ij} = \lambda_{ij\infty}$ ($t\to\infty$). In this case the system of first order linear differential equations is reduced to a system of first order algebraic equations. The roots of the system of algebraic equations can be found by means of Cramer's rule (with the determinants). This method is also very well known and therefore will not be discussed here. Note that the initial values E_{io} are not needed if one is interested in the asymptotic solution only.

State analysis is a very general method which can be used in principle to calculate the occurrence probability of any event associated with a complex system. However, due to the enormous number of elementary states (which a complex system usually has), it cannot be applied in practice. It is instead applied to calculate the expectation of the primary variables of a fault tree because the number of states of a primary component is usually very small.

Eq. 4-13 can be written as follows

$$\frac{dE_i}{dt} = \sum_{j=1}^{n} J_{ji} - E_i \Lambda_i \qquad i\neq j \quad i;j= 1,2...;n \qquad (4\text{-}15)$$

where

$$J_{ji} = \lambda_{ji} E_j = \underline{\text{inlet flow to } s_i \text{ from } s_j} \qquad (4\text{-}16)$$

and

$$\Lambda_i = \sum_{\substack{j=1 \\ j\neq 1}}^{n} \lambda_{ij} = \underline{\text{total departure transition rate from } s_i} \qquad (4\text{-}17)$$

Note that the quantity J_{ji} is called outlet flow from s_j to s_i if we refer to the equation of state s_j.

Another way of writing Eq. 5-13 is of course the following

$$\frac{dE_i}{dt} = \sum_{j=1}^{n} (J_{ji} - J_{ij}) \quad i \neq j \qquad i = 1; 2 \ldots; n \tag{4-18}$$

where the quantity $J_{ji} - J_{ij}$ is called net inlet flow to s_i from s_j. The quantity $J_{ij} - J_{ji}$ is called net outlet flow from s_i to s_j.

4.2 Condensation and expansion of state diagrams. Parent primary components. Definition of the arbitrary binary component.

We want to discuss first the operation of condensation. The operation of condensation consists in lumping together in a single state some states of a state diagram. The new state generated by the condensation of these states is called macrostate. The condensation laws are very simple. If s_k and s_q are two states which have to be condensed, the macrostate s_{k+q} replaces the two old states in the new state diagram. The transition rates λ_{kq} and λ_{qk} do not appear in the new state diagram.

The arrival transition rates of the two states s_k and s_q from the same state s_j must be lumped (summed) together to give the transition rate from state s_j to state s_{k+q}, namely

$$\lambda_{j(k+q)} = \lambda_{jk} + \lambda_{jq} \tag{4-19}$$

The departure transition rate of the new state s_{k+q} to state s_j is given by the following equation

$$\lambda_{(k+q)j} = \frac{\lambda_{kj}E_k + \lambda_{qj}E_q}{E_k + E_q} \tag{4-20}$$

It is easy to prove that if one applies the Eqs. 4-19 and 4-20, the new system of linear differential equations is of order n-1 and is consistent with the original one. This means that both systems give the same solution for the occurrence probabilities of each state with the exception of course of the two states which have been condensed. It can also easily be shown that the occurrence probability of the macrostate s_{k+q} is equal to the sum of the occurrence probabilities of its predecessors, that is

$$E_{k+q} = E_k + E_q \tag{4-21}$$

Eq. 4-21 can be understood as a relationship between the expectation of the variable associated with the macrostate and the expectations of the variables associated with the old states. The boolean relationship between the new variable and the old variables is obviously the following

$$S_{k+q} = S_k \vee S_q \tag{4-22}$$

Eq. 4-20 tell us that the new transition rate $\lambda_{(k+q)j}$ is in general a function of the quantities E_k and E_q which are unknown. It follows that the method of condensation of states can be profitably applied in the cases in which the unknown E_k and E_q can be eliminated from Eq. 4-20. For instance in the special case

$$\lambda_{kj} = \lambda_{qj} = \lambda \tag{4-23}$$

Eq. 4-20 gives simply

$$\lambda_{(k+q)j} = \lambda = \text{known quantity} \tag{4-24}$$

Another example is that in which, due to a symmetry in the state diagram, it is possible to deduce that

$$E_k = E_q \tag{4-25}$$

Taking into account Eq. 4-25, Eq. 4-20 becomes

$$\lambda_{(k+q)j} = (\lambda_{kj} + \lambda_{qj})/2 = \text{known quantity} \tag{4-26}$$

In this case too it is convenient to condense the states s_k and s_q.

The condensation rules can be expressed in terms of equations among flows. Eqs. 4-19 and 4-20 become respectively

$$J_{j(k+q)} = J_{jk} + J_{jq} \tag{4-27}$$

and

$$J_{(k+q)j} = J_{jk} + J_{qj} \tag{4-28}$$

We consider now the case of the condensation of m states with $m \geq 2$. We can indicate with s_i $(i = 1;2...;m)$ the states of a state diagram which we want to condense in a single macrostate $(s_{1+2...;+m})$ and with s_j $(j = m+1;\ m+2...;n)$ the remaining states. The boolean variable associated with the macrostate is given by the disjunction of the variables associated with the states which are being condensed. We have the first condensation rule:

$$S_{1+2+..;+m} = \bigvee_{i=1}^{m} S_i \tag{4-29}$$

The inlet flow to the macrostate from state s_j is given by the sum of the inlet flows from state s_j to the states which are being condensed. This is called the second condensation rule and is written as follows.

$$J_{j(1+2+..;+m)} = \sum_{i=1}^{m} J_{ji} \tag{4-30}$$

Finally the outlet flow from the macrostate to state s_j is equal to the sum of the outlet flows from the condensing states towards state s_j (third condensation rule)

$$J_{(1+2\ldots;+m)j} = \sum_{i=1}^{m} J_{ij} \qquad (4\text{-}31)$$

In conclusion, by condensing the states of a system S, one can generate new state diagrams. Each one of these state diagrams can be thought of as the state diagram of a component whose variables are in general boolean functions of some of the primary variables of the system. The variables of this component obviously satisfy the two restriction types (Eqs. 3-1 and 3-2).
Let us now consider the boolean expression of a variable of a component. A literal appearing in the boolean function is said to be parent to the variable, and the primary component to which the literal belongs is said to be parent to the component under consideration.

If we recall the definition of mutual logical independence (section 3.1), we can state the following

"Two mutually logically independent components have no primary parent component in common."

The operation of expansion is complementary to that of condensation. Here a macrostate is dissected (expanded) into two or more states. In the case of the expansion of a state into two states, Eqs. 4-27 and 4-28 must also be applied but in the reverse direction. Note that in this case the problem is not completely defined. In fact, given a value for $J_{j(k+q)}$ there is an infinite number of pairs of values for J_{jk} and J_{jq} which satisfy Eq. 4-27. The same can be said for J_{kj} and J_{qj} in the case of Eq. 4-28. Since Eq. 4-22 must also be satisfied, the new boolean variables can be expressed as follows

$$S_k = S_{k+q} \wedge X_1 \qquad (4\text{-}32)$$

and

$$S_q = S_{k+q} \wedge X_2 \qquad (4\text{-}33)$$

where X_1 and X_2 must obviously satisfy the two boolean identities

$$X_1 \vee X_2 = 1 \quad (\text{because } S_k \vee S_q = S_{k+q}) \qquad (4\text{-}34)$$

and

$$X_1 \wedge X_2 = 0 \quad (\text{because } S_k \wedge S_q = 0) \qquad (4\text{-}35)$$

This means that X_1 and X_2 belong to a binary component. If we want to expand a macrostate into "m" states, we have first to define a new component, characterized by m variables. Each new state is characterized by a variable which results from the conjunction between the variable associated with the macrostate and one of the variables of the new component. The new flows must be chosen in such a way that, by recondensing the m states again into the macrostate, one finds again the original state diagram (with the same flows).

From the above discussion we can state the following rule for the operation of expansion.

"To expand a variable A_j (associated to a state a_j of s given state diagram) with respect to a component X means to generate a number of new states equal to the number of variables of component X, each new state being characterized by a variable given by the conjunction of the original variable A_j with one variable of component X. The stochastic properties of component X must be such that by recondensing the new variables into the original variable A_j (i.e. the new states into the macrostate) one finds again the original state diagram (with the same flows)."

We want to give an example now.

The state diagram 1 of Fig. 4-6 refers to the binary component A. The state diagram 4 of Fig. 4-6 is the original state diagram 1 expanded into four states. The expansion can be carried out in one step alone. However, in order to better illustrate the method, we shall carry out the expansion in two successive steps. Two path are possible, namely the path 1-2-4 and the path 1-3-4. Both paths are shown in Fig. 4-6. We shall follow the path 1-2-4.

By comparing the state diagrams 1 and 2, one can write the following two equations

$$\sigma' + \sigma'' = \sigma \qquad \text{(by applying Eq. 4-30)} \tag{4-36}$$

and (by applying Eq. 4-31)

$$\rho' E\{A_1 \wedge X_1\} + \rho'' E\{A_1 \wedge X_2\} = \rho E\{A_1\} \tag{4-37}$$

By applying the same procedure between the state diagrams 2 and 4, we get

$$\lambda_{31} E\{A_2 \wedge X_1\} + \lambda_{41} E\{A_2 \wedge X_2\} = \rho' E\{A_2\} \tag{4-38}$$

$$\lambda_{13} + \lambda_{14} = \rho' \tag{4-39}$$

$$\lambda_{23} + \lambda_{24} = \rho'' \tag{4-40}$$

$$\lambda_{42} E\{A_2 \wedge X_2\} + \lambda_{32} E\{A_2 \wedge X_1\} = \sigma'' E\{A_2\} \tag{4-41}$$

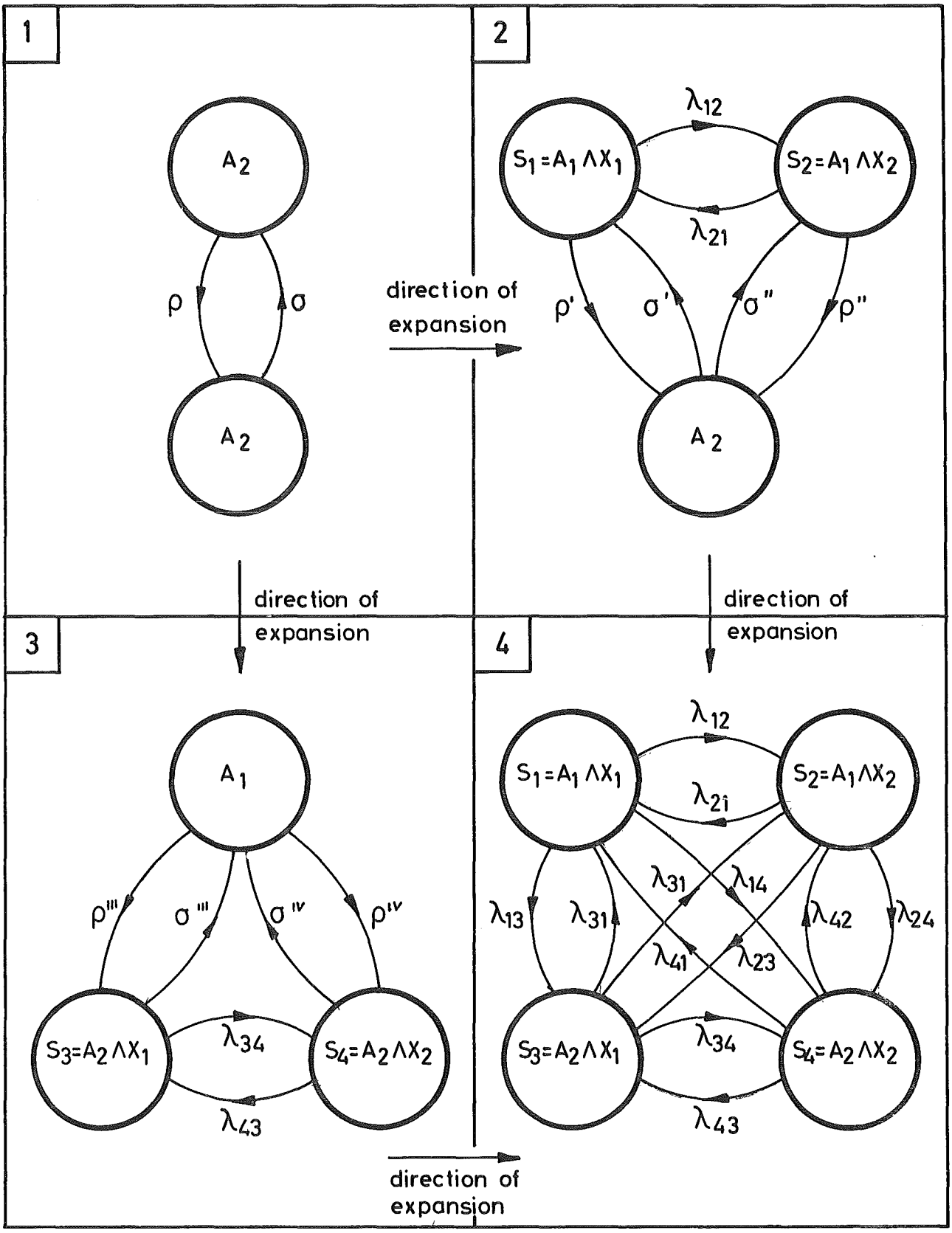


Fig. 4-6: Method of Expansion. An Example.

By adding Eq. 4-41 to El. 4-38 and by taking into account Eq. 4-36, we get

$$(\lambda_{31} + \lambda_{32})\ E\{A_2 \wedge X_1\} + (\lambda_{41} + \lambda_{42})E\ \{A_2 \wedge X_2\} = \rho\ E\ \{A_2\} \quad (4\text{-}42)$$

By repalcing in Eq. 4-37 ρ' and ρ'' by means of Eqs. 4-39 and 4-40, we get

$$(\lambda_{13} + \lambda_{41})E\ \{A_1 \wedge X_1\} + (\lambda_{23} + \lambda_{24})\ E\{A_1 \wedge X_2\} = \rho\ E\ \{A_1\} \quad (4\text{-}43)$$

Eqs. 4-42 and 4-43 are the only conditions which the transition rates of the state diagram 4 must satisfy because of the expansion.

Let us consider now the state diagram of Fig. 4-7 which has been derived from the state diagram of Fig. 4-4 by lumping together (condensing) some states. Here the binary component X has been introduced which is characterized by the two variables defined as follows

$$X_1 = B_1 \wedge C_1 \quad (4\text{-}44)$$

and

$$X_2 = \overline{X}_1 = B_2 \vee C_2 \quad (4\text{-}45)$$

The state diagram of Fig. 4-7 has 6 states whose variables are:

$$S_{12} = A_1 \wedge X_1 \quad (4\text{-}46)$$

$$S_{1+10+11} = S_1 \vee S_{10} \vee S_{11} = A_1 \wedge X_2 \quad (4\text{-}47)$$

$$S_8 = A_2 \wedge X_1 \quad (4\text{-}48)$$

$$S_{2+4+6} = S_2 \vee S_4 \vee S_6 = A_2 \wedge X_2 \quad (4\text{-}49)$$

$$S_7 = A_3 \wedge X_1 \quad (4\text{-}50)$$

$$S_{1+3+5} = S_1 \vee S_3 \vee S_5 = A_3 \wedge X_2 \quad (4\text{-}51)$$

One could of course get another state diagram by using two equations for X_1 and X_2, different from Eqs. 4-44 and 4-45.

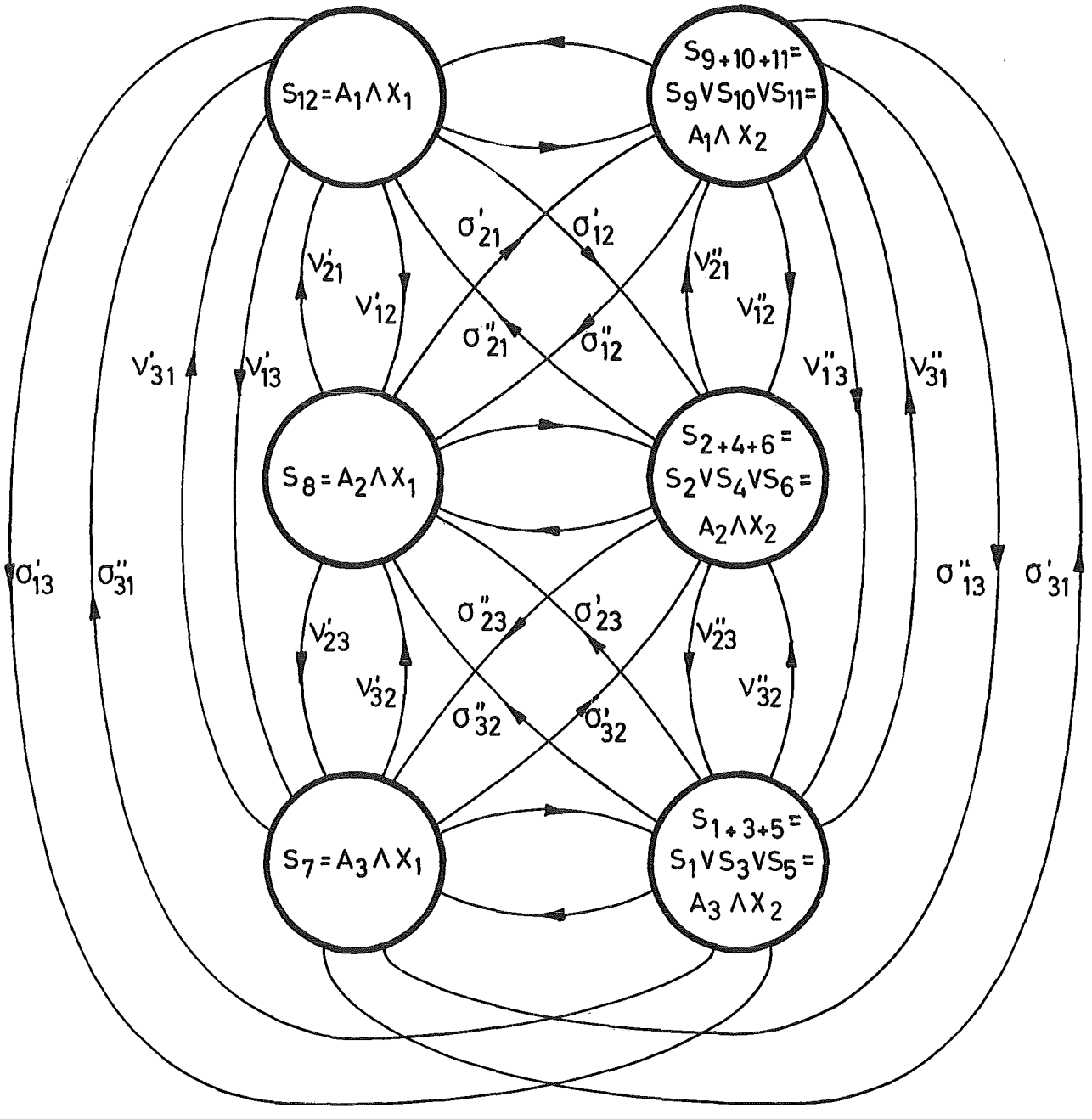


Fig.4-7: State Diagram Obteined by Condesation from that of Fig. 4-4 with $X_1 = B_1 \wedge C_1$ and $X_2 = \overline{X}_1 = B_2 \vee C_2$

Component X is called arbitrary binary component. The word arbitrary is here understood in the sense that component X can be any of the binary components which multiplied by A gives a super component $A \pi X$ whose state diagram can be obtained from that of S by properly condensing it.

In other words an arbitrary binary component simulates the rest of the system.

We can state now the following definition of arbitrary binary component.

> "Given a system S and a component A, we call an arbitrary binary component any arbitrarily chosen binary component X, which satisfies the only condition that the state diagram of the super component generated by multiplying A and X ($A \pi X$) can be obtained from that of S by proper condensation".

Given a component A and an arbitrary binary component X, two possibilities exist: either they are mutually logically independent or they are mutually logically dependent. In the case that A and X are mutually logically independent, they have no parent primary component in common.

4.3 Privileged and Unprivileged Components

Let us go back now to the state diagram of Fig. 4-7. Here the transition rates in which component A is involved are shown. We assume now that A is a primary component. We consider the two pairs of transition rates $(\nu'_{12}, \sigma'_{12})$ and $(\nu''_{12}, \sigma''_{12})$.

With reference to the state diagram of Fig. 4-7 and taking into account the definition of transition rate given in section 4-1, we can write the following equation

$$\nu'_{12} + \sigma'_{12} =$$

$$= \lim_{dt \to 0} \frac{1}{dt} \frac{E\{(A_2 \wedge X_1 \text{ at } t+dt) \wedge (A_1 \wedge X_1 \text{ at } t)\} + E\{(A_2 \wedge X_2 \text{ at } t+dt) \wedge (A_1 \wedge X_1 \text{ at } t)\}}{E\{A_1 \wedge X_1 \text{ at } t\}} \qquad (4\text{-}52)$$

Since we obviously have

$$E\{(A_2 \wedge X_1 \text{ at } t+dt) \wedge (A_1 \wedge X_1 \text{ at } t)\} + E\{(A_2 \wedge X_2 \text{ at } t+dt) \wedge (A_1 \wedge X_1 \text{ at } t) =$$

$$= E\{[(A_2 \wedge X_1 \text{ at } t+dt) \vee (A_2 \wedge X_2 \text{ at } t+dt)] \wedge (A_1 \wedge X_1 \text{ at } t)\} =$$

$$= E\{[A_2 \wedge (X_1 \vee X_2) \text{ at } t+dt] \wedge (A_1 \wedge X_1 \text{ at } t)\} =$$

$$= E\{(A_2 \text{ at } t+dt) \wedge (A_1 \wedge X_1 \text{ at } t)\} , \qquad (4\text{-}53)$$

Eq. 4-52 becomes

$$\nu'_{12} + \sigma'_{12} = \lim_{dt \to 0} \frac{1}{dt} E\{A_2 \text{ at } t+dt \mid A_1 \wedge X_1 \text{ at } t\} \qquad (4\text{-}54)$$

By applying the same procedure to ν''_{12} and σ''_{12} we can write

$$\nu''_{12} + \sigma''_{12} = \lim_{dt \to 0} \frac{1}{dt} E\{A_2 \text{ at } t+dt \mid A_1 \wedge X_2 \text{ at } t\} \qquad (4\text{-}55)$$

We introduce now the transition rate η_{12} from state a_1 to state a_2 of primary component A. This transition rate is defined by the following equation

$$\eta_{12} = \lim_{dt \to 0} \frac{1}{dt} \; E \{A_2 \text{ at } t+dt \mid A_1 \text{ at } t\} \qquad (4\text{-}56)$$

We have

$$E \{A_2 \text{ at } t+dt \mid A_1 \text{ at } t\} = \frac{E \{(A_2 \text{ at } t+dt) \wedge (A_1 \text{ at } t)\}}{E \{A_1 \text{ at } t\}} =$$

$$= \frac{E \{(A_2 \text{ at } t+dt) \wedge (A_1 \wedge X_1 \vee A_1 \wedge X_2 \text{ at } t)\}}{E \{A_1 \text{ at } t\}} =$$

$$= \frac{E \{(A_2 \text{ at } t+dt) \wedge (A_1 \wedge X_1 \text{ at } t)\} + E \{(A_2 \text{ at } t+dt) \wedge (A_1 \wedge X_2 \text{ at } t)\}}{E \{A_1 \text{ at } t\}} \qquad (4\text{-}57)$$

Taking into account Eqs. 4-54 and 4-55 and 4-57, Eq. 4-56 becomes

$$\eta_{12} = \frac{(\nu'_{12} + \sigma'_{12}) \, E\{A_1 \wedge X_1 \text{ at } t\} + (\nu''_{12} + \sigma''_{12}) E \{A_1 \wedge X_2 \text{ at } t\}}{E \{A_1 \text{ at } t\}} \qquad (4\text{-}58)$$

Eq. 4-58 is practically the equation that one would get by condensing the states whose variables are $A_1 \wedge X_1$ and $A_1 \wedge X_2$ into a macrostate (A_1) and the states whose variables are $A_2 \wedge X_1$ and $A_2 \wedge X_2$ into another macrostate (A_2), and by applying the condensation rule for the transition from the first macrostate to the second one (Fig. 4-8).

If we have for all arbitrary binary components X which are mutually logically independent with A

$$\nu'_{12} + \sigma'_{12} = \nu''_{12} + \sigma''_{12} \qquad (4\text{-}59)$$

Eq. 4-58 gives

$$\eta_{12} = \nu'_{12} + \sigma'_{12} = \nu'_{12} + \sigma''_{12} \qquad (4\text{-}60)$$

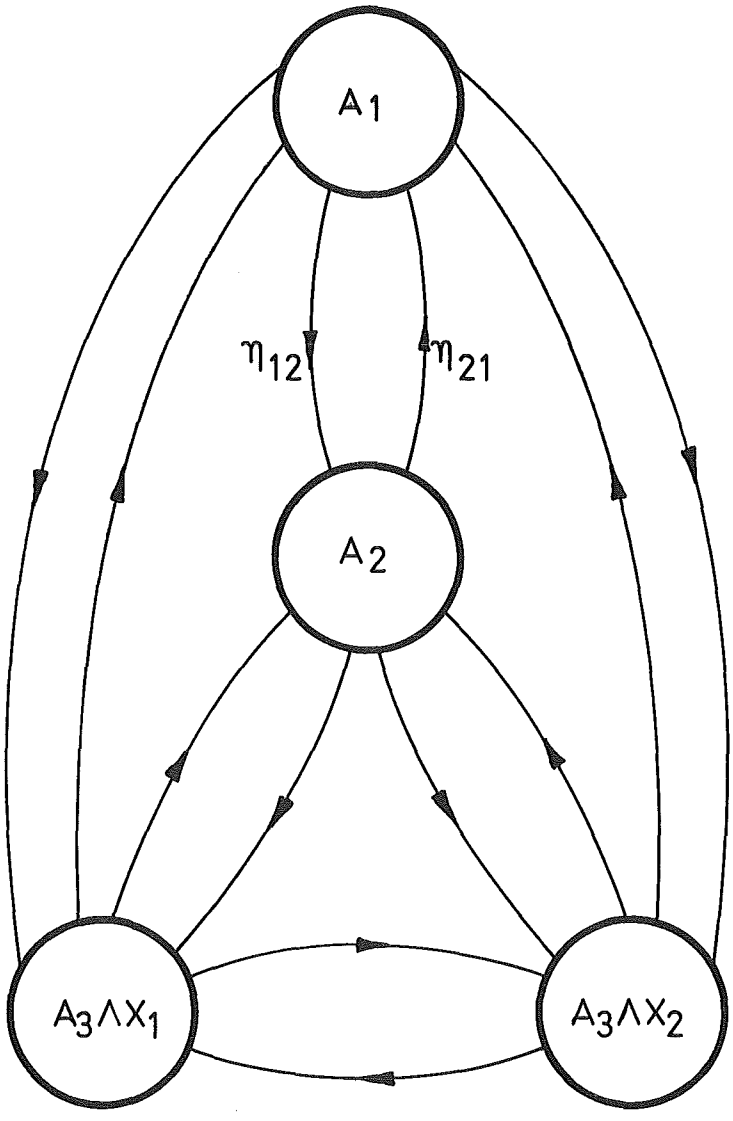


Fig. 4-8: State Diagram Obtained by Condensation from that of Fig. 4-7

Taking into account the meaning of the quantities $\nu'_{12} + \sigma'_{12}$ (Eq. 4-54) and $\nu''_{12} + \sigma''_{12}$ (Eq. 4-55) and the fact that η_{12} is independent of the choice of the arbitrary binary component X which is mutually logically independent with A, Eq. 4-60 tells us that the transition rate from state a_1 to state a_2 of primary component A is invariant with respect to the states occupied at any time by all other primary components of the system. In this case we say that the transition rate from state a_1 to state a_2 is a privileged transition rate.

If all transition rates of A are privileged we say that primary component A is privileged.

We can state now the two following definitions

1st Definition (privileged transition rate)

"If the transition rate from one state to another of a primary component is invariant with respect to the state occupied at any time by all other primary components of the system, the transition rate is said to be privileged."

2nd Definition (privileged primary component)

"If the transition rates of a primary component are all privileged, the primary component is said to be privileged."

Note that the latter definition does not exclude the possibility that the state occupied by the privileged primary component influences some transition rates of some other primary components of the system. In this case, according to the definition of statistical independence given in chapter 3 (Eq. 3-6), the privileged primary component is statistically dependent (because its variables are statistically dependent). If instead the privileged primary component does not affect any transition rate of any other primary component of the system and, by having a transition, does not cause any other primary component to have a transition simultaneously, the privileged primary component is also statistically independent.

A more general definition of privileged primary component is the following:

"A primary component whose performance at each time is independent of the state occupied by all other primary components (belonging to the system), as well as from their past history, is said to be privileged."

The privileged primary components have the following important property

"The expectation of a stochastic literal belonging to a privileged primary component can be calculated by using only the probability data of the primary component to which it belongs. No knowledge about the system or about the other primary components is required".

We come now to the definition of privileged component

> "If the expectations of all variables of a component can be calculated by using only the probability data of its parent primary components, the component is said to be privileged."

A component which is not privileged is said to be unprivileged.

The classification of components into privileged and unprivileged is directly linked to the method for the calculation of the expectation of the conjunction of two boolean variables, say A_i and B_k. We can split the expectation of $A_i \wedge B_k$ into the product of the expectation of one variable and the conditional expectation of the other variable given the first. Two equivalent expressions can be written, namely

$$E\{A_i \wedge B_k\} = E\{A_i\} \cdot E\{B_k \mid A_i\} \qquad (4\text{-}61)$$

and

$$E\{A_i \wedge B_k\} = E\{B_k\} \cdot E\{A_i \mid B_k\} \qquad (4\text{-}62)$$

One would obviously choose Eq. 4-61 if component A is privileged (and B is unprivileged) and Eq. 4-62 if component B is privileged (and A is unprivileged).
In fact, if A is privileged and B is not privileged, the quantity $E\{A_i\}$ can be calculated by considering the state diagram of component A alone. This state diagram is certainly smaller than that of the super component $A \pi B$. It is instead not possible to calculate $E\{B_k\}$ by considering the state diagram of B alone.

The variables of a privileged component are called privileged variables. The variables of an unprivileged component are called unprivileged variables.

Finally, by taking into account the definition of logical and statistical independence, we can state the following

> "If two mutually logically independent components are both privileged, they are also mutually statistically independent."

4.4 Primary components. Master and slave components. Inhibitors. Smallest privileged super component associated with an unprivileged primary component.

Primary components are classified into two categories: privileged primary components and unprivileged primary components (see section 4.3). Since the set of probability laws governing the behaviour of a privileged primary component (i.e. the transition rates) is unique and known, the state diagram of the primary component can be drawn immediately according to the procedure shown in section 4.1 and the corresponding system of linear differential equations can also be written.

Finally the expectation of each individual primary variable of the primary component can easily be calculated by solving the system of linear differential equations.

In the case of an unprivileged primary component, on the other hand, all primary components upon which the primary component under consideration is statistically dependent must also be taken into account.

The stochastic behaviour of an unprivileged primary component is governed by more than one set of probability laws. In general one can identify an universal set of pairwise mutually exclusive events (master events) and can associate with each of these master events a particular set of transition rates governing the stochastic behaviour of the unprivileged primary component. In addition, since a transition from a master event to another master event may cause a transition from one state to another state of the unprivileged component, one can define the conditional probability that a specific transition in the master event space (conditioning transition) causes a specific transition in the state space of the unprivileged primary component (conditioned transition). In general one can also associate with each conditioning transition a set of conditional probabilities, each of them being related to a specific conditioned transition.

We now associate with each of these master events a stochastic boolean binary variable which takes the value 1 if the event occurs and the value 0 otherwise. The set of these variables constitute a component (master component). The unprivileged primary component is called the slave of the master component. The variables belonging to a master component are called master variables.

A master component can be either privileged or unprivileged.

A privileged master component is called an Inhibitor. The variables belonging to an Inhibitor are called inhibiting variables.

We can make the following two statements.

"If a privileged primary component is not parent to the master component of an unprivileged primary component, the two primary components are mutually statistically independent."

and

"A statistically independent primary component is a privileged primary component which is parent to none of the master components of the system."

We want to introduce now the very important concept of smallest privileged super component associated with an unprivileged primary component.

In the case that the master component is privileged, the smallest privileged super component is the super component which results from the product of the unprivileged primary component and its Inhibitor.

If the master component is unprivileged, at least one of its parent primary components is unprivileged. The unprivileged primary components, which are parent to the master component, have their own master components, which in turn can be either privileged or unprivileged, and so on. These master components, too, influence indirectly the stochastic behaviour of the unprivileged primary component under consideration. In this case the smallest privileged super component is the super component which results from the product of the unprivileged primary component with its own master component and with all other concerned master components.

4.5 The well designed and well maintained technical system.

The state diagram of a complex system is usually very large, so that the calculation of the occurrence probability of the top state obtained by summing up the occurrence probabilities of the elementary states belonging to the top is in practice impossible. For this reason one is bound to carry out the fault tree analysis of the system. However, the fault tree analysis alone can be applied only if the primary components are all privileged. If a primary component is unprivileged one is compelled to carry out at least the state analysis of the smallest privileged super component associated with the unprivileged primary component. The states of this super component can be considered as macrostates obtained by a proper condensation of the elementary states of the system.

The problem now arises whether or not the probabilities calculated by analysing the state diagram of the super component alone can be directly incorporated in the fault tree analysis. One has first to satisfy himself that the most important effects due to the statistical dependence have been taken into account and that one does not need to consider the rest of the system, because in this case one would be compelled to analyse the state diagram of the elementary states of the system.

One has to demonstrate that either the effect of the rest of the system can be neglected or that this effect can be properly accounted for by calculating some correction coefficients. This result must of course be obtained without analysing the state diagram of the elementary states of the system. For this reason we have introduced in the preceeding section the arbitrary binary component which simulates the behaviour of the rest of the system.

It is clear that it would be extremely difficult (if not impossible) to carry out any analysis if we are not able to reduce the degree of arbitrariness of this arbitrary binary component. This can be done by considering some properties of symmetry or of asymmetry that the system has. By considering these properties, the analyst can then impose some restrictive conditions on the degree of arbitrariness of the arbitrary binary component.

Since the variety of technical systems is very large, it is not possible to set general rules on how to proceed. For instance some systems can be characterized by some parts which are duplicated, but not all systems have this type of symmetry.

There are however some properties which are common to all systems which are supposed to have been well designed, well constructed and are being well maintained.

We want now to list some of the properties that a system must satisfy in order to receive the attribute of "well designed and well maintained,"

The first property is that the occurrence probability of the top (failed state) is a very small number (10^{-3}; 10^{-5}). This is due to the fact that the transition rates of a component can be of two types: either they are related to a transition from an intact to a failed state or vice versa. In the first case we speak of failure rate and in the second case of repair rate.

For a given component repair rates are orders of magnitude larger than failure rates. All well designed and well maintained technical systems satisfy the above requirement.

The second property is that the statistical dependence among components is the exception and not the rule. In other words the aim of the designer is to design a system in which most components are pairwise mutually statistically independent. If a common mode failure is discovered, one tries by appropriate measures either to eliminate it, or at least to strongly reduce the failure rate due to the common cause.

A third property is that the designer usually tries to reach an high performance (low unavailability) of the system by making its parts to have comparable reliability. For instance, if a system consists of two mutually statistically independent subsystems (1 and 2) and the system fails if at least one of the two subsystems fails, the system unavailability U is simply given by

$$U = U_1 + U_2 - U_1 \cdot U_2$$

where

U_1 = unavailability of subsystem 1

U_2 = unavailability of subsystem 2

Nobody would designe subsystems such that $U_1=10^{-2}$ and $U_2=10^{-9}$. A well designed and well maintained technical system is also usually well balanced, that is one tries to design the various parts of the system in such a way that they have comparable unavailabilities.

Finally a hierarchy among components exists: there are components which have a main task in the system and components which assist the main components to perform their task. Take for instance

the case of an electric generator and of a circuit breaker associated with it. The electric generator has the function to generate electric power which is the main function of the system (the electric power supply system) to which the generator belongs. The circuit breaker has a subordinate role, namely that of connecting or disconnecting the generator from the bus bars. The electric generator is a complex and heavy machine, the circuit breaker instead is much less complex. Due to this difference in complexity, one should reasonably expect that the time required to repair a failed electric generator is usually much larger than that required to repair or to replace a failed circuit breaker. In addition nobody would couple a very reliable electric generator with a circuit breaker which fails often. In other words one should reasonably expect that, in a well designed and well maintained electric power supply system, the contribution to the total system unavailability due to the electric generator is probably higher than that due to the associated circuit breaker.

In conclusion, one can classify components into two categories: main components and subordinate components. The main components perform the main function of the system to which they belong. Electric generators, pumps are usually main components. The subordinate components have a minor and simpler task, namely that of assisting the main components to perform their function. A main component is usually much more complex than a subordinate component associated with it. It is reasonable to expect that in well designed and well maintained systems the repair rate of a main component is smaller than that of the subordinate component associated with it. It is also reasonable to expect that the failure rate of a main component is larger than that of the subordinate component associated with it.

5. STATE ANALYSIS OF AN UNPRIVILEGED PRIMARY COMPONENT

5.1 Generalities

In order to carry out the state analysis of an unprivileged primary component, one must consider also all the other primary components upon which the unprivileged primary component is statistically dependent.

Two methods are suggested here. They are

1. The method of the substitution of the primary variables.

2. The method of the conditional expectation.

The first method is rather general and is applied especially in the case in which the master component is unprivileged.

The second method is less general and can be applied only in the case in which the master component is privileged, i.e. it is an Inhibitor.

5.2 The method of the substitution of the unprivileged primary variables

According to what said in section 4.4, we have to identify the smallest privileged super component G associated with the unprivileged primary component. In general the smallest privileged super component is the super component which results from the product of the unprivileged primary component with its master component and with all other master components which influence indirectly the stochastic behaviour of the unprivileged primary component. We consider now the state diagram of the smallest privileged super component G.

We can associate with each of these states a stochastic binary boolean variable which takes the value 1 if G occupies the associated state and the value 0 otherwise. We can also write the system of linear differential equations and calculate the expectations of the variables associated with G. The literals contained in the variables of G are now expressed as functions of the variables of G which now become the new primary variables. Finally the old literals are replaced by the new primary variables in the fault tree. In this way the statistical dependence among the old literals is removed from the fault tree and is replaced by the logical dependence among the new literals (those of G).

We shall illustrate the method by means of an example. In a fault tree there are two primary components (A and B) each being characterized by two states (intact and failed). Each component can fail either alone or together with the other component at exactly the same time (common mode failure). We shall indicate with a_1 and b_1 respectively the failed states of A and B and with a_2 and b_2 the intact states. The failure rate of A failing alone is λ_A' if B occupies state b_2 and λ_A'' if B occupies state b_1. The failure rate of B failing alone is λ_B' if A occupies state a_2 and λ_B'' if A occupies state a_1. The failure rate associated with the common mode failure is λ_{AB}. The repair rates of A and B are respectively μ_A and μ_B. We can say that A is the master of B and B is the master of A.

We introduce the super-component G (characterized by four states), which one obtains by multiplying the components A and B. The states of G are shown in Fig. 5-1 with associated transition rates among the various states.

According to the state diagram of Fig.5-1 , we define the new primary variables

$$G_1 = A_1 \wedge B_1 \qquad (5\text{-}1)$$

$$G_2 = A_2 \wedge B_1 \qquad (5\text{-}2)$$

$$G_3 = A_1 \wedge B_2 \qquad (5\text{-}3)$$

$$G_4 = A_2 \wedge B_2 \qquad (5\text{-}4)$$

Eqs. 5- 1 to 5- 4 can be solved to get A_1, A_2, B_1 and B_2. We have

$$A_1 = G_3 \vee G_1 \qquad (5\text{-}5)$$

$$A_2 = G_2 \vee G_4 \qquad (5\text{-}6)$$

$$B_1 = G_1 \vee G_2 \qquad (5\text{-}7)$$

$$B_2 = G_3 \vee G_4 \qquad (5\text{-}8)$$

Eqs.5-5 to 5-8 can be used to replace in the fault tree the old primary variables A_1,A_2,B_1 and B_2 by means of the new primary variables G_1,G_2,G_3 and G_4.

In this way the statistical dependence between the failures of A and B has been removed from the fault tree, and has been replaced by the logical dependence among the literals of G. It is important to point out that the new primary component G is privileged.

We want to solve the state diagram of Fig. 5-1 in the asymptotic case ($t \to \infty$).

We introduce the symbol E_j defined as follows

$$E_j = E\left\{ G_j \right\} \qquad j=1,2,3,4 \qquad (5\text{-}9)$$

With reference to Fig. 5-1 we can write the following equations

$$1 = E_1 + E_2 + E_3 + E_4 \qquad (5\text{-}10)$$

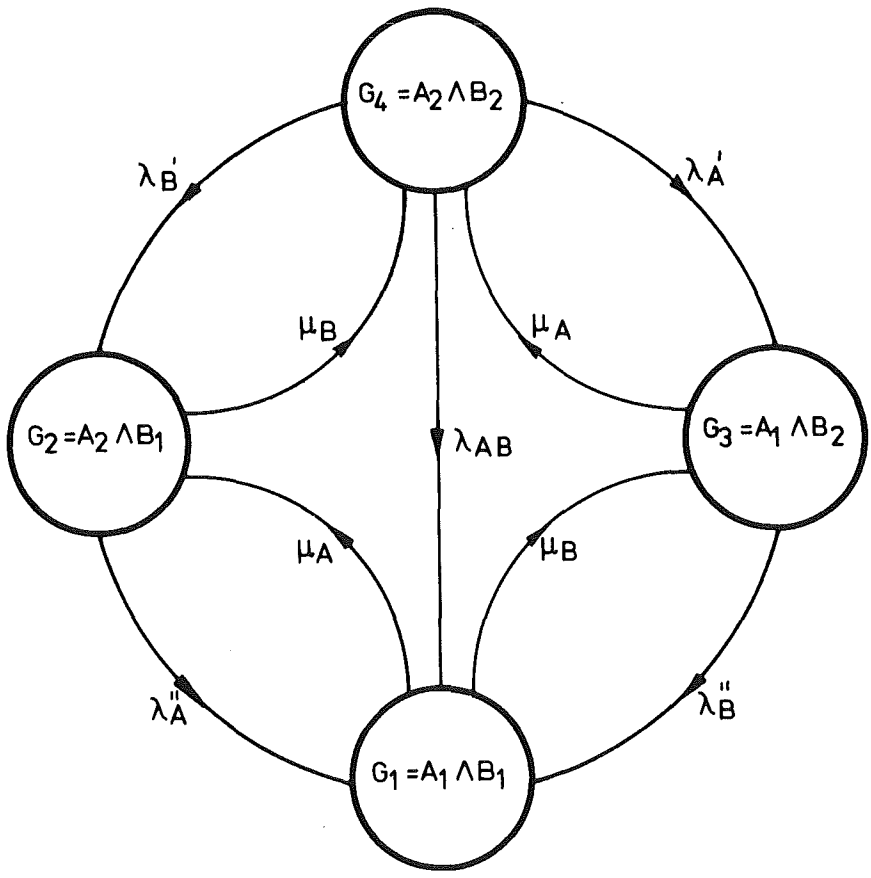


Fig. 5-1. State diagram of super-component G.

$$0 = \mu_A E_1 - (\lambda_A'' + \mu_B) E_2 + \lambda_B' E_4 \qquad (5\text{-}11)$$

$$0 = \mu_B E_1 - (\lambda_B'' + \mu_A) E_3 + \lambda_A' E_4 \qquad (5\text{-}12)$$

$$0 = \mu_B E_2 + \mu_A E_3 - (\lambda_A' + \lambda_B' + \lambda_{AB}) E_4 \qquad (5\text{-}13)$$

Eqs. 5-11; 5-12 and 5-13 refer respectively to the states g_2; g_3 and g_4 of the state diagram of Fig. 5-1. One can solve of course the system of Eqs. 5-10 to 5-13 by using the Cramer's rule. We use here another method. We solve Eq. 5-13 with respect to E_4. We get

$$E_4 = E_2 \frac{\mu_B}{\lambda_A' + \lambda_B' + \lambda_{AB}} + E_3 \frac{\mu_A}{\lambda_A' + \lambda_B' + \lambda_{AB}} \qquad (5\text{-}14)$$

We replace E_4 in Eqs. 5-11 and 5-12 by means of Eq. 5-14. We get

$$\mu_A E_1 + E_2 \left[\frac{\lambda_B' \mu_B}{\lambda_A' + \lambda_B' + \lambda_{AB}} - (\lambda_A'' + \mu_B) \right] + \frac{\lambda_B' \mu_A}{\lambda_A' + \lambda_B' + \lambda_{AB}} E_3 = 0 \qquad (5\text{-}15)$$

and

$$\mu_B E_1 + E_2 \frac{\lambda_A' \mu_B}{\lambda_A' + \lambda_B' + \lambda_{AB}} + E_3 \left[\frac{\lambda_A' \mu_A}{\lambda_A' + \lambda_B' + \lambda_{AB}} - (\lambda_B'' + \mu_A) \right] = 0 \qquad (5\text{-}16)$$

We multiply Eqs. 5-15 and 5-16 respectively by μ_B and μ_A and we subtract one equation from the other. We get finally

$$\frac{E_2}{E_3} = \frac{\alpha_2}{\alpha_3} \qquad (5\text{-}17)$$

where

$$\alpha_2 = \mu_A \left[\lambda_B' (\mu_A + \mu_B) + \lambda_B'' (\lambda_A' + \lambda_B') + \lambda_{AB} (\lambda_B'' + \mu_A) \right] \qquad (5\text{-}18)$$

and

$$\alpha_3 = \mu_B \left[\lambda_A'(\mu_A+\mu_B)+\lambda_A''(\lambda_A'+\lambda_B')+\lambda_{AB}(\lambda_A''+\mu_B) \right] \qquad (5\text{-}19)$$

We can now condense together the states g_2 and g_3 of the state diagram of Fig.5-1 into a macrostate. We get the state diagram of Fig. 5-2.

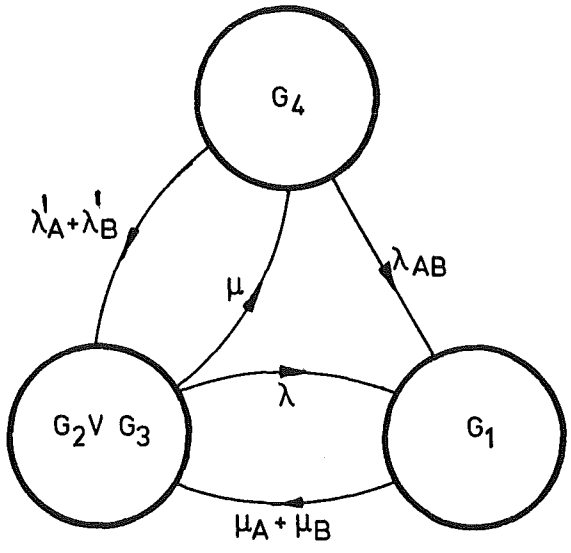


Fig. 5-2. State diagram of super-component G obtained from that of Fig. 5-1 by condensing the states g_2 and g_3 into a macrostate.

In the state diagram of Fig. 5-2 the transition rates λ and μ are given respectively by the following equations

$$\lambda = \frac{\lambda_A''E_2+\lambda_B''E_3}{E_2+E_3} = \frac{\alpha_2\lambda_A''+\alpha_3\lambda_B''}{\alpha_2+\alpha_3} \qquad (5\text{-}20)$$

and

$$\mu = \frac{\mu_B E_2 + \mu_A E_3}{E_2 + E_3} = \frac{\mu_B \alpha_2 + \mu_A \alpha_3}{\alpha_2 + \alpha_3} \tag{5-21}$$

Eqs. 5-20 and 5-21 are obtained by applying the two condensation rules (Eq. 4-20).

We can write now the asymptotic equations for the state diagram of Fig. 5-2. We have

$$0 = -(\mu_A+\mu_B)E_1 + \lambda(E_2+E_3) + \lambda_{AB}E_4 \tag{5-22}$$

$$0 = (\mu_A+\mu_B)E_1 - (\lambda+\mu)(E_2+E_3) + (\lambda_A'+\lambda_B')E_4 \tag{5-23}$$

$$E_1 + (E_2 + E_3) + E_4 = 1 \tag{5-24}$$

The solution of the system of equations 5-22 to 5-24 is the following

$$E_1 = \frac{\lambda_{AB}(\lambda+\mu) + (\lambda_A'+\lambda_B')\lambda}{\Delta} \tag{5-25}$$

$$E_4 = \frac{\mu(\mu_A + \mu_B)}{\Delta} \tag{5-26}$$

and

$$E_2 + E_3 = \frac{(\mu_A+\mu_B)(\lambda_A'+\lambda_B'+\lambda_{AB})}{\Delta} \tag{5-27}$$

where

$$\Delta = \lambda_{AB}(\lambda+\mu+\mu_A+\mu_B)+(\lambda_A'+\lambda_B')(\lambda+\mu_A+\mu_B)+\mu(\mu_A+\mu_B) \tag{5-28}$$

From Eq. 5-17 we get

$$\frac{E_2}{E_2+E_3} = \frac{\alpha_2}{\alpha_2+\alpha_3} \tag{5-29}$$

and

$$\frac{E_3}{E_2+E_3} = \frac{\alpha_3}{\alpha_2 + \alpha_3} \tag{5-30}$$

By replacing in Eqs. 5-29 and 5-30 the term (E_2+E_3) using Eq. 5-27, we get respectively

$$E_2 = \frac{\alpha_2}{\alpha_2+\alpha_3} \frac{(\mu_A+\mu_B)(\lambda_A'+\lambda_B'+\lambda_{AB})}{\Delta} \tag{5-31}$$

and

$$E_3 = \frac{\alpha_3}{\alpha_2 + \alpha_3} \frac{(\mu_A+\mu_B)(\lambda_A'+\lambda_B'+\lambda_{AB})}{\Delta} \tag{5-32}$$

5.3 The method of the conditional expectation

The method of the substitution of the primary variables (sect. 5.2) can in principle always be applied. There is however a simpler method which can be applied in some cases frequently met in practice.

The problem of statistical dependence in fault tree analysis can be reduced to the calculation of the following expression

$$E\left\{D_j \wedge X_s\right\} \tag{5-33}$$

where

D_j = literal belonging to the unprivileged primary component D

X_s = generic boolean variable

We indicate with I the Inhibitor of D.

We make the conjunction between the variables D_j, X_s and the disjunction of all the variables I_k (k=1,2,...,m) belonging to the Inhibitor I. We have

$$E\left\{D_j \wedge X_s\right\} = \sum_{k=1}^{m} E\left\{D_j \wedge X_s \wedge I_k\right\} \tag{5-34}$$

The problem is reduced to the calculation of expressions of the type

$$E\left\{D_j \wedge X_s \wedge I_k\right\} \tag{5-35}$$

We have

$$E\left\{D_j \wedge X_s \wedge I_k\right\} = E\left\{X_s \wedge I_k\right\} \cdot E\left\{D_j \mid I_k \wedge X_s\right\} \tag{5-36}$$

In some cases it is possible to demonstrate that

$$E\left\{D_j \wedge X_s \wedge I_k\right\} = E\left\{X_s \wedge I_k\right\} E\left\{D_j \mid I_k\right\} \qquad (5\text{-}37)$$

Eq. 5-37 tells us that only the conditional expectations $E\left\{D_j \mid I_k\right\}$ need to be known. These expectations are obviously much easier to calculate than the expectations $E\left\{D_j \mid I_k \wedge X_s\right\}$. In addition their total number is lower. In fact, in the case that Eq. 5-37 is satisfied, only the supercomponent G generated by multiplying D with I needs to be considered. From the state analysis of G one can derive the required conditional expectations. Super component G is the smallest privileged super component associated with the unprivileged primary component D. Instead, in the case in which Eq. 5-37 is not satisfied, a larger super component must be considered because also the variables of component X must be taken into account. We recall the discussion on the mesh size made in the introduction. We can say that the mesh size required to handle the problem of statistical dependences in the case in which Eq. 5-37 is satisfied is coarser than that required to handle the same problem in the case that Eq. 5-37 is not satisfied.

The problem now arises to find out when Eq. 5-37 is satisfied.

A special case is that in which a variable Y_q exists which is statistically independent of I_k as well as of D_j and is such that $Y_q \wedge I_k = X_s \wedge I_k$ (theorem of chapter 3).

If Eq. 5-37 is satisfied for any variable of the fault tree, we say that the variable D_j is homogeneously dependetn of I_k.

5.4 Homogeneous dependence

We introduce the definition of homogeneous dependence.

> "An unprivileged literal D_j is said to be homogeneously dependent on one of its inhibiting variables I_k if the conditional expectation of D_j given any arbitrary implicant of I_k (which does not contain any literal of D) is equal to the conditional expectation of D_j given I_k."

If we indicate with X_s an arbitrary boolean variable which does not contain any literal of D, the boolean variable generated by the conjunction between I_k and X_s is an implicant of I_k. The primary variable D_j is homogeneously dependent of I_k if Eq. 5-37 is satisfied.

The problem now arises how to find out that an unprivileged component can be treated as homogeneously dependent on its Inhibitor I. We shall illustrate this problem by means of an example.

Let us assume that a binary component I is mounted in a system "S" in such a way that it is not allowed to change its state if a binary primary component D is in its failed state. If instead D is in its intact state the failure and repair rates of I are respectively λ_I and μ_I. The failure and repair rates of D are assumed to be respectively σ_1 and ρ_1 if I is failed and σ_2 and ρ_2 if I is intact. The other primary components which are not parent to I are assumed not to affect the stochastic behaviours of I and of D.

We consider the super-component G obtained by multiplying the two components I and D.

We introduce the following symbols:

I_1 and D_1 are the variables associated with the failed states respectively of I and D.

I_2 and D_2 are the variables associated with the intact states respectively of I and D.

The state diagram of the super-component G is shown in Fig. 5.3.

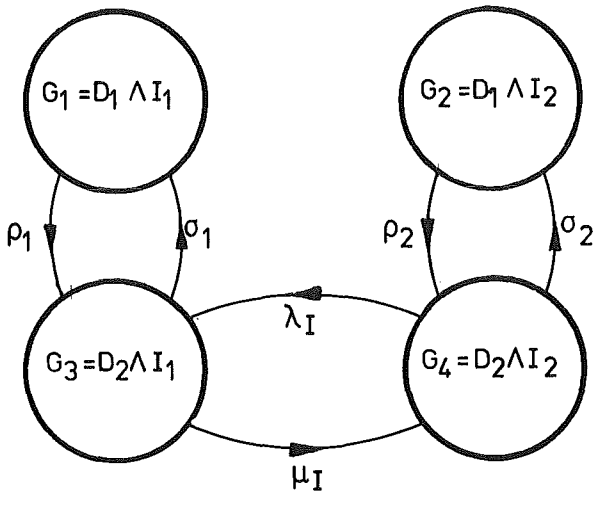


Fig. 5-3. State diagram of a super-component G made of two components.

The meaning of the other symbols used in Fig. 5-3 is the following:

λ_I = failure rate of I given that D is not failed.
μ_I = repair rate of I given that D is not failed.
σ_1^I = failure rate of D given that I is failed
ρ_1 = repair rate of D given that I is failed
σ_2 = failure rate of D given that I is intact
ρ_2 = repair rate of D given that I is intact.

With reference to the state diagram of Fig. 5-3, we can write the following two boolean identities

$$G_1 \vee G_3 = I_1 \tag{5-39}$$

and

$$G_2 \vee G_4 = I_2 \tag{5-40}$$

In the following we shall limit ourselves to consider the asymptotic case ($t \to \infty$) only. We can also write the following equation (Fig.5-3) for state g1.

$$\rho_1 \; E\{G_1\} - \sigma_1 \; E\{G_3\} = 0 \tag{5-41}$$

Taking into account Eq.5-39, one can also write

$$E\{G_1\} + E\{G_3\} = E\{I_1\} \tag{5-42}$$

From Eqs. 5-41 and 5-42 it follows

$$\frac{E\{G_1\}}{E\{I_1\}} = \frac{\sigma_1}{\rho_1 + \sigma_1} \tag{5-43}$$

and

$$\frac{E\{G_3\}}{E\{I_1\}} = \frac{\rho_1}{\rho_1 + \sigma_1} \tag{5-44}$$

We notice that

$$\frac{E\{G_1\}}{E\{I_1\}} = \frac{E\{D_1 \wedge I_1\}}{E\{I_1\}} = E\{D_1 \mid I_1\} \tag{5-45}$$

and

$$\frac{E\{G_3\}}{E\{I_1\}} = \frac{E\{D_2 \wedge I_1\}}{E\{I_1\}} = E\{D_2 \mid I_1\} \tag{5-46}$$

From Eqs. 5-43 and 5-45 it follows

$$E\{D_1 \mid I_1\} = \frac{\sigma_1}{\rho_1 + \sigma_1} \tag{5-47}$$

From Eqs. 5-44 and 5-46 it follows

$$E\{D_2 \mid I_1\} = \frac{\rho_1}{\rho_1 + \sigma_1} \tag{5-48}$$

By applying a similar procedure to G_2 and G_4, one obtains

$$E\{D_1 \mid I_2\} = \frac{E\{G_2\}}{E\{I_2\}} = \frac{\sigma_2}{\rho_2 + \sigma_2} \tag{5-49}$$

and

$$E\{D_2 \mid I_2\} = \frac{E\{G_4\}}{E\{I_2\}} = \frac{\rho_2}{\rho_2 + \sigma_2} \tag{5-50}$$

We now condense the state G_1 and G_3 on one side and the states G_2 and G_4 on the other side. We get the state diagram of Fig.5-4.

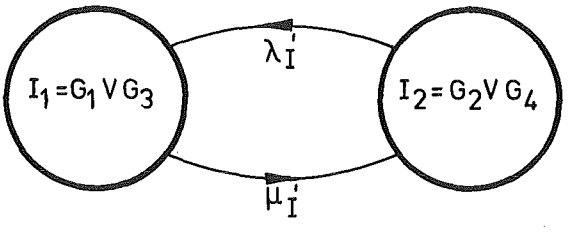


Fig. 5-4. State diagram of component I.

By applying the condensation rules given in section 4.2 (Eq. 4-20), on gets

$$\lambda_I' = \lambda_I \frac{E\{G_4\}}{E\{I_2\}} = \lambda_I \; E\{D_2 \mid I_2\} \qquad (5\text{-}51)$$

and

$$\mu_I' = \mu_I \frac{E\{G_3\}}{E\{I_1\}} = \mu_I \; E\{D_2 \mid I_1\} \qquad (5\text{-}52)$$

Taking into account Eqs. 5-50 , Eq. 5-51 becomes

$$\lambda_I' = \lambda_I \frac{\rho_2}{\rho_2 + \sigma_2} \qquad (5\text{-}53)$$

Taking into account Eq. 5-48, Eq. 5-52 becomes

$$\mu_I' = \mu_I \frac{\rho_1}{\rho_1 + \sigma_1} \qquad (5\text{-}54)$$

In well designed and maintained technical systems (section 4.5) repair rates are orders of magnitude larger than failure rates. This is equivalent to writing

$$\rho_2 \gg \sigma_2 \tag{5-55}$$

and

$$\rho_1 \gg \sigma_1 \tag{5-56}$$

Eqs. 5-55 and 5-56 can also be written as follows

$$\frac{\rho_2}{\rho_2 + \sigma_2} \cong 1 \tag{5-57}$$

and

$$\frac{\rho_1}{\rho_1 + \sigma_1} \cong 1 \tag{5-58}$$

Taking into account Eqs. 5-57 and 5-58, Eqs. 5-53 and 5-54 become respectively

$$\lambda_I' \cong \lambda_I \tag{5-59}$$

and

$$\mu_I' \cong \mu_I \tag{5-60}$$

From the state diagram of Fig. 5-4 and taking into account Eqs. 5-59 and 5-60 we can write

$$E\{I_1\} \cong \frac{\lambda_I}{\lambda_I + \mu_I} \tag{5-61}$$

and

$$E\{I_2\} \cong \frac{\mu_I}{\lambda_I + \mu_I} \tag{5-62}$$

Eqs. 5-61 and 5-62 tell us that the expectations of I_1 and I_2 are almost equal to the expectations that one would calculate by assuming that the failure and repair rates of I are invariant also with respect to the state occupied by D. In other words we would not make any appreciable error if we assume that I is privileged. On the other hand, since the conditional expectations of the variables of D (Eqs. 5-47 to 5-50) clearly indicate that D depends on I, we can conclude that I is a privileged master component (i.e. an Inhibitor) and D is its slave.

According to what is said in section 4.2 let us consider an arbitrary binary component X. The two variables of X are assumed not to contain any literal of D. The state diagram of Fig. 5-5 has been obtained from that of Fig. 5-3 by expanding the variables of G with respect to X. Component X is either privileged or unprivileged. In the latter case we shall make the hypothesis that the system is such that the master variables of X do not contain any literal of D. The above assumption means that the stochastic behaviour of all other primary components of the system which are not parent to I is not influenced by the state occupied by component D. Under the above hypothesis it seems reasonable to assume that the following equalities among transition rates approximately hold (Fig. 5-5).

$$\lim_{\substack{dt\to 0\\ t\to\infty}} \frac{1}{dt} E\{D_1 \wedge I_1 \wedge X_2 \text{ at } t+dt \mid D_1 \wedge I_1 \wedge X_1 \text{ at } t\}$$

$$\cong \lim_{\substack{dt\to 0\\ t\to\infty}} \frac{1}{dt} E\{D_2 \wedge I_1 \wedge X_2 \text{ at } t+dt \mid D_2 \wedge I_1 \wedge X_1 \text{ at } t\} =$$

$$\cong \lim_{\substack{dt\to 0\\ t\to\infty}} \frac{1}{dt} E\{I_1 \wedge X_2 \text{ at } t+dt \mid I_1 \wedge X_1 \text{ at } t\} = \lambda_{12} \qquad (5\text{-}63)$$

$$\lim_{\substack{dt\to 0\\ t\to\infty}} \frac{1}{dt} E\{D_1 \wedge I_1 \wedge X_1 \text{ at } t+dt \mid D_1 \wedge I_1 \wedge X_2 \text{ at } t\} =$$

$$\cong \lim_{\substack{dt\to 0\\ t\to\infty}} \frac{1}{dt} E\{D_2 \wedge I_1 \wedge X_1 \text{ at } t+dt \mid D_2 \wedge I_1 \wedge X_2 \text{ at } t\} =$$

$$\cong \lim_{\substack{dt\to 0\\ t\to\infty}} \frac{1}{dt} E\{I_1 \wedge X_1 \text{ at } t+dt \mid I_1 \wedge X_2 \text{ at } t\} = \lambda_{21} \qquad (5\text{-}64)$$

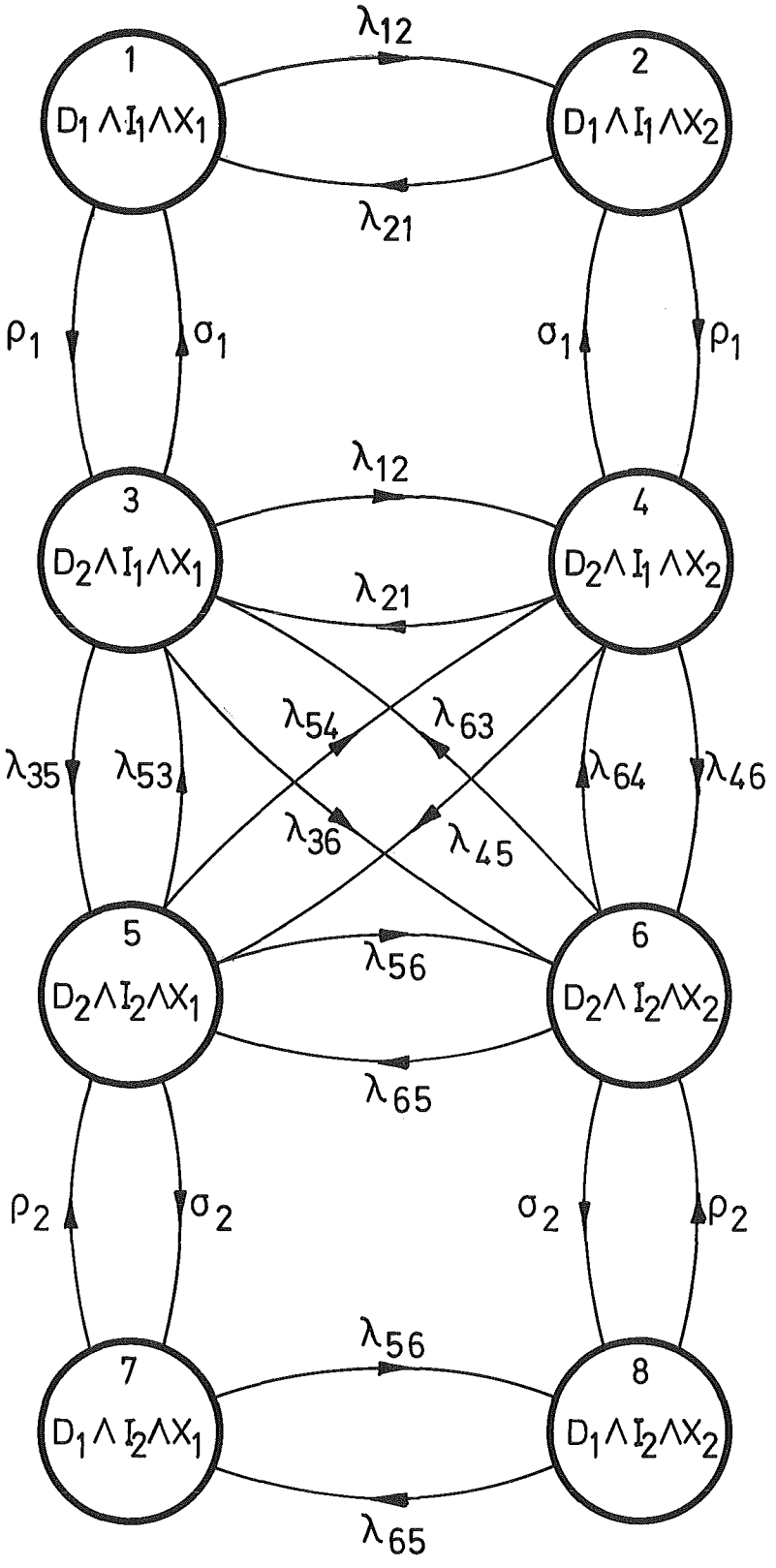


Fig. 5-5: State Diagram Obtained from that of Fig. 5-3 by Espanding it with Respect to the Binary Component X.

$$\lim_{\substack{dt\to 0\\ t\to\infty}} \frac{1}{dt}\ E\{D_2 \wedge I_2 \wedge X_1 \text{ at } t+dt \mid D_2 \wedge I_2 \wedge X_2 \text{ at } t\} =$$

$$\cong \lim_{\substack{dt\to 0\\ t\to\infty}} \frac{1}{dt}\ E\{D_1 \wedge I_2 \wedge X_1 \text{ at } t+dt \mid D_1 \wedge I_2 \wedge X_2 \text{ at } t\} =$$

$$\tilde{=} \lim_{\substack{dt\to 0\\ t\to\infty}} \frac{1}{dt}\ E\{I_2 \wedge X_1 \text{ at } t+dt \mid I_2 \wedge X_2 \text{ at } t\} = \lambda_{56} \qquad (5\text{-}65)$$

and

$$\lim_{\substack{dt\to 0\\ t\to\infty}} \frac{1}{dt}\ E\{D_2 \wedge I_2 \wedge X_2 \text{ at } t+dt \mid D_2 \wedge I_2 \wedge X_1 \text{ at } t\} =$$

$$\tilde{=} \lim_{\substack{dt\to 0\\ t\to\infty}} \frac{1}{dt}\ E\{D_1 \wedge I_2 \wedge X_2 \text{ at } t+dt \mid D_1 \wedge I_2 \wedge X_1 \text{ at } t\} =$$

$$\tilde{=} \lim_{\substack{dt\to 0\\ t\to B}} \frac{1}{dt}\ E\{I_2 \wedge X_2 \text{ at } t+dt \mid I_2 \wedge X_1 \text{ at } t\} = \lambda_{65} \qquad (5\text{-}66)$$

The same hypothesis (i.e. the master variables of X do not contain any literal of D) allows us to deduce that D and X cannot change their states at exactly the same time due to a common cause. This is equivalent to writing that the following diagonal transition rates (Fig. 5-5) are equal to zero

$$\lambda_{14} = \lambda_{41} = \lambda_{23} = \lambda_{32} = \lambda_{58} = \lambda_{85} = \lambda_{67} = \lambda_{76} = 0 \qquad (5\text{-}67)$$

In addition, since the stochastic behaviour of D depends only on its Inhibitor I, the following equalities must hold (Fig. 5-5)

$$\lambda_{13} = \lambda_{24} = \rho_1 \tag{5-68}$$

$$\lambda_{31} = \lambda_{42} = \sigma_1 \tag{5-69}$$

$$\lambda_{75} = \lambda_{86} = \rho_2 \tag{5-70}$$

$$\lambda_{57} = \lambda_{68} = \sigma_2 \tag{5-71}$$

Finally it is reasonable to assume that the repair rate μ_I of I is invariant with respect to X. By taking into account the above assumption and by applying the condensation rules (Eqs. 4-30 to 4-31) between the two state diagrams of Fig. 5-5 and Fig. 5-3, the following relationship holds

$$\lambda_{35} + \lambda_{36} = \lambda_{45} + \lambda_{46} = \mu_I \tag{5-72}$$

We now condense the states 5; 6; 7 and 8 of the state diagram of Fig. 5-5 into a macrostate. We get the state diagram of Fig. 5-6. Due to the condensation laws, the transition rates λ_{I1}' and λ_{I2}' must obviously satisfy the following relationship

$$\lambda_{I1} + \lambda_{I2} = \lambda_I' \tilde{=} \lambda_I \tag{5-73}$$

It is easy to demonstrate (by applying the condensation rules and Eq. 5-72) that the two transition rates in Fig. 5-6 from state 3 to state 5 and from state 4 to state 5 are both equal to μ_I.

With reference to the state diagram of Fig. 5-6 , we can write the following equation

$$(\rho_1+\lambda_{12})\ E\{D_1 \wedge I_1 \wedge X_1\} = \sigma_1\, E\{D_2 \wedge I_1 \wedge X_1\} + \lambda_{21}\ E\{D_1 \wedge I_1 \wedge X_2\} \tag{5-74}$$

We have obviously

$$\sigma_1\ E\{D_2 \wedge I_1 \wedge X_1\} =$$

$$= \sigma_1 \left[E\{I_1 \wedge X_1\} - E\{D_1 \wedge I_1 \wedge X_1\} \right] \tag{5-75}$$

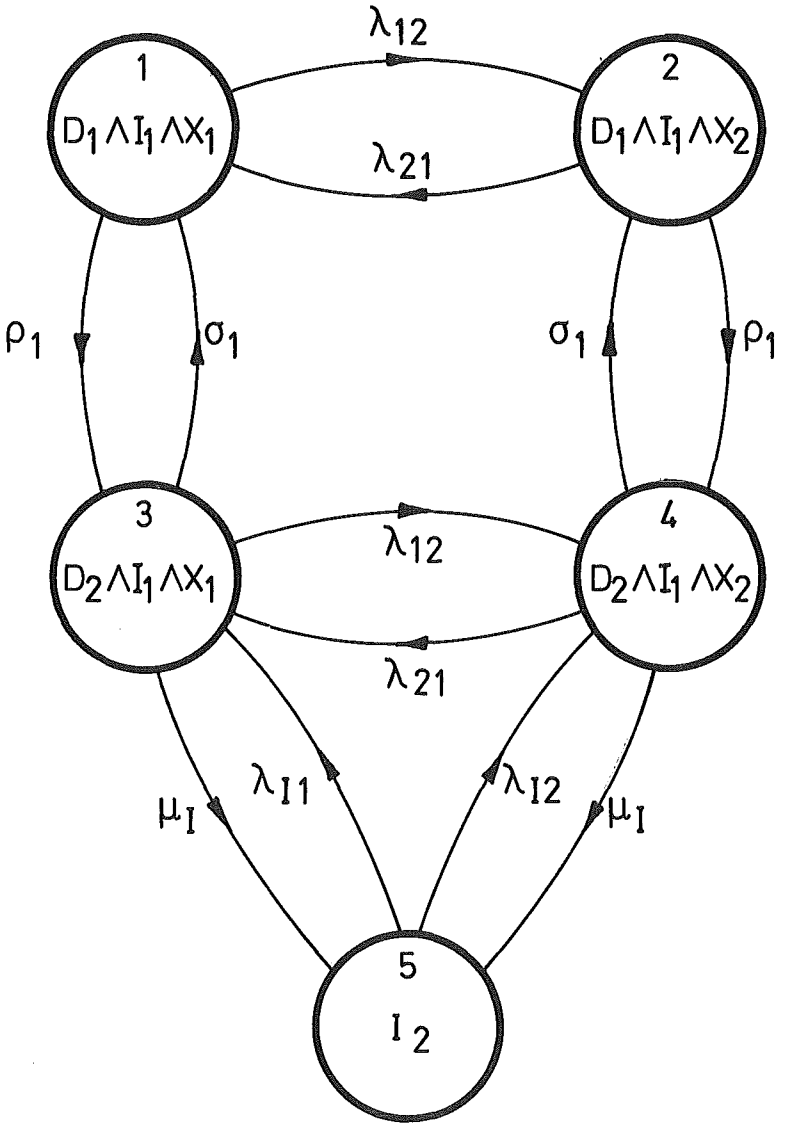


Fig.5-6: State Diagram Obtained from that of Fig.5-5 by Condensing the States 5,6,7 and 8 of Fig. 5-5 into One Single Macrostate(Nr. 5)

We can obviously write

$$E\left\{D_1 \wedge I_1 \wedge X_2\right\} = E\left\{D_1 \wedge I_1\right\} - E\left\{D_1 \wedge I_1 \wedge X_1\right\} \tag{5-76}$$

Taking into account Eqs. 5-75 and 5-76 , Eq. 5-74 becomes

$$E\left\{D_1 \wedge I_1 \wedge X_1\right\} = \frac{\sigma_1}{\sigma_1+\rho_1+\lambda_{12}+\lambda_{21}} E\left\{I_1 \wedge X_1\right\} +$$

$$+ \frac{\lambda_{21}}{\sigma_1+\rho_1+\lambda_{12}+\lambda_{21}} E\left\{D_1 \wedge I_1\right\} \tag{5-77}$$

We divide both terms of Eq. 5-77 by $E\left\{I_1 \wedge X_1\right\}$. Taking into account Eq. 5-47 also, we get from Eq. 5-77

$$E\left\{D_1 \mid I_1 \wedge X_1\right\} = \frac{\sigma_1}{\sigma_1+\rho_1+\lambda_{12}+\lambda_{21}} \left[1 + \frac{\lambda_{21}}{\sigma_1+\rho_1} \frac{E\left\{I_1\right\}}{E\left\{I_1 \wedge X_1\right\}}\right] \tag{5-78}$$

We want to calculate now an upper bound for the term $\lambda_{21} \cdot E\left\{I_1\right\} / E\left\{I_1 \wedge X_1\right\}$ in Eq. 5-78.

For this purpose we condense the two pairs of states (1 and 3) and (2 and 4) respectively into two macrostates we get the state diagram of Fig. 5-7.

With reference to the state diagram of Fig. 5-7, we can write the following equation (state 1)

$$(\lambda_{12} + \mu_I)\ E\ \{I_1 \wedge X_1\} = \lambda_{21}\ E\ \{I_1 \wedge X_2\} + \lambda_{I1}\ E\ \{I_2\} \tag{5-79}$$

We have obviously

$$E\ \{I_1 \wedge X_2\} = E\ \{I_1\} - E\ \{I_1 \wedge X_1\} \tag{5-80}$$

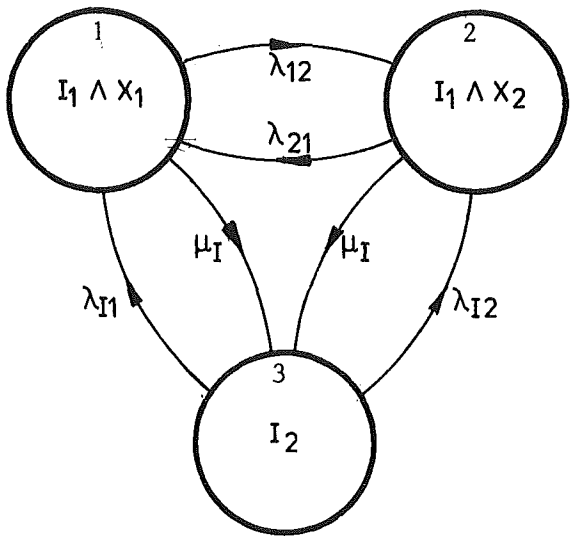


Fig. 5-7. State diagram derived by condensation from that of Fig. 5-6.

From Eqs. 5-61 and 5-62 one gets

$$E\{I_2\} = \frac{\mu_I}{\lambda_I} E\{I_1\} \tag{5-81}$$

Taking into account Eqs. 5-80 and 5-81, Eq. 5-79 becomes

$$\frac{E\{I_1\}}{E\{I_1 \wedge X_1\}} = \frac{\lambda_{12} + \lambda_{21} + \mu_I}{\lambda_{21} + \mu_I \lambda_{I1}/\lambda_I} \tag{5-82}$$

From Eq. 5-82 we get

$$\frac{E\{I_1\}}{E\{I_1 \wedge X_1\}} \leq \frac{\lambda_{12} + \lambda_{21} + \mu_I}{\lambda_{21}} \tag{5-83}$$

Taking into account Eq. 5-83, Eq. 5-78 becomes

$$E\left\{D_1 \mid I_1 \wedge X_1\right\} \leq \frac{\sigma_1}{\sigma_1+\rho_1+\lambda_{12}+\lambda_{21}} \left[1 + \frac{\lambda_{12}+\lambda_{21}+\mu_I}{\sigma_1+\rho_1}\right] \tag{5-84}$$

Eq. 5-84 can be written as follows

$$E\left\{D_1 \mid I_1 \wedge X_1\right\} \leq \frac{\sigma_1}{\sigma_1+\rho_1} \overline{/}1 + \frac{\mu_I}{\sigma_1+\rho_1+\lambda_{12}+\lambda_{21}} \overline{\ }7 \qquad (5\text{-}85)$$

Finally by neglecting the term $\lambda_{12}+\lambda_{21}$ in Eq. 5-85 we can write

$$E\left\{D_1 \mid I_1 \wedge X_1\right\} < \frac{\sigma_1}{\sigma_1+\rho_1} \overline{/}1 + \frac{\mu_I}{\sigma_1+\rho_1} \overline{\ }7 \qquad (5\text{-}86)$$

Eq. 5-86 can be written as follows

$$E\{D_1 \mid I_1 \wedge X_1\} \leq \frac{\sigma_1'}{\sigma_1'+\rho_1} \qquad (5\text{-}87)$$

where

$$\sigma_1' = \sigma_1 \frac{\sigma_1 + \rho_1 + \mu_I}{\sigma_1 + \rho_1 - \sigma_1\mu_I/\rho_1} \qquad (5\text{-}88)$$

We go back now to the state diagram of Fig. 5-5 and we condense now the states 1; 2; 3 and 4 into a simple macrostate. We get the state diagram of Fig. 5-8. We apply now to the state diagram of Fig. 5-8 the same procedure already applied to that of Fig. 5-6 and we take into account that in well designed and well maintained technical systems (section 4-5), failure rates are orders of magnitude smaller than repair rates, that is

$$\lambda_{14} << \rho_2 \qquad (5\text{-}89)$$

By taking into account Eq. 5-89 and by applying the same procedure used in the case of the state diagram of Fig. 5-6, it is easy to demonstrate that

$$E\{D_1 \mid I_2 \wedge X_1\} \tilde{=} \frac{\sigma_2}{\sigma_2+\rho_2} = E\{D_1 \mid I_2\} \qquad (5\text{-}90)$$

By looking at Eqs. 5-87 and 5-88, we notice that we overestimate the expressions of $E\{D_1 \mid I_1 \wedge X_1\}$ and $E\{D_1 \mid I_1\}$ by setting

$$E\{D_1 \mid I_1\} = E\{D_1 \mid I_1 \wedge X_1\} = \frac{\sigma_1'}{\sigma_1'+\rho_1} \qquad (5\text{-}91)$$

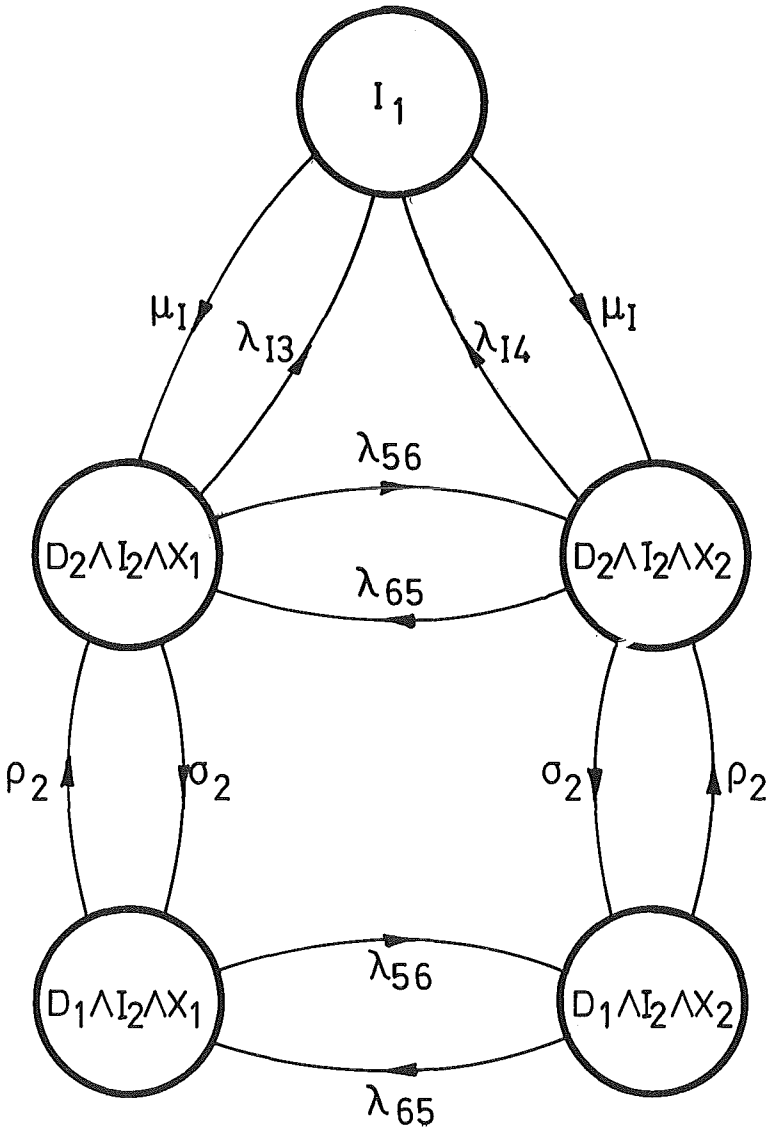


Fig. 5-8: State Diagram Obtained from that of Fig. 5-5 by Condensing the States 1, 2, 3 and 4 of Fig. 5-5 into One Single Macrostate (I_1)

It is important to point out that the above assumption is conservative because Eq. 5-91 overestimates the occurrence probability of a failed state.

The expressions $E\{D_2 \mid I_1\}$; $E\{D_2 \mid I_2\}$; $E\{D_2 \mid I_1 \wedge X_1\}$ and $E\{D_2 \mid I_2 \wedge X_1\}$ must be calculated respectively from the relationships

$$E\{D_1 \mid I_1 \wedge X_1\} + E\{D_2 \mid I_1 \wedge X_1\} = E\{D_1 \mid I_1\} + E\{D_2 \mid I_1\} = 1 \quad (5\text{-}92)$$

and

$$E\{D_1 \mid I_2 \wedge X_1\} + E\{D_2 \mid I_2 \wedge X_1\} = E\{D_1 \mid I_2\} + E\{D_2 \mid I_2\} = 1 \quad (5\text{-}93)$$

In conclusion the following set of equations can be used for the conditional expectations

$$E\{D_1 \mid I_1\} = E\{D_1 \mid I_1 \wedge X_1\} = \frac{\sigma_1'}{\sigma_1' + \rho_1} \quad (5\text{-}94)$$

$$E\{D_2 \mid I_1\} = E\{D_2 \mid I_1 \wedge X_1\} = \frac{\rho_1}{\sigma_1' + \rho_1} \quad (5\text{-}95)$$

$$E\{D_1 \mid I_2\} = E\{D_1 \mid I_2 \wedge X_1\} = \frac{\sigma_2}{\sigma_2 + \rho_2} \quad (5\text{-}96)$$

and

$$E\{D_2 \mid I_2\} = E\{D_2 \mid I_2 \wedge X_1\} = \frac{\rho_2}{\sigma_2 + \rho_2} \quad (5\text{-}97)$$

where σ_1' is given by Eq. 5-88.

The use of Eqs. 5-94 to 5-97 offers the great advantage that these expressions do not contain any transition rate of the arbitrary binary component X. This is equivalent to saying that the variables of D are homogeneously dependent upon the variables of I. Eqs. 5-94 to 5-97 tell us in fact that Eq. 5-37 is satisfied for all variables of D with respect to any arbitrary implicant of the variables of I.

6. THE BIPOLAR SWITCH

The bipolar switch is a statistically dependent component characterized by two positions (bipolar) and by three states. The two positions are those which the switch is asked to take depending upon the value of the input signal. They are closed and open. The three states are: intact, failed closed and failed open. Note that the position indicates the required position of the switch which is identical with its effective position only if the switch is intact.

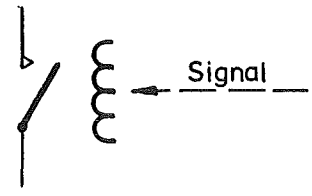


Fig. 6-1. Schematic diagram of an electrical bipolar switch (circuit breaker).

Fig. 6-1 shows the schematic diagram of an electrical bipolar switch (circuit breaker). The signal may be e.g. the state of another component. Fig. 6-2 shows a system consisting of an electrical generator I connected to the grid through a circuit breaker D.

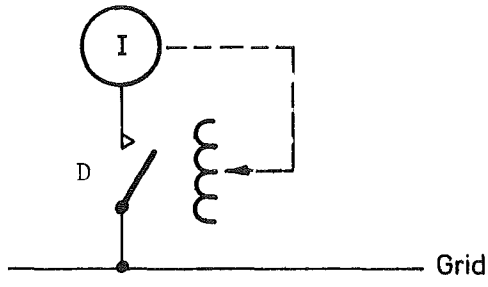


Fig. 6-2. System consisting of a generator I connected to the grid through a circuit breaker D.

The operating state of the system of Fig. 6-2 is: electrical generator I is supplying electrical power to the grid through the closed contacts of circuit breaker D. If the generator I fails,

circuit breaker D will open and the generator will be disconnected from the grid. In this case the input signal to D is the state of the generator and exactly position closed corresponds to generator intact and position open to generator failed. The two boolean variables associated to the generator (corresponding respectively to generator failed and generator intact) will constitute therefore the master component of D.

The master component I will contain two boolean variables, namely

I_1 associated with state i_1 (generator failed)

I_2 associated with state i_2 (generator intact)

Since the switch D has three states, there will be three primary variables, namely

D_1 associated with state d_1 (failed open)

D_2 associated with state d_2 (failed closed)

D_3 associated with state d_3 (intact).

We consider now super-component G obtained by multiplying switch D and master component I. Super-component G is characterized by the six states which one obtains by carrying out the cartesian product of the states of D and I in all possible ways. The six boolean variables associated with super-component G are:

$$G_1 = I_1 \wedge D_1 \qquad (6\text{-}1)$$

$$G_2 = I_2 \wedge D_1 \qquad (6\text{-}2)$$

$$G_3 = I_1 \wedge D_3 \qquad (6\text{-}3)$$

$$G_4 = I_2 \wedge D_3 \qquad (6\text{-}4)$$

$$G_5 = I_1 \wedge D_2 \qquad (6\text{-}5)$$

$$G_6 = I_2 \wedge D_2 \qquad (6\text{-}6)$$

The state diagram of super-component G is shown in Fig. 6-3.

Required Position: Open

Required Position: Closed

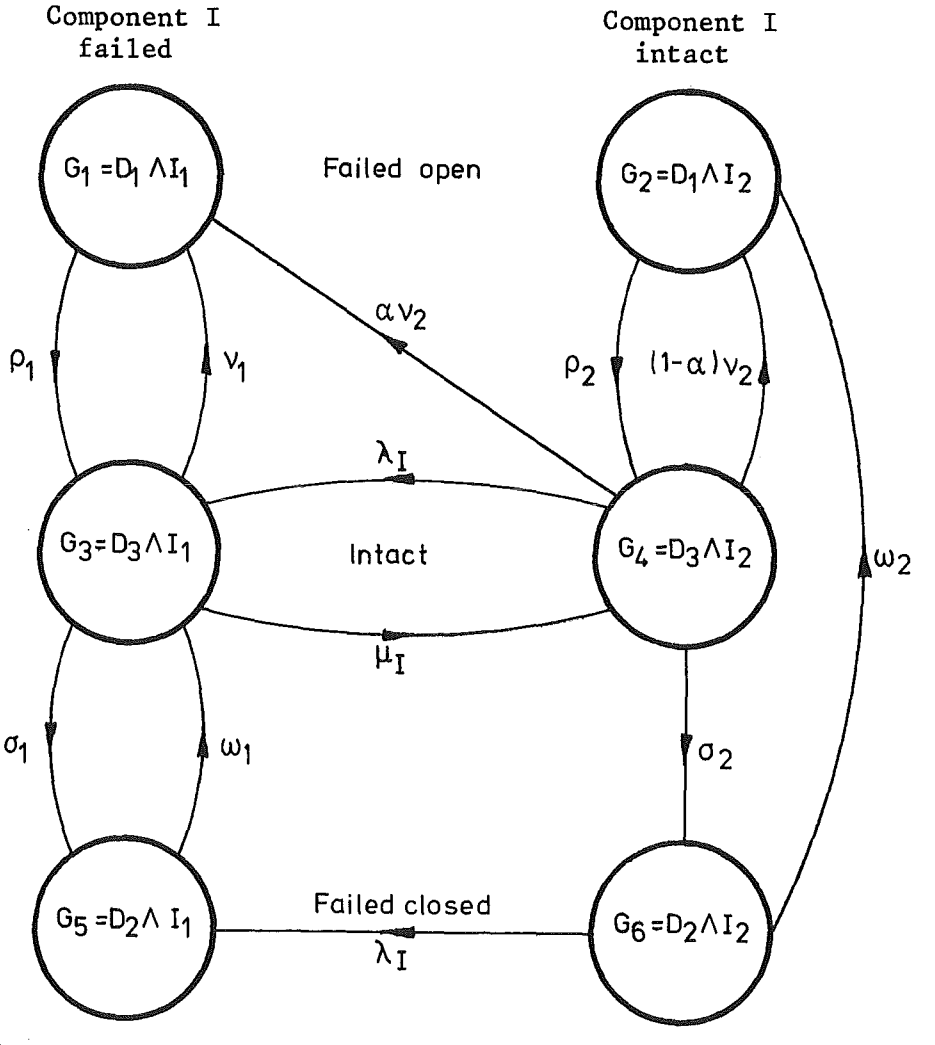


Fig. 6-3. State diagram of super-component G made of master component I and switch D.

The state diagram of Fig. 6-3 depends upon some details of the design of the electrical circuit and upon the repair strategy of the system(generator + switch).

(a) The state of normal operation is g_4. The failure of generator I is accounted for by means of the transition from state g_4 to g_3 (transition rate λ_I).

(b) Electrical circuits are usually provided with additional contactors. When the generator fails, the circuit breaker will open the circuit. However the additional contactors will be opened before starting to repair the generator, so that the generator windings will remain disconnected from the grid also in the case in which the circuit breaker closes inadvertently. This means that when the switch is already in the open position and the generator is being repaired the two types of failure namely switch fails open and switch closes inadvertently, have exactly the same effect, that is the generator remains disconnected in both cases. The two types of failure can be lumped together is state g_1 (Fig.6-3). The failure rate ν_1 and the repair rate ρ_1 properly account for both types of failure and repair. If instead during the repair of the generator the additional contacts are closed (because of a failure or of an operating mistake) and the switch closes inadvertently, the generator windings will be connected to the grid (transition from g_3 to g_5). The failure rate σ_1 accounts for this type of failure.

(c) When the repair of the generator I has been completed, the circuit breaker will be tested (in order to check that it is intact) before closing the additional contactors. After having verified that the circuit breaker is functioning, the generator I will be started, the additional contactors will be closed and finally the circuit breaker will be closed. This means that the return to the operating conditions (i.e. to the closed position) can only take place from the state g_3 of the state diagram of Fig.6-3 (transition rate μ_I).

(d) When the switch is intact in the closed position (state g_4 in Fig.6-3) and fails open, two possibilities exist:

(i) the failure of D causes I to fail, i.e. transition from g_4 to g_1 with failure rate $\alpha\nu_2$ where ν_2 is the failure rate of D opening inadvestently and α is the conditional probability of I failing due to the failure of D.

(ii) the failure of D does not cause I to fail, i.e. transition from g_4 to g_2 with failure rate $(1-\alpha)\nu_2$.

(e) When the switch fails open in the closed position (i.e. opens inadvertently, state g_2 in Fig.6-3) the following actions will take place: (1) the generator I will be immediately stopped, the switch will be driven in the open position and the additional contactors will be opened, (2) the switch will be repaired and (3) the generator will be started again. The three actions are properly lumped together in the repair rate ρ_2.

(f) When the switch is in the closed position and fails closed (state g_6 in Fig. 6-3), the failure will remain undetected until either the next inspection occurs or the generator I fails. For this reason two transitions are possible from state g_6 and exactly:

(i) If the generator fails before the failure of the switch is detected and repaired, there will be a transition (transition rate λ_I) from state g_6 to state g_5 (Fig. 6-3), i.e. the switch changes its position (from closed to open) but it remains failed closed. As soon as the switch is in state g_5, the failure will be immediately detected and the switch will be repaired first (transition from g_5 to g_3, transition rate ω_1).

(ii) The failure of the switch is detected before the generator I fails. In this case the generator will be immediately disconnected from the grid and stopped. Since this type of failure has the same effect as that of switch failed open with I intact, we can lump it together with the latter into state g_2. We shall have therefore a transition rate ω_2 from g_6 to g_2.

With reference to the state diagram of Fig. 6-3, we can write the following equation.

$$E\{G_2\} + E\{G_4\} + E\{G_6\} = E\{I_2\} \qquad (6\text{-}7)$$

We consider here only the asymptotic solution ($t\to\infty$). With reference to Fig. 6-3, we can write the following two equations (states g_6 and g_2)

$$E\{G_6\} = \frac{\sigma_2}{\lambda_I + \omega_2} E\{G_4\} \qquad (6\text{-}8)$$

and

$$E\{G_2\} = E\{G_4\}\frac{(1-\alpha)\nu_2}{\rho_2} + E\{G_6\}\frac{\omega_2}{\rho_2} \qquad (6\text{-}9)$$

Taking into account Eqs. 6-8 and 6-9, Eq. 6-7 becomes

$$E\{G_4\}\left[1 + \frac{(1-\alpha)\nu_2}{\rho_2} + \left(1+\frac{\omega_2}{\rho_2}\right)\frac{\sigma_2}{\lambda_I+\omega_2}\right] = E\{I_2\} \qquad (6\text{-}10)$$

and

$$E\left\{D_3 \mid I_2\right\} = \frac{E\left\{G_4\right\}}{E\left\{I_2\right\}} = \frac{1}{1+\frac{(1-\alpha)\nu_2}{\rho_2}+(1+\frac{\omega_2}{\rho_2})\frac{\sigma_2}{\lambda_I+\omega_2}} \tag{6-11}$$

From Eqs. 6- 8 and 6-11 we get

$$E\left\{D_2 \mid I_2\right\} = \frac{E\left\{G_6\right\}}{E\left\{I_2\right\}} = \frac{\sigma_2/(\lambda_I+\omega_2)}{1+\frac{(1-\alpha)\nu_2}{\rho_2}+(1+\frac{\omega_2}{\rho_2})\frac{\sigma_2}{\lambda_I+\omega_2}} \tag{6-12}$$

From Eqs. 6- 9 6-11 and 6-12, we get

$$E\left\{D_1 \mid I_2\right\} = \frac{E\left\{G_2\right\}}{E\left\{I_2\right\}} = \frac{\frac{(1-\alpha)\nu_2}{\rho_2}+\frac{\omega_2}{\rho_2}\frac{\sigma_2}{\lambda_I+\omega_2}}{1+\frac{(1-\alpha)\nu_2}{\rho_2}+(1+\frac{\omega_2}{\rho_2})\frac{\sigma_2}{\lambda_I+\omega_2}} \tag{6-13}$$

With reference to Fig. 6- 3 we can write the following equations

$$E\left\{G_1\right\} + E\left\{G_3\right\} + E\left\{G_5\right\} = E\left\{I_1\right\} \tag{6-14}$$

$$E\left\{G_1\right\} = \frac{\nu_1}{\rho_1} E\left\{G_3\right\} + \frac{\alpha\nu_2}{\rho_1} E\left\{G_4\right\} \tag{6-15}$$

and

$$E\left\{G_5\right\} = \frac{\lambda_I}{\omega_1} E\left\{G_6\right\} + \frac{\sigma_1}{\omega_1} E\left\{G_3\right\} \tag{6-16}$$

The system of Eqs. 6-14 to 6-16 can be solved to give the three quantities $E\left\{G_3\right\}$, $E\left\{G_5\right\}$, and $E\left\{G_1\right\}$.

We have

$$E\{D_3 \mid I_1\} = \frac{E\{G_3\}}{E\{I_1\}} =$$

$$= \frac{1 - \frac{E\{I_2\}}{E\{I_1\}} \left[\frac{\lambda_I}{\omega_1} E\{D_2 \mid I_2\} + \frac{\alpha\nu_2}{\rho_1} E\{D_3 \mid I_2\} \right]}{1 + \frac{\nu_1}{\rho_1} + \frac{\sigma_1}{\omega_1}} \qquad (6\text{-}17)$$

$$E\{D_2 \mid I_1\} = \frac{E\{G_5\}}{E\{I_1\}} =$$

$$= \frac{\frac{\sigma_1}{\omega_1} + \frac{E\{I_2\}}{E\{I_1\}} \left[\frac{\lambda_I}{\omega_1} (1 + \frac{\nu_1}{\rho_1}) E\{D_2 \mid I_2\} - \frac{\sigma_1}{\omega_1} \frac{\alpha\nu_2}{\rho_1} E\{D_3 \mid I_2\} \right]}{1 + \frac{\nu_1}{\rho_1} + \frac{\sigma_1}{\omega_1}} \qquad (6\text{-}18)$$

and

$$E\{D_1 \mid I_1\} = \frac{E\{G_1\}}{E\{I_1\}} =$$

$$= \frac{\frac{\nu_1}{\rho_1} + \frac{E\{I_2\}}{E\{I_1\}} \left[\frac{\alpha\nu_2}{\rho_1} (1 + \frac{\sigma_1}{\omega_1}) E\{D_3 \mid I_2\} - \frac{\nu_1}{\rho_1} \frac{\lambda_I}{\omega_1} E\{D_2 \mid I_2\} \right]}{1 + \frac{\nu_1}{\rho_1} + \frac{\sigma_1}{\omega_1}} \qquad (6\text{-}19)$$

With reference to Fig. 6-3 we lump now the states g_1, g_3 and g_5 together on one side, and the states g_2, g_4 and g_6 on the other side. We get the state diagram of Fig. 6-4

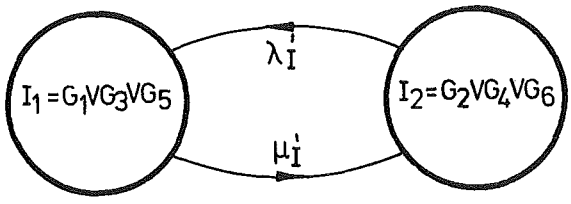


Fig. 6-4. State diagram of the super-component G of Fig. 6-3 with the states lumped into two groups.

The failure rate λ_I' and the repair rate μ_I' are given respectively by:

$$\lambda_I' = \frac{\lambda_I \left[E\{D_3 \wedge I_2\} + E\{D_2 \wedge I_2\} \right] + \alpha\nu_2 E\{D_3 \wedge I_2\}}{E\{D_1 \wedge I_2\} + E\{D_2 \wedge I_2\} + E\{D_3 \wedge I_2\}} =$$

$$= \lambda_I \left[E\{D_3 \mid I_2\} + E\{D_2 \mid I_2\} \right] + \alpha\nu_2 E\{D_3 \mid I_2\} \quad (6\text{-}20)$$

and

$$\mu_I' = \mu_I \frac{E\{D_3 \wedge I_1\}}{E\{I_1\}} = \mu_I E\{D_3 \mid I_1\} \quad (6\text{-}21)$$

Taking into account Eqs. 6-11 and 6-12, Eq. 6-20 becomes

$$\lambda_I' = \frac{\lambda_I \left[1 + \sigma_2/(\lambda_I + \omega_2) \right] + \alpha \nu_2}{1 + \frac{(1-\alpha)\nu_2}{\rho_2} + \frac{\sigma_2}{\lambda_I+\omega_2} + \frac{\sigma_2}{\rho_2} \cdot \frac{\omega_2}{\lambda_I+\omega_2}} \qquad (6-22)$$

We point out that in well designed and well maintained technical systems (sect. 4.5) the repair rates (μ_I;ρ_1;ρ_2;ω_1;and ω_2) are orders of magnitude larger than failure rates (λ_I; ν_1;ν_2;σ_1 and σ_2). This means that the following four relationships hold

$$\sigma_2/(\lambda_I + \omega_2) << 1 \qquad (6-23)$$

$$\sigma_2/\rho_2 << 1 \qquad (6-24)$$

$$(1-\alpha)\nu_2/\rho_2 << 1 \qquad (6-25)$$

and

$$\omega_2/(\lambda_I + \omega_2) \cong 1 \qquad (6-26)$$

Taking into account Eqs. 6-23 to 6-26., Eq. 6-22 becomes simply

$$\lambda_I' \cong \lambda_I + \alpha\nu_2 \qquad (6-27)$$

With reference to the state diagram of Fig. 6-4 we can write

$$\frac{E\{I_2\}}{E\{I_1\}} = \frac{\mu_I'}{\lambda_I'} \cong \frac{\mu_I'}{\lambda_I + \alpha\nu_2} \qquad (6-28)$$

In addition we have also (according to the requirements of sect.4.5)

$$\frac{\nu_1}{\rho_1} << 1 \qquad (6\text{-}29a)$$

$$\frac{\sigma_1}{\omega_1} << 1 \qquad (6\text{-}29b)$$

and

$$\frac{\alpha\nu_2}{\rho_1} << 1 \qquad (6\text{-}29c)$$

Taking into account Eqs. 6-29a to 6-29c it is easy to check that Eq. 6-17 gives a value of $E\{D_3|I_1\}$ very near to 1. For this reason, from Eq. 6-21 we simply get

$$\mu'_I \cong \mu_I \qquad (6\text{-}30)$$

Taking into account Eqs. 6-27 and 6-30 we can write

$$E\{I_1\} = \frac{\lambda_I+\alpha\nu_2}{\mu_I+\lambda_I+\alpha\nu_2} \qquad (6\text{-}31)$$

and

$$E\{I_2\} = \frac{\mu_I}{\mu_I+\lambda_I+\alpha\nu_2} \qquad (6\text{-}32)$$

Eqs. 6-31 and 6-32 tell us that the expectation of I_1 and of I_2 are almost equal to the expectations that one would calculate by assuming that the failure and the repair rates of I are invariant with respect to the state occupied by D, provided that its failure rate has been previously properly corrected (Eq. 6-27). In other words we would not make any appreciable error by assuming that I is <u>privileged</u>.

We point out that

$$\lambda_I + \alpha\nu_2 << \omega_2 \qquad (6\text{-}33)$$

Taking into account Eq. 6-33, Eqs. 6-11, 6-12 and 6-13 become respectively

$$E\{D_3|I_2\} \cong \frac{1}{1+\frac{(1-\alpha)\nu_2}{\rho_2}+\frac{\sigma_2}{\omega_2}+\frac{\sigma_2}{\rho_2}} \qquad (6\text{-}34)$$

$$E\{D_2|I_2\} \cong \frac{\sigma_2/\omega_2}{1+\frac{(1-\alpha)\nu_2}{\rho_2}+\frac{\sigma_2}{\omega_2}+\frac{\sigma_2}{\rho_2}} \qquad (6\text{-}35)$$

and

$$E\{D_1 | I_2\} \cong \frac{(1-\alpha)\frac{\nu_2}{\rho_2} + \frac{\sigma_2}{\rho_2}}{1 + \frac{(1-\alpha)\nu_2}{\rho_2} + \frac{\sigma_2}{\omega_2} + \frac{\sigma_2}{\rho_2}} \qquad (6\text{-}35)$$

We consider now in Eq. 6-19 the term

$$\frac{E\{I_2\}}{E\{I_1\}} \frac{\nu_1}{\rho_1} \frac{\lambda_I}{\omega_1} E\{D_2 | I_2\} \qquad (6\text{-}37)$$

Taking into account Eqs. 6-31; 6-32 and 6-35, we can write

$$\frac{E\{I_2\}}{E\{I_1\}} \frac{\nu_1}{\rho_1} \frac{\lambda_I}{\omega_1} E\{D_2 | I_2\} = \frac{\nu_1}{\rho_1} \frac{\mu_I}{\omega_1} \frac{\sigma_2/\omega_2}{1 + \frac{(1-\alpha)\nu_2}{\rho_2} + \frac{\sigma_2}{\omega_2} + \frac{\sigma_2}{\rho_2}} \frac{\lambda_I}{\lambda_I + \alpha\nu_2} \qquad (6\text{-}38)$$

In well designed and well maintained technical systems (section 4.5) the time required to repair a main component (the generator) is usually much larger than that required to repair its associated subordinate component (the circuit breaker). We have therefore

$$\mu_I/\omega_1 < 1 \qquad (6\text{-}39)$$

and

$$\mu_I/\rho_1 < 1 \qquad (6\text{-}40)$$

From Eq. 6-39 it follows that the term given by Eq. 6-38 is very small. We observe that we overestimate the value of $E\{D_1 | I_1\}$ if we delete in Eq. 6-19 the term given by Eq. 6-38. We point out also that the deletion of this term in Eq. 6-19 is a conservative assumption because we overestimate the conditional expectation of a variable associated with a failed state. In conclusion we set

$$E\{D_1 | I_1\} = \frac{(\nu_1 + \alpha\nu_2\mu_I/\lambda_I)/\rho_1}{1 + \nu_1/\rho_1 + \sigma_1/\omega_1} \qquad (6\text{-}41)$$

We consider now in Eq. 6-18 the term

$$\frac{E\{I_2\}}{E\{I_1\}} \frac{\sigma_1}{\omega_1} \frac{\alpha\nu_2}{\rho_1} E\{D_3 \mid I_2\} \cong \frac{\mu_I}{\lambda_I + \alpha\nu_2} \frac{\alpha\nu_2}{\rho_1} \frac{\sigma_1}{\omega_1} \tag{6-42}$$

Taking into account Eq. 6-40 and that in well designed and well maintained technical systems we certainly have

$$\alpha\nu_2 << \lambda_I \tag{6-43}$$

we can conclude that the term 6-42 is small. We point out also that the deletion of this term in Eq. 6-18 is a conservative assumption because we overestimate the conditional expectation of a variable associated with a failed state. In conclusion, taking into account Eqs. 6-12, we set

$$E\{D_2 \mid I_1\} = \frac{(\sigma_1 + \mu_I\sigma_2/\omega_2)/\omega_1}{1 + \nu_1/\rho_1 + \sigma_1/\omega_1} \tag{6-44}$$

Eqs. 6-41 and 6-44 can be written as follows

$$E\{D_1 \mid I_1\} = \frac{\nu_1'/\rho_1}{1 + \nu_1'/\rho_1 + \sigma'_1/\omega_1} \tag{6-45}$$

and

$$E\{D_2 \mid I_1\} = \frac{\sigma_1'/\omega_1}{1 + \nu'_1/\rho_1 + \sigma_1'/\omega_1} \tag{6-46}$$

where

$$\nu_1' = \frac{\nu_1 + \alpha\nu_2\mu_I/\lambda_I}{1 - \mu_I\sigma_2/\omega_1\omega_2 - \alpha\nu_2\mu_I/\lambda_I\rho_1} \tag{6-47}$$

and

$$\sigma_1' = \frac{\sigma_1 + \mu_I \sigma_2 / \omega_2}{1 - \mu_I \sigma_2 / \omega_1 \omega_2 - \alpha \nu_2 \mu_I / \lambda_I \rho_1} \qquad (6\text{-}48)$$

The conditional expectation $E\{D_3 | I_1\}$ can be calculated from the following equation

$$E\{D_1 | I_1\} + E\{D_2 | I_1\} + E\{D_3 | I_1\} = 1 \qquad (6\text{-}49)$$

Taking into account Eqs. 6-45 and 6-46, we get from Eq. 6-49

$$E\{D_3 | I_1\} = \frac{1}{1 + \nu_1'/\rho_1 + \sigma_1'/\omega_1} \qquad (6\text{-}50)$$

In conclusion the state diagram of Fig. 6-3 can be approximatively replaced by that of Fig. 6-5.

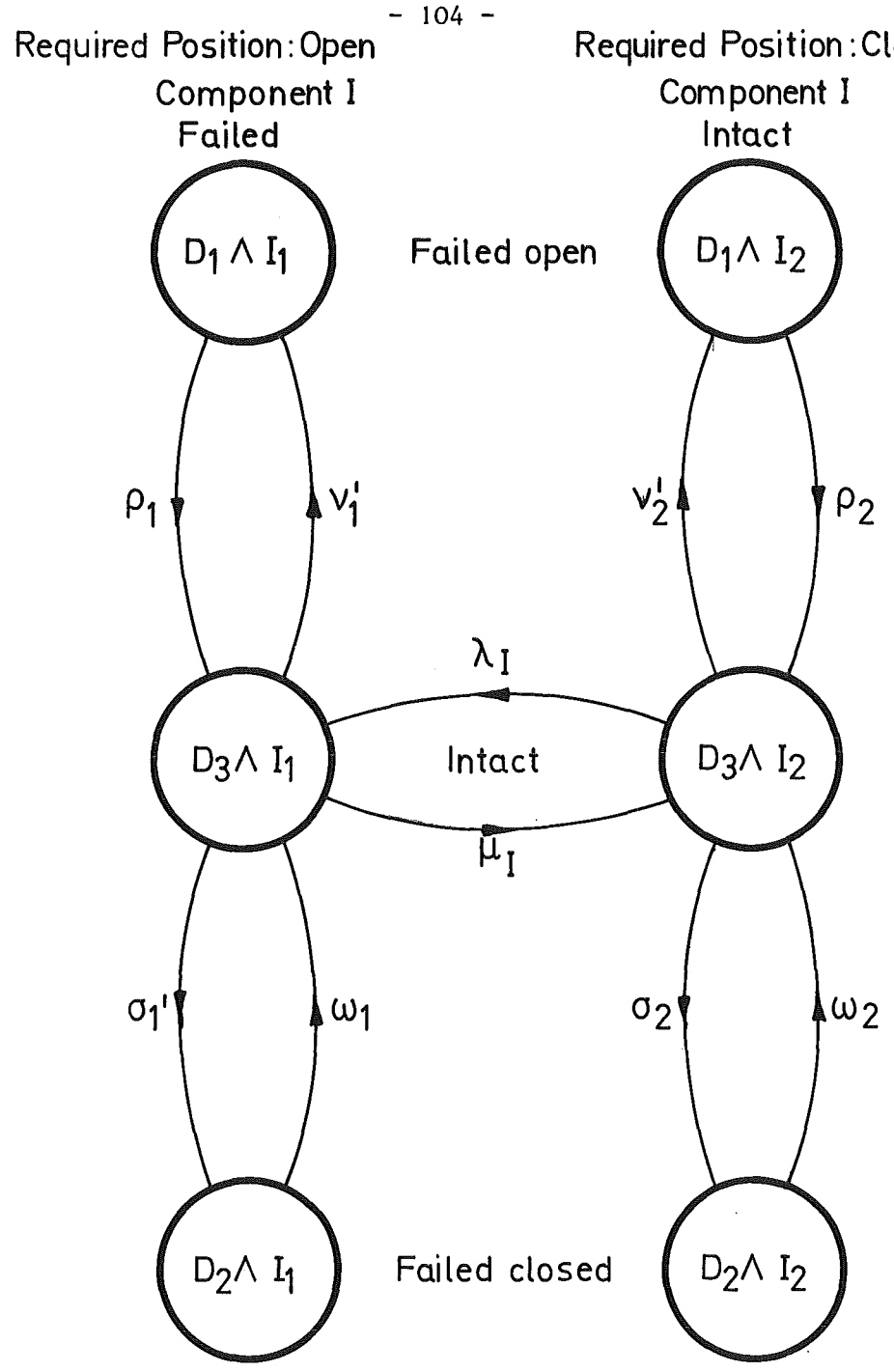
We recall the theory of section 5.4 on homogeneous dependence. If we assume that the bipolar switch is parent to none of the master components of the system to which it belongs, we can say that the bipolar switch is approximately homogeneously dependent. We have to correct the failure rates ν_1' and σ_1' by introducing a correcting coefficient similar to that of Eq.5-88. The corrected failure rates are ν_1'' and σ_1'', which are given by the following equations.

$$\nu_1'' = \nu_1' \frac{\nu_1' + \rho_1 + \mu_I}{\nu_1' + \rho_1 - \nu_1' \mu_I / \rho_1} \qquad (6\text{-}51)$$

and

$$\sigma_1'' = \sigma_1' \frac{\sigma_1' + \omega_1 + \mu_I}{\sigma_1' + \omega_1 - \sigma_1' \mu_I / \omega_1} \qquad (6\text{-}52)$$

The tables of Fig. 6-6 and Fig. 6-7 give a synthetic overview of the equations of the bipolar switch.



$$\nu_1' = \frac{\nu_1 + \alpha\nu_2\mu_I/\lambda_I}{1 - \mu_I\sigma_2/\omega_1\omega_2 - \alpha\nu_2\mu_I/\lambda_I\rho_1} \qquad \lambda_I' = \lambda_I + \alpha\nu_2$$

$$\sigma_1' = \frac{\sigma_1 + \mu_I\sigma_2/\omega_2}{1 - \mu_I\sigma_2/\omega_1\omega_2 - \alpha\nu_2\mu_I/\lambda_I\rho_1} \qquad \nu_2' = \sigma_2 + (1-\alpha)\nu_2$$

Fig. 6-5: State Diagram Equivalent to that of Fig. 6-3.

$$\nu_1' = \frac{\nu_1 + \alpha\nu_2\mu_I/\lambda_I}{1 - \mu_I\sigma_2/\omega_1\omega_1 - \alpha\nu_2\mu_I/\lambda_I\omega_2\rho_1} \quad (1)$$

$$\sigma_1' = \frac{\sigma_1 + \mu_I\sigma_2/\omega_2}{1 - \mu_I\sigma_2/\omega_1\omega_2 - \alpha\nu_2\mu_I/\lambda_I\omega_2\rho_1} \quad (2)$$

$$\nu_1'' = \nu_1' \frac{\nu_1' + \rho_1 + \mu_I}{\nu_1' + \rho_1 - \nu_1'\mu_I/\rho_1} \quad (3)$$

$$\sigma_1'' = \sigma_1' \frac{\sigma_1' + \omega_1 + \mu_I}{\sigma_1' + \omega_1 - \sigma_1'\mu_I/\omega_1} \quad (4)$$

$$\lambda_I' = \lambda_I + \alpha\nu_2 \quad (5)$$

$$\nu_2' = \sigma_2 + (1 - \alpha)\nu_2 \quad (6)$$

Fig. 6-6. 1st Table of the equations of the bipolar switch

$$E\{D_1 \mid I_1\} = \frac{\nu_1''/\rho_1}{1 + \nu_1''/\rho_1 + \sigma_1''/\omega_1} \tag{7}$$

$$E\{D_2 \mid I_1\} = \frac{\sigma_1''/\omega_1}{1 + \nu_1''/\rho_1 + \sigma_1''/\omega_1} \tag{8}$$

$$E\{D_3 \mid I_1\} = \frac{1}{1 + \nu_1''/\rho_1 + \sigma_1''/\omega_1} \tag{9}$$

$$E\{D_1 \mid I_2\} = \frac{\nu_2'/\rho_2}{1 + \nu_2'/\rho_2 + \sigma_2/\omega_2} \tag{10}$$

$$E\{D_2 \mid I_2\} = \frac{\sigma_2/\omega_2}{1 + \nu_2'/\rho_2 + \sigma_2/\omega_2} \tag{11}$$

$$E\{D_3 \mid I_2\} = \frac{1}{1 + \nu_2'/\rho_2 + \sigma_2/\omega_2} \tag{12}$$

Fig. 6-7. 2nd Table of the equations of the bipolar switch.

7. FAULT TREE SYMBOLOGY

The graphical symbology of a fault tree which is being used here is derived from that proposed by Fussell /7/ with some modifications and some additional symbols.

The symbols have been organized in two tables, namely

A. Table of Variables (Fig. 2-1)
B. Table of Basic Gates (Fig. 2-2)

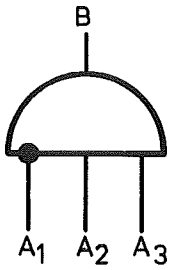
The two tables are self-explanatory so that only a few additional comments are needed for a correct use of the symbols contained in them.

1. The House (Table of Variables) is used to modify the structure of the fault tree. This is obtained by properly assigning to the House either the constant value 1 or 0.

2. Transfer IN and Transfer OUT (Table of Variables) are used in the case in which a variable is at the same time an output (Transfer OUT) from a gate and input (Transfer IN) to some other gates which are located (in the drawing of the fault tree) far away one from the other.

3. If an input to a gate (Tables of Basic Gates) is marked with a point, it means that the input variable is complemented (negated) before entering the gate.

For instance we have



$$B = \bar{A}_1 \wedge A_2 \wedge A_3$$

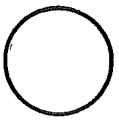
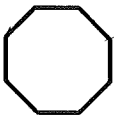
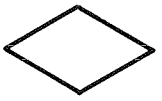
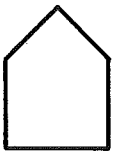
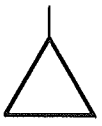
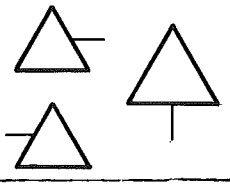
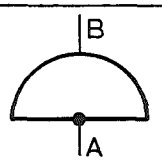
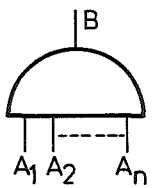
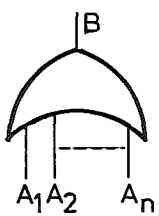
No.	Symbol	Denomination	Meaning
1		Rectangle	Variable Description
2		Circle	A primary variable belonging to a privileged component.
3		Octagon	A primary variable belonging to an unprivileged component.
4		Diamond	A non-primary variable which would require dissection into more basic variables, but that for some reasons has not been further dissected.
5		House	A variable whose domain of definition contains only one value , that is a variable which is constant and always takes either the value 1 or 0.
6		Transfer IN	A connecting or transfer symbol indicating a variable entering the fault tree.
7		Transfer OUT	A connecting or transfer symbol indicating a variable going out from the fault tree.

Fig. 7-2. Table of variables

No.	Symbol	Denomination	Boolean Notation	Output/Inputs Relationship	Rules for the Generation of the Truth Table
1		NOT	$B = \overline{A}$	$B = 1 - A$	Output takes the value 1 if predecessor takes the value 0 and vice versa.
2		AND	$B = \bigwedge_{i=1}^{n} A_i$	$B = \min(A_1; A_2 . ; A_n)$	Output takes the value 1 if and only if all predecessors take the value 1, and the value 0 if at least one of the predecessors takes the value 0.
3		OR	$B = \bigvee_{i=1}^{n} A_i$	$B = \max(A_1; A_2 . ; A_n)$	Output takes the value 1 if at least one of the predecessors takes the value 1, and the value 0 if and only if all predecessors take the value 0.

Note: A marked point at the input of a gate means that the input variable is negated before entering the gate.

Fig. 7-2. Table of Basic Gates.

8. CONSTRUCTION OF A FAULT TREE. AN EXAMPLE

Fig. 8-1 shows a very simplified electric power supply system (EPSS) consisting of the bus bars C which are supplied either by the grid B or by the electric generator A. Grid and electric generator are connected in parallel to the bus bars respectively through the electrically operated circuit breakers F and L. The dotted lines (with arrows) indicate that the position (open or closed) of each circuit breaker depends upon the state (failed or intact) of the component with which the circuit breaker is associated.

The circuit breakers in Fig. 8-1 are shown in the position open (coil deenergized). In normal operating conditions both circuit breakers F and L are closed (coil energized) and the generator A supplies electric power to the bus bars C as well as to the grid B. If the generator A fails the circuit breaker L opens and the grid feeds the bus bars C. If the network B fails the circuit breaker F opens and the generator A feeds the bus bars C only. The function of each circuit breaker is that of disconnecting its associated component (master component) when this fails. If the circuit breaker fails to open, no electric voltage will be available at the bus bars C.

The circuit breaker L has also the additional function of disconnecting the generator A in the case that the grid B fails and the circuit breaker F fails to open the circuit. This is in order to avoid that a failure of the grid causes the generator to fail. For a similar reason the circuit breaker F will open in the case in which the generator A fails and the circuit breaker L fails to open the circuit. In addition, also in the case in which both circuit breakers open the circuit (but e.g. not fast enough), the possibility exists that A by failing may cause the failure of B and vice versa (a failure of B may cause A to fail).

One can account for these cross correlated failures of A and B by assuming that when A fails there is a probability that B fails too (and vice versa). This is equivalent saying that A is the master of B and B is the master of A.

For the sake of simplicity it will be assumed in our example that the bus bars C by failing do not cause any secondary failure of A as well as of B.

The primary components with associated states are shown in the table of Fig. 8-2. Here for each primary component the inhibitors are listed in the corresponding column. The master component (in our example A and B), are also shown.

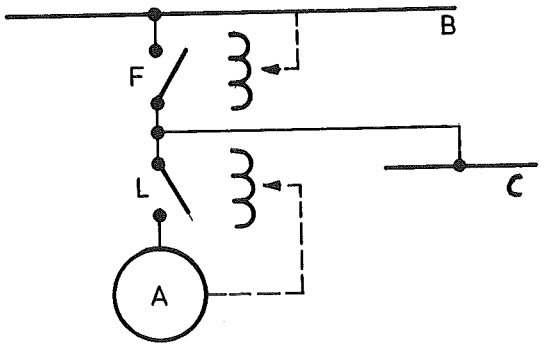


Fig. 8-1. Schematic diagram of a simplified electric power supply system (EPSS).

Primary Component		Master Component	State	
Denomination	Symbol		Denomination	Symbol of primary variable
Generator	A	B	failed	A_1
			intact	A_2
Network	B	A	failed	B_1
			intact	B_2
Bus bars	C		failed	C_1
			intact	C_2
Circuit Breaker F	F	B	failed open	F_1
			failed closed	F_2
			intact	F_3
Circuit Breaker L	L	A	failed open	L_1
			failed closed	L_2
			intact	L_3

Fig. 8-2. Table of the primary components of the EPSS.

Note that in our example the master components of F and L are also primary components. However, in general the master components are not primary (i.e. the variables belonging to them are not primary). In this case additional information must be given to identify these master components.

We can now proceed to define the TOP variable. The EPSS is failed if no electric voltage is available at the bus bars C. We have therefore

TOP = No voltage at bus bars C

We observe that the absence of voltage at the bus bars C is caused either by the failure of the bus bars C or by the fact that no voltage arrives at C. In this way we have dissected the TOP variable into the disjunction of two other variables namely "bus bars C failed" and "no voltage at the input of bus bars C". This dissection is graphically shown in Fig. 8-3, where the OR gate G01 has the TOP as output and the other two above defined variables as inputs.

We point out that the probability data associated with the variable "bus bars C failed" are available from reliability data banks. This variable is therefore a primary variable. We call it C_1 and we draw a circle in Fig. 8-3 because C is a privileged primary component (see table of Fig. 8-2).

We now dissect the variable "No voltage at the input of bus bars C".

We notice that the absence of voltage at the input of bus bars C can be caused either by a "non-disconnected failure or by an "interruption of the continuity of the electric circuit". This dissection is shown graphically in Fig. 8-4.

The process of dissection can be carried further on until all variables are primary variables. The complete fault tree is shown in Fig. 8-5. Note that the variables A_1, B_1, L_1, L_2, L_3, F_1, F_2 and F_3 are all represented by octagons because they belong to unprivileged components.

The fault tree of Fig. 8-5 has been redrawn in simplified form in Fig. 8-6 without rectangles (i.e. without variable descriptions).

Since there are different possible ways of dissecting the variables, different fault trees of the same TOP can be drawn. The fault tree of Fig. 8-7 has exactly the same TOP variable of that of Fig. 8-6. In general different people generate different fault trees for the same TOP variable.

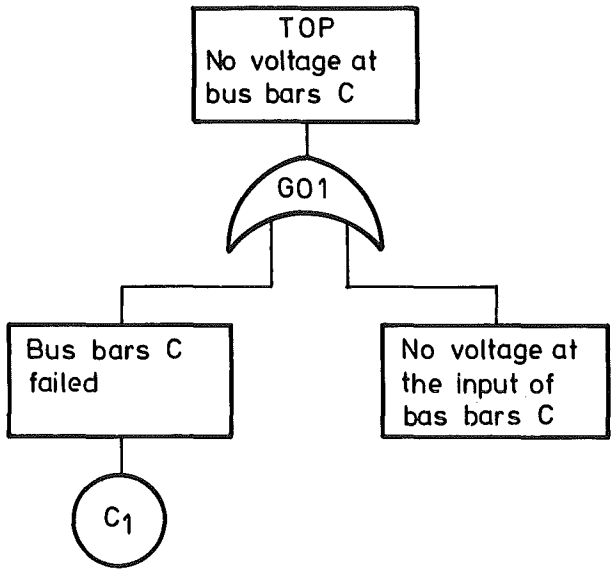


Fig. 8-3. Partial fault tree of the EPPS (1st step)

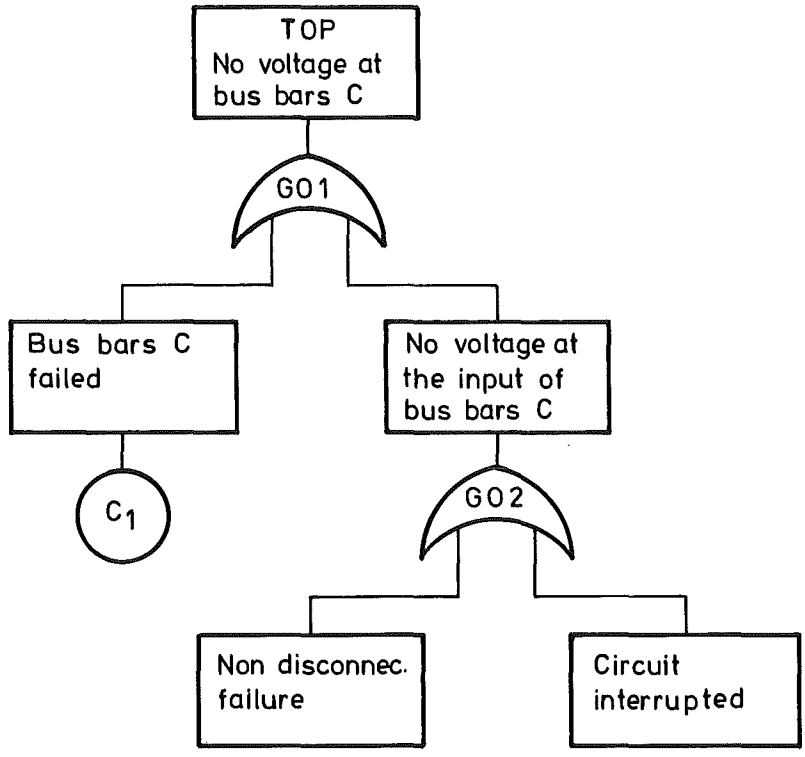


Fig. 8-4. Partial fault tree of the EPPS (2nd step)

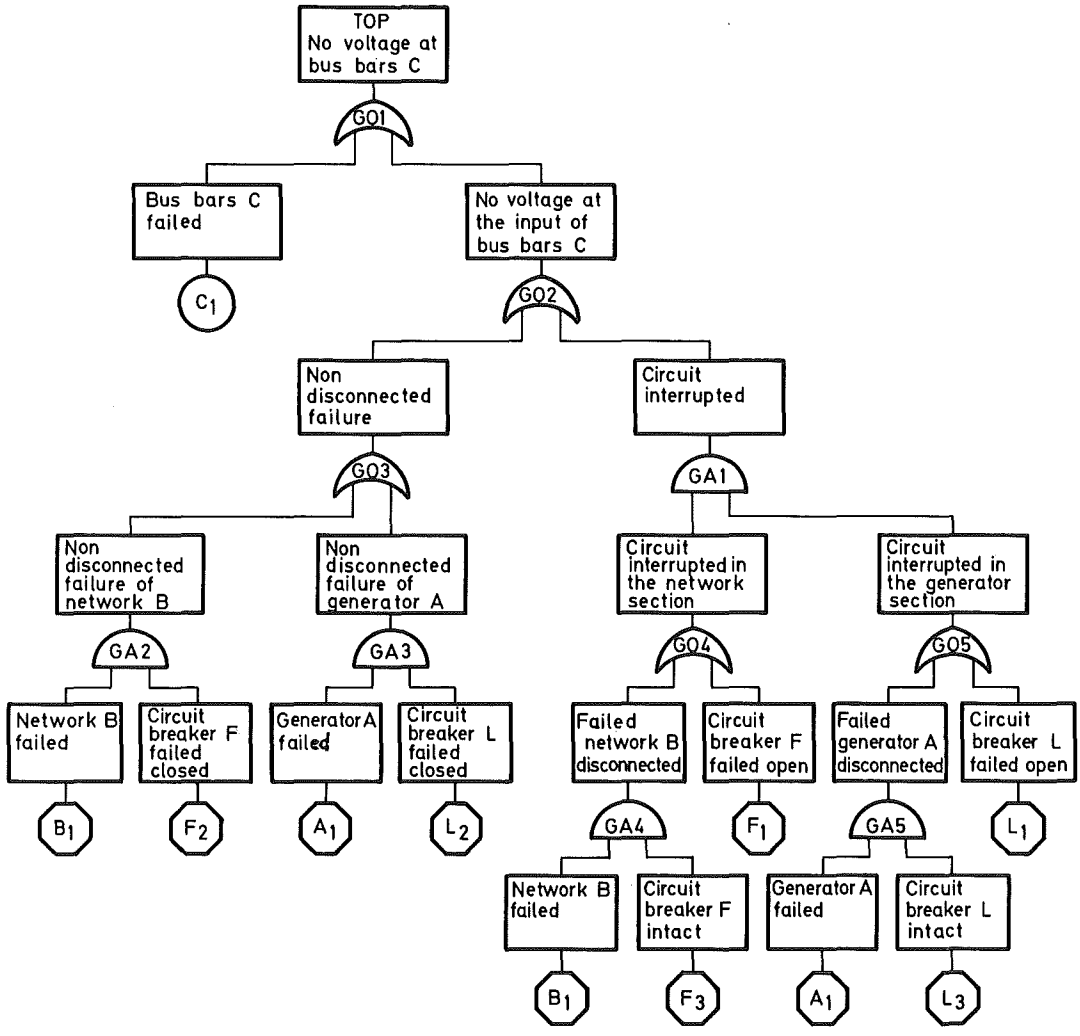


Fig. 8-5. Fault Tree of the EPSS.

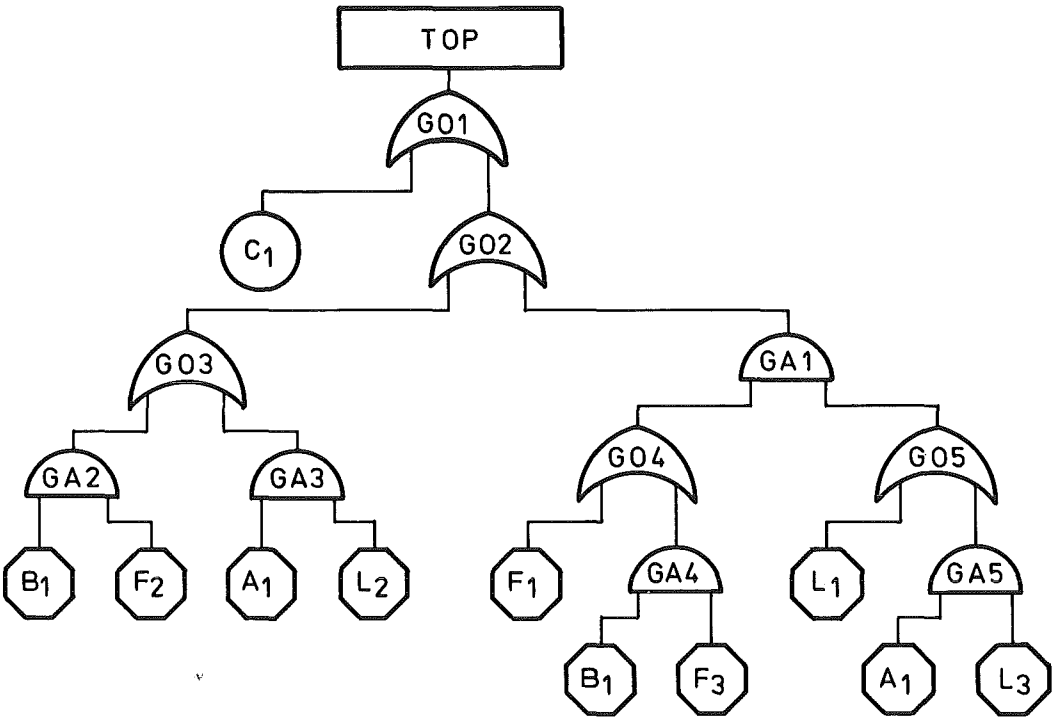


Fig. 8-6. Fault tree of the EPPS (without variable descriptions)

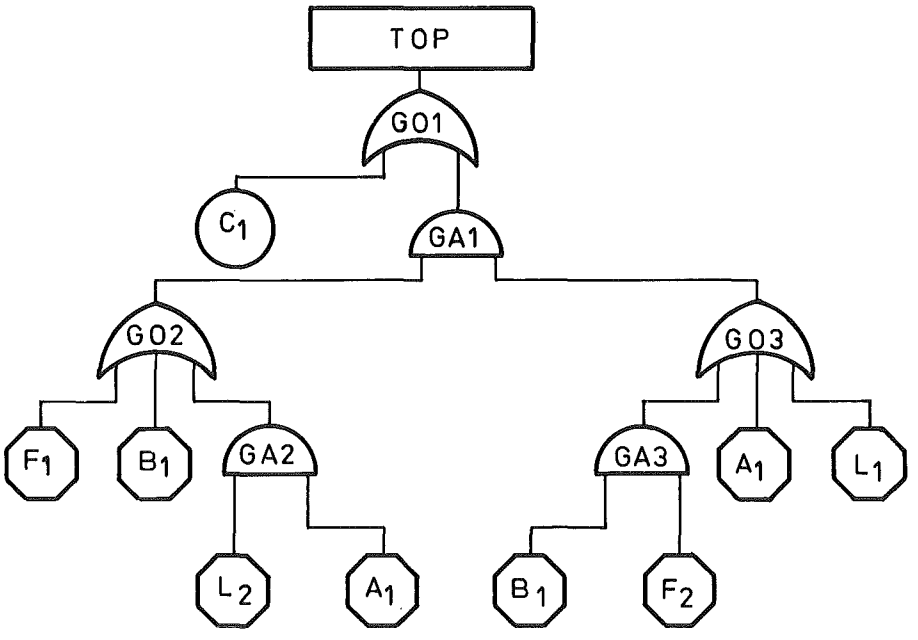


Fig. 8-7. Fault tree of the EPPS (Alternative)

9. MODIFIED FAULT TREE. OCCURRENCE PROBABILITY OF THE PRIMARY EVENTS

The probability data related to the primary variables of the system described in the previous section are given in the table of Fig. 9-1. These data have only the purpose to illustrate the method: they do not refer to any particular existing EPSS. Here we assume that all failure and repair rates of the primary components are constant. The transition rates are identified as follows. The primary variable of the row refers to the state before the transition (state of departure). The number of the column identifies the state after the transition (state of arrival). The two primary components A and B are characterized by two states (intact and failed). The failure of each of the two above primary components is assumed to be caused either inherently or by the failure of the other primary component. We shall indicate with a_1 and b_1 respectively the failed states of A and B and with a_2 and b_2 the intact states. The inherent failure rates are respectively λ_A and λ_B (both constant). If A fails first there is a constant probability K_B that this causes the failure of B. In this case the transition $b_2 \rightarrow b_1$ is the conditioned transition and the transition $a_2 \rightarrow a_1$ is the conditioning transition. If instead B fails first (conditioning transition $b_2 \rightarrow b_1$) there is a constant probability K_A that this causes the failure of A (conditioned transition $a_2 \rightarrow a_1$). Both primary components A and B are assumed to be repairable independently. The repair rates μ_A and μ_B are assumed to be both constant.

We recall the theory of the bipolar switch of chapter 6. We refer to Eq. 5 of the table of Fig. 6-6 which tells us that the failure rate of the generator I must be increased to account for the failure of the generator caused by the associated circuit breaker opening inadvertently (transition from g_4 with failure rate $\alpha\nu_2$ in Fig. 6-3). The numerical values of λ_A and λ_B given in the table of Fig. 9-1 are assumed to have already been corrected for this additional induced failure.

Since A is the master component of B and B is the master component of A, the smallest privileged super component associated with both of them is the super component G which results from the product of A and B.

The state diagram of super-component G is shown in Fig. 9-2.

With reference to the state diagram of Fig. 9-2, we can now express the primary variables of components A and B as functions of the primary variables of G. We have

$$A_1 = G_1 V G_3 \tag{9-1}$$

$$A_2 = G_2 V G_4 \tag{9-2}$$

$$B_1 = G_1 V G_2 \tag{9-3}$$

$$B_2 = G_3 V G_4 \tag{9-4}$$

We now replace in fault tree of Fig. 8-6 the primary variables A_1 and B_1 with the new primary variables G_1, G_2; G_3 and G_4 by making use of Eqs. 9-1 and 9-3. The new fault tree is shown in Fig. 9-3.

Primary Component	Master Component	Primary Variable	Transition Rates (hours^{-1})			Correlated Transitions		
			Master Variable	1	2	3	Conditioning Transition	Conditioned Transition	Conditional Probability
A	B	A_1			$\mu_A=10^{-3}$				
		A_2		$\lambda_A=10^{-4}$			$B_2 \rightarrow B_1$	$A_2 \rightarrow A_1$	$K_A=0.1$
B	A	B_1			$\mu_B=10^{-3}$				
		B_2		$\lambda_B=10^{-5}$			$A_2 \rightarrow A_1$	$B_2 \rightarrow B_1$	$K_B=0.1$
C		C_1			$\mu_c=5\cdot10^{-2}$				
		C_2		$\lambda_c=10^{-6}$					
F	B	F_1	B_1			$\rho_1=10^{-2}$			
		F_2				$\omega_1=10^{-2}$			
		F_3		$\nu_1=10^{-6}$	$\sigma_1=1.5\cdot10^{-5}$				
		F_1	B_2			$\rho_2=10^{-2}$			
		F_2				$\omega_2=10^{-2}$			
		F_3		$\nu_2=1.5\cdot10^{-5}$	$\sigma_2=5\cdot10^{-6}$				
L	A	L_1	A_1			$\eta_1=10^{-2}$			
		L_2				$\gamma_1=10^{-2}$			
		L_3		$\varepsilon_1=10^{-6}$	$\zeta_1=1.5\cdot10^{-5}$				
		L_1	A_2			$\eta_2=10^{-2}$			
		L_2				$\gamma_2=10^{-2}$			
		L_3		$\varepsilon_2=1.5\cdot10^{-5}$	$\zeta_2=5\cdot10^{-6}$				

Fig. 9-1. Table of the input probability data of the primary variable (System of Fig. 8-1).

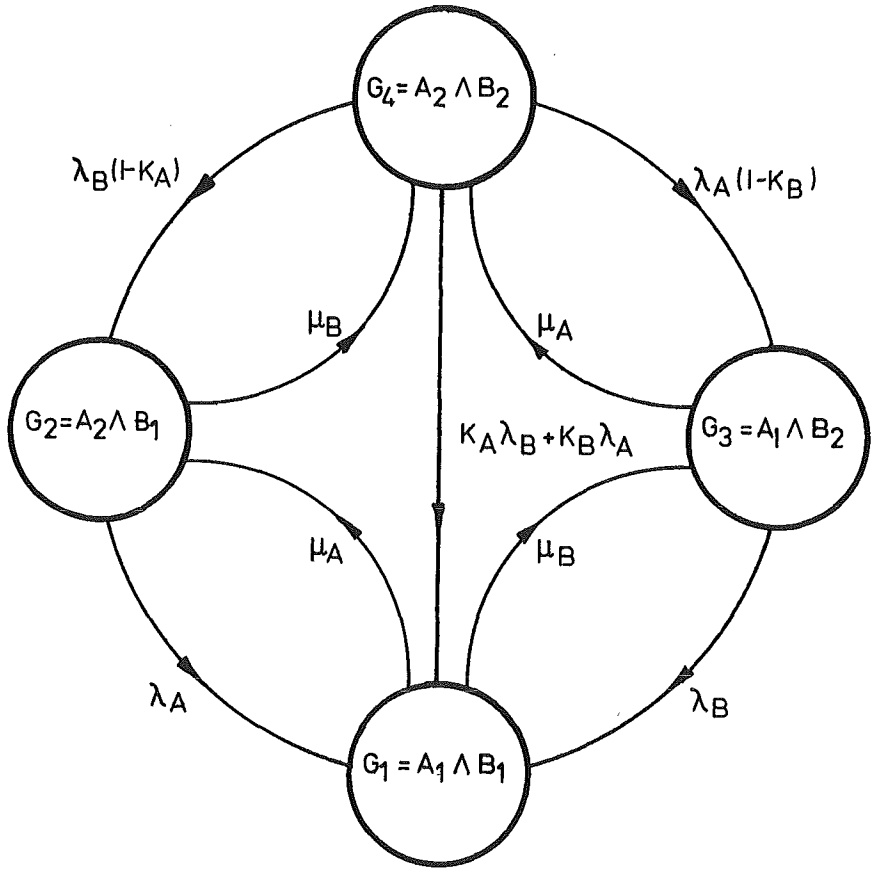


Fig. 9-2. State diagram of the smallest privileged super-component G associated with A and B.

In the fault tree of Fig. 9-3 the primary variables A_1 and B_1 have been replaced respectively by the OR Gates G07 (inputs G_1 and G_3) and G06 (inputs G_1 and G_2). Note that the primary variables G_1; G_2 and G_3 are represented by circles because they belong to a privileged component. In fact their expectations can be calculated by solving the state diagram of Fig. 9-2. The new primary variables have been introduced also in the fault tree of Fig. 8-7 (see Fig.9-4).

We point out the G is a privileged primary component. Due to Eqs. 9-1 to 9-4, we can say, that A and B have become now privileged components. They are however not any more primary. We can therefore say that B is the Inhibitor of the circuit breaker F and A is the Inhibitor of the circuit breaker L.

In other words in the fault trees of Figs. 9-3 and 9-4 the survived unprivileged primary components (namely F and L) have only master components which are privileged, i.e. Inhibitors.

The expectation of the primary variables G_1; G_2; G_3 and G_4 can now be calculated. We point out that the state diagram of Fig. 9-2 and that of Fig. 5-1 are the same provided that

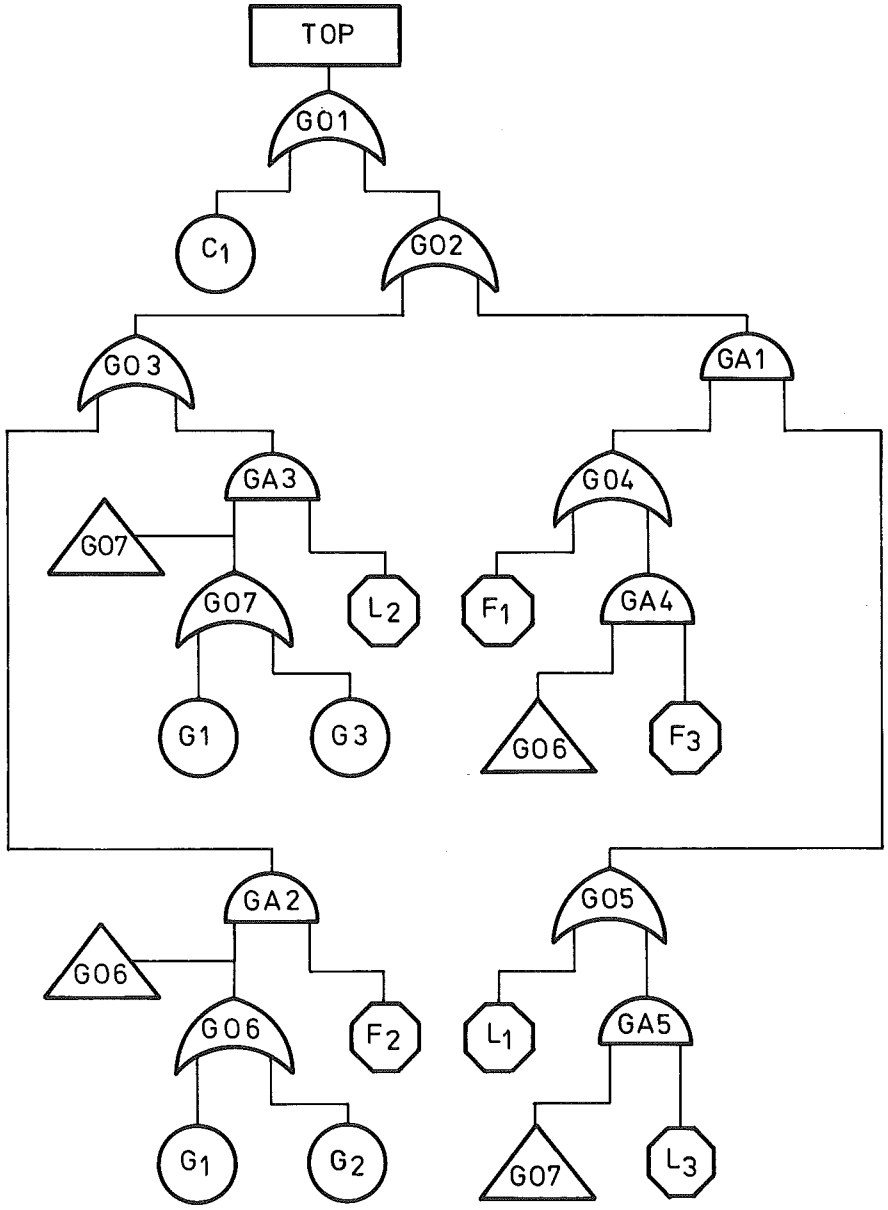


Fig. 9-3. Modified fault tree of the EPPS

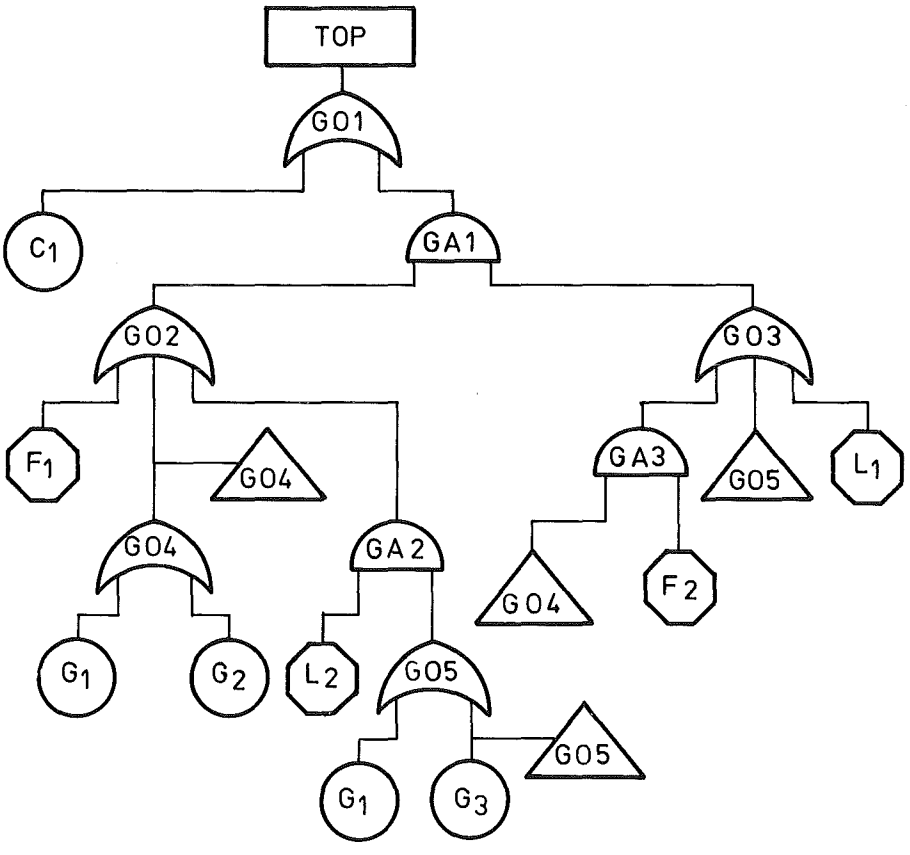


Fig. 9-4. Modified fault tree of the EPPS (Alternative)

$$\lambda_{AB} = K_A \lambda_B + K_B \lambda_A \tag{9-5}$$

$$\lambda'_B = \lambda_B (1 - K_A) \tag{9-6}$$

$$\lambda'_A = \lambda_A (1 - K_B) \tag{9-7}$$

$$\lambda''_B = \lambda_B \tag{9-8}$$

$$\lambda''_A = \lambda_A \tag{9-9}$$

We can therefore apply the theory developed in section 5.2. We consider here the asymptotic ($t \to \infty$) solution only. Taking into account Eqs. 9-5 to 9-9, Eqs.5-18 and 5-19 become respectively

$$\alpha_2 = \mu_A \left[\lambda_B(\lambda_A + \lambda_B + \mu_A + \mu_B) + K_B \lambda_A \mu_A - K_A \lambda_B \mu_B \right] \tag{9-10}$$

and

$$\alpha_3 = \mu_B \left[\lambda_A(\lambda_A + \lambda_B + \mu_A + \mu_B) - K_B \lambda_A \mu_A + K_A \lambda_B \mu_B \right] \tag{9-11}$$

We take the numerical values of Table 9-1. We get

$$\alpha_2 = 10^{-3}\left[10^{-5}(10^{-4}+10^{-5}+10^{-3}+10^{-3}) + 0.1\cdot 10^{-4}\cdot 10^{-3} - 0.1\cdot 10^{-5}\cdot 10^{-3}\right] =$$

$$\simeq 3.01 \cdot 10^{-11} \ (\text{hours}^{-3}) \tag{9-12}$$

and

$$\alpha_3 = 10^{-3}\left[10^{-4}(10^{-4}+10^{-5}+10^{-3}+10^{-3}) - 0.1\cdot 10^{-4}\cdot 10^{-3} + 0.1\cdot 10^{-5}\cdot 10^{-3}\right]$$

$$= 2.02 \cdot 10^{-10} \ (\text{hours})^{-3} \tag{9-13}$$

From Eqs. 9-12 and 9-13, we get

$$\frac{\alpha_2}{\alpha_2+\alpha_3} = \frac{3.01 \cdot 10^{-11}}{2.32 \cdot 10^{-10}} \simeq 0.13 \tag{9-14}$$

and

$$\frac{\alpha_3}{\alpha_2 + \alpha_3} = 1 - 0.13 = 0.87 \qquad (9\text{-}15)$$

We write now Eqs.5-20 and 5-21 We get

$$\lambda = \frac{\alpha_2}{\alpha_2 + \alpha_3} \lambda_A + \frac{\alpha_3}{\alpha_2 + \alpha_3} \lambda_B = 2.17 \cdot 10^{-5} \text{ hours}^{-1} \qquad (9\text{-}16)$$

and

$$\mu = \frac{\alpha_2}{\alpha_2 + \alpha_3} \mu_B + \frac{\alpha_3}{\alpha_2 + \alpha_3} \mu_A = 10^{-3} \text{ hours}^{-1} \qquad (9\text{-}17)$$

We can now calculate Δ (Eq.5-28). Taking into account Eqs. 9-5, to 9-9, Eq.5-28 becomes

$$\Delta = (\lambda_A + \lambda_B)(\lambda + \mu_A + \mu_B) + \mu (\mu_A + \mu_B + K_A \lambda_B + K_B \lambda_A) \qquad (9\text{-}18)$$

Taking into account the numerical values of the table of Fig. 9-1 and Eqs. 9-16 and 9-17, we get

$$\Delta = (10^{-4} + 10^{-5})(2.17 \cdot 10^{-5} + 10^{-3} + 10^{-3}) +$$

$$+ 10^{-3} (10^{-3} + 10^{-3} + 0.1 \cdot 10^{-5} + 0.1 \cdot 10^{-4}) =$$

$$= 2.233 \cdot 10^{-6} \qquad (9\text{-}19)$$

Taking into account Eqs. 9-5 to 9-9, Eqs. 5-25 , 5-31 and 5-32 become respectively

$$E\{G_1\} = \frac{\lambda(\lambda_A + \lambda_B) + \mu(K_A \lambda_B + K_B \lambda_A)}{\Delta} =$$

$$= \frac{2.17 \cdot 10^{-5}(10^{-4} + 10^{-5}) + 10^{-3}(0.1 \cdot 10^{-5} + 0.1 \cdot 10^{-4})}{2.233 \cdot 10^{-6}} \cong$$

$$\cong 6 \cdot 10^{-3} \qquad (9\text{-}20)$$

$$E\{G_2\} = \frac{\alpha_2}{\alpha_2+\alpha_3} \quad \frac{(\mu_A+\mu_B)(\lambda_A+\lambda_B)}{\Delta} = 0.13 \frac{(10^{-3}+10^{-3})(10^{-4}+10^{-5})}{2.233 \cdot 10^{-6}} =$$

$$= 0.13 \cdot 9.85 \cdot 10^{-2} = 1.28 \cdot 10^{-2} \qquad (9\text{-}21)$$

$$E\{G_3\} = \frac{\alpha 3}{\alpha_2+\alpha_3} \quad \frac{(\mu_A+\mu_B)(\lambda_A+\lambda_B)}{\Delta} = 0.87 \cdot 9.85 \cdot 10^{-2} =$$

$$= 8.57 \cdot 10^{-2} \qquad (9\text{-}22)$$

We have also

$$E\{G_4\} = 1 - E\{G_1\} - E\{G_2\} - E\{G_3\} =$$

$$= 1 - 6 \cdot 10^{-3} - 1.28 \cdot 10^{-2} - 8.57 \cdot 10^{-2} = 0.8955 \qquad (9\text{-}23)$$

We go back now to the table of Fig. 9-1 and we consider the circuit breaker F. The circuit breaker F is a bipolar switch with Inhibitor B. The theory of the bipolar switch has been developed in chapter 6. By using this theory we can therefore easily calculate the conditional expectations of the primary variables of F.

We shall use the equations 7 to 12 of Fig. 6-7 and we shall assume that the numerical values of the transition rates given in the table of Fig. 9-1 have already been properly corrected according to the theory of the bipolar switch developed in chapter 6.

We have

$$E_1\{F_1\} = E\{F_1 \mid B_1\} = E\{F_1 \mid G_1 \vee G_2\} = \frac{\nu_1 / \rho_1}{1 + \frac{\nu_1}{\rho_1} + \frac{\sigma_1}{\omega_1}} =$$

$$= \frac{10^{-6} / 10^{-2}}{1 + \frac{10^{-6}}{10^{-2}} + \frac{10^{-5}}{10^{-2}}} \simeq 10^{-4} \qquad (9\text{-}24)$$

$$E_1\{F_2\} = E\{F_2|B_1\} = E\{F_2|G_1 \vee G_2\} =$$

$$= \frac{\sigma_1 / \omega_1}{1 + \frac{\nu_1}{\rho_1} + \frac{\sigma_1}{\omega_1}}$$

$$= \frac{1.5 \cdot 10^{-5} / 10^{-2}}{1 + \frac{10^{-6}}{10^{-2}} + \frac{10^{-5}}{10^{-2}}}$$

$$\cong 1.5 \cdot 10^{-3} \qquad (9\text{-}25)$$

$$E_1\{F_3\} = E\{F_3|B_1\} = E\{F_3|G_1 \vee G_2\} = 1 - E\{F_1|B_1\} - E\{F_2|B_1\} =$$

$$= 1 - 10^{-4} - 1.5 \cdot 10^{-3} = 0.9984 \qquad (9\text{-}26)$$

$$E_2\{F_1\} = E\{F_1|B_2\} = F\{F_1|\ G_3 \vee G_4\} = \frac{\nu_2 / \rho_2}{1 + \frac{\nu_2}{\rho_2} + \frac{\sigma_2}{\omega_2} + \frac{\sigma_2}{\rho_2}} \cong$$

$$\cong 1.5 \cdot 10^{-3} \qquad (9\text{-}27)$$

$$E_2\{F_2\} = E\{F_2|B_2\} = E\{F_2|G_3 \vee G_4\} = \frac{\sigma_2 / \omega_2}{1 + \frac{\nu_2}{\rho_2} + \frac{\sigma_2}{\omega_2} + \frac{\sigma_2}{\rho_2}} \cong$$

$$\cong 5 \cdot 10^{-4} \qquad (9\text{-}28)$$

$$E_2\{F_3\} = E\{F_3|B_2\} = E\{F_3|G_3 \vee G_4\} =$$

$$1 - E\{F_1|B_2\} - E\{F_2|B_2\} = 0.998 \qquad (9\text{-}29)$$

The conditional expectations of the primary variables of the circuit breaker L can be calculated in a similar way as we have shown in the case of F.

The table of Fig. 9-5 shows the conditional expectations of all primary variables of the fault tree of Fig. 9-3.

Primary Component	Inhibiting Variable	Primary Variable	Expectation	
			Symbol	Value
G		G_1	$E\{G_1\}$	$6 \cdot 10^{-3}$
		G_2	$E\{G_2\}$	$1.28 \cdot 10^{-2}$
		G_3	$E\{G_3\}$	$8.57 \cdot 10^{-2}$
		G_4	$E\{G_4\}$	0.8955
C		C_1	$E\{C_1\}$	$2 \cdot 10^{-5}$
		C_2	$E\{C_2\}$	0.99998
F	$G_1 \vee G_2$	F_1	$E_1\{F_1\}$	10^{-4}
		F_2	$E_1\{F_2\}$	$1.5 \cdot 10^{-3}$
		F_3	$E_1\{F_3\}$	0.9984
	$G_3 \vee G_4$	F_1	$E_2\{F_1\}$	$1.5 \cdot 10^{-3}$
		F_2	$E_2\{F_2\}$	$5 \cdot 10^{-4}$
		F_3	$E_2\{F_3\}$	0.998
L	$G_1 \vee G_3$	L_1	$E_1\{L_1\}$	10^{-4}
		L_2	$E_1\{L_2\}$	$1.5 \cdot 10^{-3}$
		L_3	$E_1\{L_3\}$	0.9984
	$G_2 \vee G_4$	L_1	$E_2\{L_1\}$	$1.5 \cdot 10^{-3}$
		L_2	$E_2\{L_2\}$	$5 \cdot 10^{-4}$
		L_3	$E_2\{L_3\}$	0.998

Fig. 9-5. Table of the expected values of the primary variables.

10. BOOLEAN OPERATIONS

10.1 Generalities

The reader must become acquainted with some terms which are currently used throughout this paper.

We say that a monomial X_j is a "prime implicant" (minimal cut set) of the boolean function TOP if (1) X_j implies the TOP ($X_j \wedge TOP = X_j$) and (2) any other monomial Y subsumed by X_j (i.e. obtained from X_j by replacing one of its literals with 1) does not imply the TOP ($Y \wedge TOP \neq Y$).

We shall call any disjunction of prime implicants, which is equivalent to the function TOP, a "base of the function TOP". The disjunction of all prime implicants has this property. We shall call it the "complete base". We shall describe as an "irredundant base" a base which ceases to be a base if one of the prime implicants occurring in it is removed (deleted). Boolean functions may have many irredundant bases. We shall call "smallest irredundant base" the irredundant base having the smallest number of prime implicants. There may be more than one base with the smallest number of prime implicants.

The identification of an irredundant base (or one of the smallest irredundant bases) of the boolean function TOP of a fault tree is carried out in three steps:

Step No. 1 Identification of the associated normal disjunctive form. Note that the associated normal disjunctive form has been already defined in chapter 2.

Step No. 2 Identification of the complete base starting from the associated normal disjunctive form.

Step No. 3 Extraction of an irredundant base (or one of the smallest irredundant bases) from the complete base.

After having identified an irredundant base of the TOP variable, some other transformations are carried out to get the boolean function in a form more suitable for probability calculations. For this purpose we have first to introduce the concept of simple boolean function.

> "A boolean function in said to be simple if it is possible to express it as a conjunction between a monomial (keystone monomial) and a normal disjunction of monomials, all monomials (including the keystone monomial) being pairwise mutually logically independent".

According to the above definition we have that a simple boolean function Y_i is expressed as follows:

$$Y_i = M_i \wedge \left(\bigvee_{s=1}^{n_i} P_{is}\right) \qquad (10\text{-}1)$$

where the M_i and the P_{is} are non zero boolean monomials satisfying the following two conditions

- the monomials P_{is} are pairwise logically independent, that is if a literal A_q appears in a monomial P_{is}, no other literal belonging to the same component will appear in any other monomial P_{ir} $(r \neq s \; r;s = 1;2...;n_i)$.
- each monomial P_{is} is logically independent of M_i.

The last two conditions can be expressed in the following way

If $A_q \wedge P_{is} = P_{is}$

then $0 \neq A_q \wedge M_i \neq M_i$ and

$0 \neq A_q \wedge P_{ir} \neq P_{ir} \qquad (r \neq s)$

AND

If $A_q \wedge M_i = M_i$

then $0 \neq A_q \wedge P_{is} \neq P_{is}$

In other words a primary component A can appear only once in a simple function Y_i: either in the monomial M_i or in one of the monomials P_{is}.

We can now specify the step No. 4.

Step No. 4 Expression of the TOP as a disjunction of pairwise mutually exclusive simple boolean functions.

This means that we want to get an expression of the TOP of the type

$$TOP = \bigvee_{i=1}^{Q} Y_i \qquad (10\text{-}2)$$

The monomials Y_i must be pairwise mutually exclusive, that is

$$Y_i \bigwedge Y_k = 0 \qquad i \neq k \quad (i;k = 1;2...;Q) \qquad (10\text{-}3)$$

Taking into account Eq. 10-1, it follows from Eq. 10-3 that the keystone monomials must be pairwise mutually exclusive, that is

$$M_i \bigwedge M_k = 0 \qquad (10\text{-}4)$$

The purpose of step No. 4 is to get an expression of the TOP which facilitates the operation of expectation. This will become clear in section 11 of this paper.

In order to calculate the conditional expectations of the unprivileged primary variables, it is necessary to identify for each unprivileged primary variable its associated inhibiting variable. We come therefore to the last boolean operation, that is to the step No. 5.

Step No. 5 Identification of the inhibiting variables to be associated with each simple function.

10.2 Step No. 1 - Identification of the Associated Normal Disjunctive Form

The variables of the fault tree are ordered in a list (table of variables). The literals are first listed. The acceptance criterion of a variable (gate) in the list is the following: the variable is accepted if and only if the input variables to the gate have already been accepted. If the gate satisfies the acceptance criterion it is written in the list. The ordering process comes to an end when all variables have been written in the list.

By simple inspection of the fault tree of Fig. 9-3 we get the table of variables of Fig. 10-1.

The algorithm to identify the monomials of the associated normal disjunctive form is the so called "downward algorithm" which is based on the principle already described in /7/ by Fussell and in /8/. Some additional features have been incorporated in the original downward algorithm so that the NOT gate and the multistate components can be handled. The algorithm begins with the TOP and systematically goes down through the tree from the highest to the lowest variable, that is from the bottom to the top of the ordered list of variables. The fault tree is developed in a table (table of monomials). The elements of the table are variables. Each row of the table is a monomial. The

Ordering Numbers	Variable	Boolean Relationship	Predecessors	Successors
1	C_1	-	-	GO1
2	G_1	-	-	GO6;GO7
3	G_2	-	-	GO6
4	G_3	-	-	GO7
5	L_1	-	-	GO5
6	L_2	-	-	GA3
7	L_3	-	-	GA5
8	F_1	-	-	GO4
9	F_2	-	-	GA2
10	F_3	-	-	GA4
11	GO6	OR	$G_1;G_2$	GA2;GA4
12	GO7	OR	G1;G3	GA3;GA5
13	GA5	AND	GO7;L_3	GO5
14	GA4	AND	GO6;F_3	GO4
15	GA3	AND	L_2;GO7	GO3
16	GA2	AND	GO6;F_2	GO3
17	GO4	OR	F_1;GA4	GA1
18	GO5	OR	L_1;GA5	GA1
19	GA1	AND	GO4;GO5	GO2
20	GO3	OR	GA2;GA3	GO2
21	GO2	OR	GO3;GA1	GO1
22	GO1(TOP)	OR	C_1;GO2	-

Fig. 10-1. Table of variables of the fault tree of Fig. 9-3.

number of elements contained in a row is called the length ot the row. Each time an OR gate is encountered new rows are produced (as many as the number of input variables to the gate). Each time an AND gate is encountered the length of the rows (in which the gate appears) is increased. Each time a NOT gate is encountered the input variable to the gate receives a negation mark. If a negated non primary variable is dissected, the gate type is replaced by its dual type (AND is changed into OR and vice versa) and the negation mark is transmitted to all input variables of the gate. If a primary variable is negated, it is replaced by an OR gate which has as input variables all the remaining primary variables belonging to the same primary component.

The process of dissection comes to an end when all the elements of the table of monomials are primary variables (literals).

In addition the three following simplification rules are applied:

1. Delete zero monomials, that is rows which contain at least one pair of mutually exclusive literals.
   $Cj_q \wedge Cj_k = 0$ for $q \neq k$ (exclusion law).

2. Delete the repeated literals of a monomial (row).
   $Cj_q \wedge Cj_q = Cj_q$ (idempower law).

3. Delete any subsuming monomial, that is any row which contains all elements of another row.
   $X_a \vee X_b = X_a$ if $X_a \wedge X_b = X_b$ (absorption law).

At the end of the process each row of the table of monomials is a monomial and the disjunction of all monomials is the normal disjunctive form of the TOP associated to the fault tree under considerations.

We now apply the above described procedure to the table of variables of Fig. 10-1. The example is self explanatory. We have

Ordering Number	Boolean Identity	Table of Monomials
	TOP = GO1	GO1
22	GO1 = C_1 V GO2	C_1 GO2
21	GO2 = GO3 V GA1	C_1 GO3 GA1

Ordering Number	Boolean Identity	Table of Monomials
20	GO3 = GA2 V GA3	C_1 / GA2 / GA3 / GA1
19	GA1 = GO4 ∧ GO5	C_1 / GA2 / GA3 / GO4 GO5
18	GO5 = L_1 V GA5	C_1 / GA2 / GA3 / GO4 L_1 / GO4 GA4

and so on.

At the end of the process the table of monomials will be that of Fig. 10-2.

We can therefore write the following boolean identity for the TOP (we indicate from now on the conjunction ∧ by means of the simpler multiplication symbol "·").

$$TOP = C_1 \vee F_2 \cdot G_1 \vee F_2 \cdot G_2 \vee L_2 \cdot G_1 \vee L_2 \cdot G_3 \vee G_1 \cdot F_3 \cdot L_1 \vee G_2 \cdot F_3 \cdot L_1 \vee$$

$$\vee F_1 \cdot G_1 \cdot L_3 \vee F_1 \cdot G_3 \cdot L_3 \vee F_1 \cdot L_1 \vee G_1 \cdot F_3 \cdot L_3 \qquad (10\text{-}5)$$

If we now apply the above procedure to the fault tree of Fig. 9-4, we get

$$TOP = C_1 \vee L_1 \cdot F_1 \vee F_1 \cdot G_3 \vee G_3 \cdot L_2 \vee L_1 \cdot G_2 \vee G_1 \vee F_2 \cdot G_2 \qquad (10\text{-}6)$$

C_1		
F_2	G_1	
F_2	G_2	
L_2	G_1	
L_2	G_3	
G_1	F_3	L_1
G_2	F_3	L_1
F_1	G_1	L_3
F_1	G_3	L_3
F_1	L_1	
G_1	F_3	L_3

Fig. 10-2. Table of monomials of the fault tree of Fig. 9-3.

The two expressions 10-1 and 10-2 look very different. However they are the same boolean function. This will be shown in the next section. Here we can say that it is not possible to prove whether or not two boolean functions are equal by making use only of algorithms which calculate normal disjunctive forms of boolean functions.

10.3 Step No. 2 - Identification of the complete base

Various algorithms for the identification of the complete base of a boolean function (step No. 2) are available from the literature /9/. An algorithm due to Nelson /10/ is particularly convenient. This algorithm consists simply in complementing (negating) a normal disjunctive form of a boolean function TOP (which from now on we also call ϕ) and then in complementing its complement $\overline{\phi}$. After each of the two complement operations, the three simplification rules (section 10.2) are applied to the result.

Nelson's algorithm can be described as follows

1. Complement ϕ, expand $\overline{\phi}$ into normal disjunctive form and call the result $\overline{F}$.

2. Complement $\overline{F}$, expand F into normal disjunctive form and call the result K.

The disjunction of the monomials of K is the complete base of the boolean function

We now apply the Nelson algorithm to our case, that is to Eq. 10-5. By complementing Eq. 10-5, we can write

$$\overline{TOP} = \overline{C}\cdot(\overline{F}_2 \vee \overline{G}_1)\cdot(\overline{F}_2 \vee \overline{G}_2)\cdot(\overline{L}_2 \vee \overline{G}_1)\cdot(\overline{L}_2 \vee \overline{G}_3)\cdot$$
$$\cdot(\overline{G}_1 \vee \overline{F}_3 \vee \overline{L}_1)\cdot(\overline{G}_2 \vee \overline{F}_3 \vee \overline{L}_1)\cdot(\overline{F}_1 \vee \overline{G}_1 \vee \overline{L}_3)\cdot$$
$$\cdot(\overline{F}_1 \vee \overline{G}_3 \vee \overline{L}_3)\cdot(\overline{F}_1 \vee \overline{L}_1)\cdot(\overline{G}_1 \vee \overline{F}_3 \vee \overline{L}_3) \qquad (10\text{-}7)$$

Now we have

$$\overline{C}_1 = C_2 \qquad (10\text{-}8)$$

$$\overline{G}_k = \bigvee_{q=1}^{4} G_q \quad k\neq q \quad (k=1;\ 2;\ 3;\ 4) \qquad (10\text{-}9)$$

$$\overline{F}_k = \bigvee_{q=1}^{3} F_q \quad k\neq q \quad (k=1;\ 2;\ 3) \qquad (10\text{-}10)$$

and

$$\bar{L}_k = \bigvee_{q=1}^{3} L_q \qquad k \neq q \qquad (k=1;\ 2;\ 3) \qquad (10\text{-}11)$$

By taking into account Eqs. 10-7 to 10-11, Eq. 10-6 becomes

$$\begin{aligned}\overline{TOP} = {} & C_2 \cdot (F_1 \vee F_3 \vee G_2 \vee G_3 \vee G_4) \cdot (F_1 \vee F_3 \vee G_1 \vee G_3 \vee G_4) \cdot \\ & \cdot (L_1 \vee L_3 \vee G_2 \vee G_3 \vee G_4) \cdot (L_1 \vee L_3 \vee G_1 \vee G_2 \vee G_4) \cdot \\ & \cdot (G_2 \vee G_3 \vee G_4 \vee F_1 \vee F_2 \vee L_2 \vee I_3) \cdot (G_1 \vee G_3 \vee G_4 \vee F_1 \vee F_2 \vee L_2 \vee L_3) \cdot \\ & \cdot (F_2 \vee F_3 \vee G_2 \vee G_3 \vee G_4 \vee L_1 \vee L_2) \cdot (F_2 \vee F_3 \vee G_1 \vee G_2 \vee G_4 \vee L_1 \vee L_2) \cdot \\ & \cdot (F_2 \vee F_3 \vee L_2 \vee L_3) \cdot (G_2 \vee G_3 \vee G_4 \vee F_1 \vee F_2 \vee L_1 \vee L_2) \qquad (10\text{-}12)\end{aligned}$$

We execute the operations of Eq. 10-12 and we apply the three simplification rules. We get

$$\begin{aligned}\overline{TOP} = {} & C_2 \cdot G_2 \cdot F_1 \cdot L_2 \vee C_2 \cdot G_2 \cdot F_1 \cdot L_3 \vee C_2 \cdot G_2 \cdot F_3 \cdot L_2 \vee C_2 \cdot G_2 \cdot F_3 \cdot L_3 \vee \\ & \vee C_2 \cdot G_3 \cdot F_2 \cdot L_1 \vee C_2 \cdot G_3 \cdot F_2 \cdot L_3 \vee C_2 \cdot G_3 \cdot F_3 \cdot L_1 \vee C_2 \cdot G_3 \cdot F_3 \cdot L_3 \vee \\ & \vee C_2 \cdot G_4 \cdot F_2 \vee C_2 \cdot G_4 \cdot F_3 \vee C_2 \cdot G_4 \cdot L_2 \vee C_2 \cdot G_4 \cdot L_3 \qquad (10\text{-}13)\end{aligned}$$

We now complement $\overline{TOP}$ and we execute all operations including the application of the three simplification rules. We get finally

$$TOP = L_1 \cdot F_1 \vee F_1 \cdot G_3 \vee G_3 \cdot L_2 \vee L_1 \cdot G_2 \vee G_1 \vee F_2 \cdot G_2 \vee C_1 \qquad (10\text{-}14)$$

Eq. 10-10 is the complete base of the TOP.

We point out that Eq. 10-14 and 10-6 (that is the fault trees of Figs. 9-3 and 9-4) have the same TOP. The knowledge of the complete base of a boolean function is important also because it offers the possibility of finding out if two or more fault trees have the same TOP.

We can state the following criterion

"If two boolean functions have the same complete base they are identical".

Nelson's algorithm was improved by Hulme and Worrell /11/ to reduce the computing time. A modified Nelson's algorithm which allows one to handle multistate components has been developed at Karlsruhe /3/. The execution times of the three algorithms are compared in the table of Fig. 5-3. The examples have been taken from /11/.

Example	Number of prime implicants in complete base	CPU time (sec)		
		Nelson algorithm (CDC6600)	Sandia algorithm (CDC6600)	Karlsruhe algorithm (IBM370/168)
1	4	0.158	0.156	0.11
2	3	0.367	0.182	not performed
3	15	221.418	0.391	0.26
4	15	1413.580	0.388	0.26
5	32	5300(1)	3.868	0.42
6	61	4600(1)	303.657	1.03
7	87	6000(1)	417.371	1.12

(1) These entries indicate times at which execution was terminated without completing the algorithm.

Fig. 10-3. Computational times of different types of Nelson Algorithms.

10.4 Step No. 3 - Extraction of an Irredundant Base (or One of the Smallest Irredundant Bases) from the Complete Base.

Various algorithms for the extraction of the smallest irredundant base of a boolean function from its complete base are available from the literature /9/.

A method, which is called the method of the expansion coefficients, has been developed at Karlsruhe. The basic principles of this method have been described in /3/.

A fast algorithm based on this principle has been developed at Karlsruhe /3/ which allows one to identify the smallest irredundant base of a boolean function. The table of Fig. 10-4 gives the required execution times for the examples 3 to 7 of the table 10-3.

Example	Number of prime implicants in complete base	Number of prime implicants in smallest irredundant base	CPU time needed to identify smallest irredundant base (secs)
3	15	7	0.24
4	15	8	0.23
5	32	12	0.49
6	61	17	6.07
7	87	19	19.51

Fig. 10-4. Computational times of the algorithm for the extraction of the smallest irredundant base.

An even faster algorithm for the extraction of an irredundant base (which is not necessarily the smallest) has been developed at Karlsruhe.

The algorithm can be described as follows

1. Select a prime implicant (say X_j) from a base of the TOP and call α_j the boolean function which results from the disjunction of the remaining prime implicants.

2. Delete from α_j all prime implicants which are mutually exclusive with X_j. In each of the survived monomials replace by 1 all literals which are contained in X_j. Delete subsuming monomials. Call β_j the boolean function which results from the disjunction of the monomials which have been generated by means of the above operations.

3. Complement β_j. If $\bar{\beta}_j \neq 0$, the prime implicant X_j is kept in the base. If instead $\bar{\beta}_j = 0$, X_j is deleted from the base.

The steps 1; 2 and 3 of the algorithm are repeated for each prime implicant X_j of the base. The starting base can be any base of the TOP. In our case the starting base is of course the complete base.

We apply now the algorithm to our example, that is to Eq. 10-14. We have

$$X_1 = L_1 \cdot F_1 \tag{10-15}$$

and

$$\alpha_1 = F_1 \cdot G_3 \vee G_3 \cdot L_2 \vee L_1 \cdot G_2 \vee G_1 \vee F_2 \cdot G_2 \vee C_1 \tag{10-16}$$

We delete now from α_1 the prime implicants $G_3 \cdot L_2$ and $F_2 \cdot G_2$ because they are both mutually exclusive with X_1. In addition we replace by means of 1 the literal F_1 in the prime implicant $F_1 \cdot G_3$ and the literal L_1 in the prime implicant $L_1 \cdot G_2$ because both F_1 and L_1 are contained in X_1.

We get

$$\beta_1 = 1 \cdot G_3 \vee 1 \cdot G_2 \vee G_1 \vee C_1 = G_3 \vee G_2 \vee G_1 \vee C_1 \tag{10-17}$$

We complement now β_1 and we get simply

$$\bar{\beta}_1 = G_4 \cdot C_2 \neq 0 \tag{10-18}$$

Since $\bar{\beta}_1 \neq 0$, X_1 is kept in the base. If we repeat the same procedure for all the other prime implicants of Eq. 10-14, we shall find out that all prime implicants must be kept in the base. This means that in our example the complete base is irredundant, (see chapter 12 on coherent boolean functions).

10.5 Step No. 4 - Expression of the TOP as a Disjunction of Pairwise Mutually Exclusive Simple Boolean Functions.

We have the TOP as disjunction of the prime implicants "X_j" (irredundant base).

$$TOP = \bigvee_{j=1}^{N} X_j \qquad (10\text{-}19)$$

where

N = total number of prime implicants belonging to the irredundant base.

We now want to transform Eq. 10-19 in an expression of the type

$$TOP = \bigvee_{i=1}^{Q} Y_i \qquad (10\text{-}20)$$

where Y_i are simple boolean functions (defined in section 10.1) which are pairwise mutually exclusive, that is satisfy the conditions (Eq.10-3)

$$Y_i \cdot Y_k = 0 \quad i \neq k \quad (i; k = 1; 2...;Q) \qquad (10\text{-}21)$$

In addition each Y_i is of the form (Eq. 10-1)

$$Y_i = M_i \cdot \bigvee_{s=1}^{n_i} P_{is} \quad (i = 1; 2...;Q) \qquad (10\text{-}22)$$

where the M_i and the P_{is} are non-zero boolean monomials. The monomials M_i are called keystone monomials and satisfy the following conditions

$$M_i \cdot M_k = 0 \quad i \neq k \quad (i; k = 1; 2...;Q) \qquad (10\text{-}23)$$

$$\bigvee_{i=1}^{Q} M_i = 1 \qquad (10\text{-}24)$$

A fast algorithm has been developed to identify the keystone monomials.

One starts by selecting a literal of the most frequent primary component in the expression of the TOP (Eq. 10-19). In the case of our example (Eq. 10-14) the most frequent primary component is G. We select therefore G_1.

We have

$$M_1 = G_1 \tag{10-25}$$

We carry out the operation of conjunction between M_i (Eq. 10-25) and the TOP (Eq. 10-14). We get

$$G_1 \cdot TOP = G_1 \tag{10-26}$$

From Eq. 10-26 it follows

$$\bigvee_{s=1}^{n_1} P_{1s} = 1 \tag{10-27}$$

and therefore

$$Y_1 = G_1 \tag{10-28}$$

We put now

$$M_2 = G_2 \tag{10-29}$$

From Eqs. 10-29 and 10-14 we get

$$G_2 \cdot TOP = G_2 \cdot (L_1 \cdot F_1 \vee L_1 \vee F_2 \vee C_1)$$

$$= G_2 \, (L_1 \vee F_2 \vee C_1) \tag{10-30}$$

Since each primary component enters in Eq. 10-30 not more than once, we can write

$$Y_2 = G_2 \cdot (L_1 \vee F_2 \vee C_1) \tag{10-31}$$

By applying the same procedure we identify also Y_3 and Y_4

$$Y_3 = G_3 \cdot (C_1 \vee F_1 \vee L_2)$$

and

$$Y_4 = G_4 \cdot (C_1 \vee L_1 \cdot F_1) \tag{10-32}$$

At this point we observe that Eq. 10-24 is satisfied. We have in fact.

$$\bigvee_{i=1}^{4} M_i = \bigvee_{i=1}^{4} G_i = 1 \tag{10-33}$$

Eq. 10-33 tells us that all simple boolean functions have been identified. We can write therefore

$$TOP = \bigvee_{i=1}^{4} Y_i \tag{10-34}$$

where

$$Y_1 = G_1 \tag{10-35}$$

$$Y_2 = G_2 \cdot (C_1 \vee L_1 \vee F_2) \tag{10-36}$$

$$Y_3 = G_3 \cdot (C_1 \vee F_1 \vee L_2) \tag{10-37}$$

$$Y_4 = G_4 \cdot (C_1 \vee L_1 \cdot F_1) \tag{10-38}$$

10.6 Step No. 5 - Identification of the Inhibiting Variables to be associated with each Simple Function.

Since the primary variables belonging to a dependent primary component have different conditional expectations (table of Fig. 9-5) depending upon the inhibiting variable from which they depend, it is necessary to identify the inhibiting variables associated with each simple function before proceeding to calculate its occurrence probability.

A simple algorithm is the following.
Let us assume that the simple function Y_i contains a literal of the dependent primary component D. Let us indicate with I_k (k=1; 2...;n) the inhibiting variables of D.

The following test is carried out

1. If a literal of D is contained in P_{is} and an inhibiting variable I_k exists for which the relation

$$M_i \cdot P_{is} \cdot I_k = M_i \cdot P_{is} \qquad (10\text{-}39)$$

holds, the simple function Y_i receives the mark I_k.

2. If a literal of D is contained in the keystone monomial M_i and an inhibiting variable I_k exists which satisfies the equation

$$Y_i \cdot I_k = Y_i \qquad (10\text{-}40)$$

the simple function Y_i receives the mark I_k.

3. In all other cases the simple function Y_i is replaced by the following set of simple functions

$Y_i \cdot I_1$ with mark I_1

$Y_i \cdot I_2$ " " I_2

$Y_i \cdot I_n$ " " I_n

Note that at least two of the above newly generated simple functions must be different from zero.

By applying the above algorithm to our example (Eqs. 10-35 to 10-38), we get the table of Fig. 10-5.

The last column of the table of Fig. 10-5 indicates the conditional expectations which must be used in the calculation for each simple function and for each unprivileged primary variable.

Simple Function	Unprivileged Primary Variable	Inhibiting Variable (Mark)	Expected value of unprivileged Primary Variable
Y_1	-	-	-
Y_2	L_1	$G_2 \vee G_4$	$E_2\{L_1\}$
	F_2	$G_1 \vee G_2$	$E_1\{F_2\}$
Y_3	F_1	$G_3 \vee G_4$	$E_2\{F_1\}$
	L_2	$G_1 \vee G_3$	$E_1\{L_2\}$
Y_4	L_1	$G_2 \vee G_4$	$E_2\{L_1\}$
	F_1	$G_3 \vee G_4$	$E_2\{F_1\}$

Fig. 10-5. Table of the inhibiting variables to be associated with each simple function.

11. CALCULATION OF THE OCCURRENCE PROBABILITY OF THE EVENT {TOP = 1}

We now want to calculate the expectation of the TOP variable, that is the occurrence probability of the event {TOP = 1}.

$$E\{TOP\} = P\{TOP = 1\} \tag{11-1}$$

Taking into account Eqs. 10-20 and 10-21 we can write

$$E\{TOP\} = \sum_{i=1}^{Q} E\{Y_i\} \tag{11-2}$$

Taking into account Eq. 10-22 and the fact that all monomials contained in a simple boolean function are all pairwise mutually logically independent, we can write for each Y_i

$$E\{Y_i\} = E\{M_i\} \sum_{s=1}^{n_i} E\{P_{is}\} \prod_{q=1}^{s-1} \left[1 - E\{P_{iq}\}\right] \tag{11-3}$$

Note the remarkable simplicity of Eqs. 11-2 and 11-3. This is due to the properties of the pairwise mutually exclusive simple boolean functions Yi. Note that the functions M_i and P_{is} are monomials. The expectation of a monomial is given by the product of the expectations of the primary variables contained in it. For the unprivileged primary variables one uses the conditional expectations which are identified by the corresponding marks associated with the simple function Y_i (section 10.6).

We have shown in chapter 6 that the bipolar switch (circuit breaker) can be handled as an homogeneously dependent primary component. We recall the theory of section 5-3. Given yn homogeneously dependent primary variable D_j, an inhibiting variable I_k and a variable X_q which does not contain any literal of the primary component D, the following relationship holds

$$E\{D_j \mid I_k \cdot X_q\} \cong E\{D_j \mid I_k\} \tag{11-4}$$

Eq. 11-4 tells us that only the conditional expectation $E\{D_j|I_k\}$ needs to be calculated.

In our example (Eqs. 10-35 to 10-38 and table of Fig. 9-5) we can write

$$E\{Y_1\} = E\{G_1\} = 6 \cdot 10^{-3} \tag{11-5}$$

Taking into account the expression of Y_2 (Eq.10-36), and the conditional expectations of the variables L_1 and F_2 indicated in the table of Fig. 10-5 in correspondence of the simple function Y_2, we can write

$$E\{Y_2\} = E\{G_2\}\left[E\{C_1\} + (1-E\{C_1\})\ E_2\{L_1\} + \right.$$

$$\left. + (1-E\{C_1\})(1-E_2\{L_1\})\ E_1\{F_2\}\right] \qquad (11\text{-}6)$$

By introducing in Eq. 11-6 the numerical values of the table of Fig. 9-5, we get

$$E\{Y_2\} = 1.28\cdot10^{-2}\left[2\cdot10^{-5} + (1-2\cdot10^{-5})\ 1.5\cdot10^{-3} + \right.$$

$$\left. + (1-2\cdot10^{-5})(1-1.5\cdot10^{-3})\ 1.5\cdot10^{-3}\right] \simeq 3.9\cdot10^{-5} \qquad (11\text{-}7)$$

By applying the same procedure to Y_3 (Eq. 10-37) and to Y_4 (Eq. 10-38) we get respectively

$$E\{Y_3\} = E\{G_3\}\left[E\{C_1\} + (1-E\{C_1\})\ E_2\{F_1\} + \right.$$

$$\left. + (1-E\{C_1\})\ (1-E_2\{F_1\})\ E_1\{L_2\}\right] \simeq 2.6\cdot10^{-4} \qquad (11\text{-}8)$$

and

$$E\{Y_4\} = E\{G_4\}\left[E\{C_1\} + (1-E\{C_1\})E_2\{L_1\}\ E_2\{F_1\}\right] \simeq$$

$$\simeq 2\cdot10^{-5} \qquad (11\text{-}9)$$

By applying Eq. 11-2 to our example we get finally.

$$E\{TOP\} = E\{Y_1\} + E\{Y_2\} + E\{Y_3\} + E\{Y_4\} =$$

$$6\cdot10^{-3}+3.9\cdot10^{-5}+2.6\cdot10^{-4}+2\cdot10^{-5} \simeq 6.32\cdot10^{-3} \qquad (11\text{-}10)$$

12. Coherent boolean functions

In the literature great importance is given to the concept of coherence. Some authors /14/ argue that most technical systems are coherent in the sense that the TOPs of the fault trees of such systems are coherent boolean functions.

In the case of systems with binary components, a boolean function is said to be coherent if it is monotonic with respect to all its basic variables. In /9/ it is shown (1) that no prime implicant of a coherent boolean function contains negated literals (i.e. no intact state of the primary components) and (2) that a coherent boolean function has only one base which is complete and irredundant at the same time. Note that it can be shown that the property number 2 is a consequence of the property Nr. 1.

The problem of defining a coherent boolean function in the case of systems with multistate components is not straight forward.

Some authors /22/ extend the concept of a monotonic boolean function to the case of multistate components by introducing an ordered set of values for each primary component. This type of ordered logic can be applied only to problems in which a decreasing scale of values can be assigned to the states of the primary components (from the intact state which is the least failed to the complete failed state which is the most failed). Many technical systems however cannot be treated by using an ordered logic. It would be in fact very hard to decide whether or not the state "failed closed" of a circuit breaker is more failed than the state "failed open". We have used in our paper a non-ordered logic which can be applied in principle to any type of problem. For this reason it is difficult to extend the concept of monotonic boolean function to the case of the boolean algebra with restrictions on variables. We can however define a coherent boolean function by referring to a special property of its complete base. The following definition is proposed

> "A boolean function is said to be coherent if at least one literal of each primary component does not appear in the complete base of the function".

Note that the proposed definition is based on an extension of the property Nr. 1 of the binary case. The above definition tells us that each primary component must appear in the complete base of the function with a number of literals lower than its total number of states. For instance in the complete base of our example (Eq. 10-14) the literals associated with the intact states of all primary components (G_4,C_2,F_3,L_3) do not appear in the complete base. According to the definition proposed above, we can therefore say that our TOP (Eq. 10-14) is a coherent boolean function. In addition it is not difficult to demonstrate that a coherent boolean function has only one base which is at the same time complete and irredundant /23/. This is the same as property 2 in the binary case. In the case of our example (Eq. 10-14) we have verified that the complete base is also irredundant (see section 10.3).

The concept of coherency is very important because, if it is known in advance that a boolean function is coherent, one can enormously simplify the algorithm for the identification of the complete base (section 10.2). It is in fact possible to demonstrate that the following rule holds

> "The complete base of a coherent boolean function can be obtained from any of its normal disjunctive forms by replacing by 1 all literals which are known not to appear in the complete base and by applying the absorption rule among the monomials".

We apply now the above rule to our example. We write again the associated normal disjunctive form (Eq. 10-5)

$$TOP = C_1 \vee F_2 \cdot G_1 \vee F_2 \cdot G_2 \vee L_2 \cdot G_1 \vee L_2 \cdot G_3 \vee G_1 \cdot F_3 \cdot L_1 \vee$$
$$\vee G_2 F_3 L_1 \vee F_1 G_1 L_3 \vee F_1 G_3 L_3 \vee F_1 L_1 \vee G_1 F_3 L_3 \qquad (12\text{-}1)$$

Let us now assume that, due to some technical considerations, we already know that the literals associated with the intact states of the primary components will not be present in the complete base. These literals are: $G_4; F_3; L_3$ and C_2. We replace now by 1 the above literals in Eq. 12-1. We get

$$TOP = C_1 \vee F_2 G_1 \vee F_2 G_2 \vee L_2 G_1 \vee L_2 G_3 \vee G_1 \cdot 1 \cdot L_1 \vee G_2 \cdot 1 \cdot L_1 \vee$$
$$\vee F_1 G_1 1 \vee F_1 G_3 1 \vee F_1 L_1 \vee G_1 \cdot 1 \cdot 1 \qquad (12\text{-}2)$$

Eq. 12-2 can be written as follows

$$TOP = C_1 \vee F_2 G_1 \vee F_2 G_2 \vee L_2 G_1 \vee L_2 G_3 \vee G_1 L_1 \vee G_2 L_1 \vee$$
$$\vee F_1 G_1 \vee F_1 G_3 \vee F_1 L_1 \vee G_1 \qquad (12\text{-}3)$$

Eq. 12-3 contains the monomial G_1 which is implied by the monomials $F_2 G_1$; $L_2 G_1$; $G_1 L_1$ and $F_1 G_1$. These monomials can therefore be deleted (absorption rule). Eq. 12-3 becomes finally

$$TOP = C_1 \vee F_2 G_2 \vee L_2 G_3 \vee G_2 L_1 \vee F_1 G_3 \vee G_1 \vee F_1 L_1 \qquad (12\text{-}4)$$

We point out that Eq. 12-4 is identical with Eq. 10-14 which has been shown to be the complete base of the TOP.

An extensive and exhaustive treatment of coherent boolean functions in the case of multistate components goes beyond the limits of this paper. The problem of coherency will be treated in another paper which is being prepared /23/. It is important to point out at this stage that the greatest problem is that of recognizing in advance whether or not a boolean function is coherent and of identifying in advance which literals will not appear in the complete base. Whilst most technical systems appear to be coherent, to the best knowledge of the author there exists no general mathematical rule which allows one to establish "a priori" the coherence of any system, except of course in the case in which the intact literal of each primary component does not appear in the associated normal disjunctive form of the fault tree.

13. CONCLUSIONS

The following conclusions can be drawn:

1. The theory described in this paper is a powerful tool for the analysis of fault trees containing multistate (two or more than two states) primary components which can be statistically independent as well as dependent. This means that a very wide spectrum of problems (which are met in practice) can now be solved analytically by applying this theory.

2. A new definition of fault tree has been suggested. In contrast to the old definition the basic boolean variables are not any more associated with the primary components but with the states of the primary components.

3. A special type of boolean algebra has been developed: this is the boolean algebra with restrictions on variables.

   In contrast with the multivalued logic approach /6/, the basic rules of the boolean algebra with restrictions on variables are the same as those of the traditional boolean algebra with some additional rules due to the restrictions.

   In addition, due to the fact that the variables are binary, the operation of expectation of variables can be used for the calculation of the occurrence probability of events.

4. In the state analysis the net of states considered is characterized by a very fine mesh. The net used in the fault tree analysis has instead a much coarser mesh. Since the problem of statistical dependence among components (such as common mode failure) affects the fine structure of a system, the coarse mesh used in the fault tree analysis is not suitable to handle the problem of statistical dependence. On the other hand the fine mesh used in the state analysis, although it would be suitable to cope with statistical dependence, is much too fine to handle complex systems.

   It is therefore clear that an intermeidate mesh size is required for the analysis of statistical dependencies in complex systems. This mesh must be fine enough to retain the basic properties of statistical dependence and sufficiently coarse to still allow one to analyze complex systems. It has been shown that this can be obtained by properly combining fault tree analysis with state analysis. The boolean algebra with restrictions on variables is the mathematical tool which allows this synthesis.

5. The definition of component has been generalized. A new classification of components into two groups privileged and unprivileged has been proposed. It has been shown that this classification eases the calculation of the expectation of a stochastic boolean variable especially in the case of statistical dependence.

6. The problem of statistical dependence has been solved either (1) by removing it, that is by replacing in the fault tree the statistically dependent primary variables by means of "ad hoc" new defined primary variables, or (2) by evaluating separately (by means of the state analysis) the conditional expectations of the dependent variables. The theory then provides the tools for correctly incorporating these conditional expectations in the fault tree analysis.

   Criteria to establish which one of the two methods should be chosen have been given in the paper.

7. A new definition of coherency has been put forward in this paper. We recall it again

   "A boolean function is said to be coherent if at least one literal of each primary component does not appear in the complete base of the function".

   In chapter 12 it has been shown that the above definition is consistant with the old definition which applies only to systems with binary components. A simplified algorithm for the identification of the complete base is also given in chapter 12. Since the use of this simplified algorithm is limited to the case of coherent systems only, one is bound to use in the general case more complex algorithms like the Nelson algorithm (section 10.3).

8. The method uses also an expression of the TOP variable as a disjunction of pairwise mutually exclusive simple boolean functions. This eases the calculation of the occurrence probability of the top event.

9. The analytical computer code MUSTAFA 1 based on the above theory has been developed. It can handle fault trees of systems containing statistically independent as well as dependent components with two or more than two states.

   MUSTAFA 1 can handle coherent as well as non coherent boolean functions.

A sample problem ahs been analysed by using MUSTAFA 1. The problem contained three different types of dependencies which are commonly met in practice, namely (1) common mode failure, (2) components characterized by failure rates which take values which depend upon the occurrence of some non-primary events, and (3) the case of a component whose repair affects the operation of another component.

MUSTAFA 1 solved the problem successfully.

10. An important feature of MUSTAFA 1 is that of allowing the identification of the complete base of a boolean variable. This gives the possibility of comparing different reliability analyses of the same system at the level of events.

The comparison among different reliability analyses of the same system must be carried out not only at the level of probabilities (as it is usually done) but also at the level of events. In fact two TOP events, although they are different, could have the same occurrence probability. On the other hand two fault trees of the same system, although they look different, are equal if they have the same complete base. This has been shown in this paper.

In addition a system was given to three different persons. Three different fault trees were generated for the same TOP variable. The three associated normal disjunctive forms (output from the downward algorithm) were calculated and they looked remarkably different from each other (large differences in the total number of monomials as well as in their composition). However, it was possible to verify that the three functions were identical by calculating the complete base which proved to be exactly the same for all three fault trees /20/.

It is not possible to carry out in general this type of comparison by using the conventional analytical programs (e.g. /7/) because these programs, in addition to the limitation of handling fault trees with only binary components, cannot handle negated variables. In other words the use of these programs allows one to handle only a very special class of fault trees, namely those fault trees in which the associated normal disjunctive form is identical with the only base which is at the same time complete and irredundant.

The problem of comparison among fault trees is becoming more important because the confidence in the reliability analyses of systems will increase if the analyses are carried out by different and independent organizations.

11. The knowledge of the complete base eases also the identification of the primary components which most contribute to system unavailability. This has been shown in the analysis of the emergency core cooling system of the nuclear fast reactor SNR 300 /20/.

12. Finally it is worthwhile to point out that the adoption of computer programs for automatic fault tree construction /18/ will require the use of the boolean algebra with restrictions on variables. These programs in fact generate non-conventional fault trees which cannot be in general analyzed by the conventional computer programs for fault tree analysis which are being used today.

    A computer program is being developed at Karlsruhe /19/ to properly couple the basic theory of automatic fault tree construction with the theory developed in this paper. The use of this computer program will allow one to identify the complete base of a boolean function without even drawing a fault tree of the system. This is the same as saying fault tree analysis without fault tree!

14. ACKNOWLEDGEMENTS

The author wishes to thank Dr. Wenzelburger, Mr. Clair and Mr. Guagnini for the fruitful discussions about the theory developed in this paper.

15. REFERENCES

1. W.E. Vesely, 1970, "A time dependent methodology for fault tree evaluation", Nucl. Eng. Des. 13, 337-360.

2. L. Caldarola, A. Wickenhäuser, 1977, "Recent Advancements in fault tree methodology at Karlsruhe", International Conf. on Nucl. Systems Reliability Engineering and Risk Assessment, Gatlingburg, SIAM, 518-542, June 1977.

3. L. Caldarola, 1978, "Fault tree analysis of multistate systems with multistate components", ANS Topical Meeting on Probabilistic Analysis of Nuclear Reactor Safety, Los Angeles, California, Paper VIII.1, May 1978.

4. J.D. Murchland, G. Weber, 1972, "A moment method for the calculation of a confidence interval for the failure probability of a system", IEEE Proceedings Annual Symposium on Reliability.

5. C. Berge, 1962, "The theory of graphs", Methuen and John Wiley

6. P. Mussio, S. Garriba, S. Fumagalli, 1978, "Multiple valued logic in system representation", NATO ASI Conference, Urbino, Italy, July 1978

7. J.B. Fussell, E.B. Henry, N.N. Marschall, 1974, "MOCUS: a computer program to obtain minimal sets from fault trees", ANCR-1156.

8. L. Caldarola, A. Wickenhäuser, 1977, "The Karlsruhe computer program for the evaluation of the availability and reliability of complex repairable systems", Nucl. Eng. Des. 43, 463-470.

9. J. Kuntzmann, 1967, "Fundamental Boolean Algebra," Blackie and Sons Ltd.

10. R.J. Nelson, 1954, "Simplest normal truth functions", the Journal of Symbolic Logic, vol. 20, Nr. 2, 105-108.

11. B.L. Hulme, R.B. Worrell, 1975, "A prime implicant algorithm with factoring", IEEE Transaction on computers, vol. C-24, Nr. 11, 1129-1131.

12. L. Caldarola, 1979, "Fault tree analysis with multistate components", KFK 2761.

13. R.A. Howard, 1971, "Dynamic Probabilistic Systems", John Wiley and Sons

14. R.E. Barlow, 1975, "Statistical theory of reliability and life testing. Probability models", Holt Rinehert and Winston, INC.

15. D.R. Cox and H.D. Miller, 1972, "The theory of Stochastic Processes" Chapman and Hall Ltd.

16. L. Caldarola, 1977, "Unavailability and failure intensity of components", Nucl. Eng. Des. 44 (1977), 147-162.

17. K. Kotthoff, W. Otto
(unpublished)

18. S.L. Salem, G.E. Apostolakis and D. Okrent, 1976, "A computer-oriented approach to fault tree construction", EPRI NP-288.

19. P. Schwab, "Doctor Thesis on automatic fault tree construction" (in preparation).

20. L. Caldarola, H. Wenzelburger, A. Wickenhäuser
(unpublished)

21. W. Feller, 1968, "An introduction to probability theory and its applications", Wiley International.

22. R.E. Barlow and A.S. Wu, "Coherent systems with multistate components", Mathematics of operation research, Vol. 3, No. 4, November 1978 , 275-281.

23. L. Caldarola, "Coherent systems with multistate components". (accepted for publication in Nuclear Engineering and Design).

24. L. Caldarola, 1980, "Grundlagen der Booleschen Algebra mit beschränkten Variablen", KfK 2915.